

# Cisco Virtualization Solution for EMC VSPEX with VMware vSphere 5.1 Solution for up to 1000 Virtual Machines

Last Updated: October 18, 2013



Building Architectures to Solve Business Problems



# cisco.





# About the Authors



Mehul Bhatt



Prashanto Kochavara

#### Mehul Bhatt, Cisco Systems

Mehul Bhatt has over 12 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 Masters degree in computer systems engineering and holds various Cisco career certifications.

#### Prashanto, EMC Corporation

Prashanto has been working for the EMC solutions group for over 3 years. Prashanto is a SME on EMC Storage and Virtualization technologies including VMware and Hyper-V. He has vast amount of experience in end-to-end solution planning and deployments of VSPEX architectures. Prior to joining the solutions group at EMC, Prashanto has interned as a Systems Engineer (EMC) and Software Developer (MBMS Inc.). Prashanto holds a Bachelors degree in Computer Engineering from SUNY Buffalo and will be graduating with a Masters Degree in Computer Science from North Carolina State University in December 2013.

# **Acknowledgements**

Γ

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

- Vadiraja Bhatt-Cisco
- Tim Cerling-Cisco
- Vijaykumar D-Cisco
- Bathu Krishnan-Cisco
- Sindhu Sudhir-Cisco
- Kevin Phillips-EMC
- John Moran-EMC
- Kathy Sharp-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 SUP-PLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <a href="http://www.cisco.com/go/trademarks">http://www.cisco.com/go/trademarks</a>. 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. (1005R)

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.

© 2013 Cisco Systems, Inc. All rights reserved.

# **EMC**<sup>2</sup>

# Cisco Virtualization Solution for EMC VSPEX with VMware vSphere 5.1 Solution for up to 1000 Virtual Machines

# **Executive Summary**

Cisco solution for EMC VSPEX is a pre-validated and modular architecture built with proven best of-breed technologies to create complete end-to-end virtualization solutions that enable you to make an informed decision while choosing the hypervisor, compute, storage and networking layers. VSPEX drastically reduces server virtualization planning and configuration burdens. VSPEX infrastructures accelerate your IT Transformation by enabling faster deployments, greater flexibility of choice, efficiency, and lower risk. This Cisco Validate Design document focuses on the VSPEX VMware architecture for mid-market business segments with less than 1000 typical Virtual Machines load.

# Introduction

......

CISCO

Virtualization is a key and critical strategic deployment model for reducing the Total Cost of Ownership (TCO) and achieving better utilization of the platform components like hardware, software, network and storage. However, choosing an appropriate platform for virtualization can be challenging. Virtualization platforms should be flexible, reliable, and cost effective to facilitate the deployment of various enterprise applications. In a virtualization platform to utilize compute, network, and storage resources effectively, the ability to slice and dice the underlying platform is essential to size to the application requirements. The Cisco solution for the EMC VSPEX provides a very simplistic yet fully integrated and validated infrastructure to deploy VMs in various sizes to suit various application needs.

# **Target Audience**

The reader of this document is expected to have the necessary training and background to install and configure VMware vSphere, EMC VNX series storage arrays, and Cisco Unified Computing System (UCS) and UCS Manager. External references are provided where ever 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 describes the steps required to deploy and configure a Cisco solution for EMC VSPEX for VMware architectures to a level that will allow for confirmation that the basic components and connections are working correctly. The document covers VMware architectures for SMBs, typically for 1000 VMs or less. This document showcases two variants of the solution:

- FC-variant—EMC VNX series storage array directly attached to UCS FIs using FC for storage access.
- NFS-variant—EMC VNX series storage array using NFS for storage access through pair of Cisco Nexus 5000-Series switches.

While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are required for deploying these solutions are specifically mentioned.

# **Business Needs**

The VSPEX solutions are built with proven best-of-breed technologies to create complete virtualization solutions that enable you to make an informed decision in the hypervisor, server, and networking layers. The VSPEX infrastructures accelerate your IT transformation by enabling faster deployments, greater flexibility of choice, efficiency, and lower risk.

Business applications are moving into the consolidated compute, network, and storage environment. The Cisco solution for the EMC VSPEX using VMware reduces the complexity of configuring every component of a traditional deployment model. The complexity of integration management is reduced while maintaining the application design and implementation options. Administration is unified, while process separation can be adequately controlled and monitored. The following are the business needs for the Cisco solution for EMC VSPEX VMware architectures:

- Provide an end-to-end virtualization solution to utilize the capabilities of the unified infrastructure components.
- Provide a Cisco VSPEX for VMware ITaaS solution for efficiently virtualizing virtual machines for varied customer use cases.
- Show implementation progression of VMware vCenter 5.1 design and the results.
- Provide a reliable, flexible and scalable reference design.

# **Solution Overview**

The Cisco solution for EMC VSPEX using VMware vSphere 5.1 provides an end-to-end architecture with Cisco, EMC, VMware, and Microsoft technologies that demonstrate support for up to 1000 generic virtual machines and provide high availability and server redundancy.

I

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

- Cisco B-Series or C-Series Unified Computing System servers (as per customer's choice)
- Cisco UCS 5108 Chassis

- Cisco UCS 2204XP Fabric Extenders
- Cisco UCS 6248UP Fabric Interconnects
- Cisco UCS Manager 2.1(3a)
- Cisco VIC adapters
- Cisco Nexus 5548UP Switches
- Cisco Nexus 1000v Virtual Switch
- EMC VNX5400, VNX5600, VNX5800 storage array as per the scalability needs
- VMware vCenter 5.1
- Microsoft SQL database
- VMware DRS
- VMware HA

The solution is designed to host scalable, and mixed application workloads for up to 1000 reference virtual machines.

# **Technology Overview**

# **Cisco Unified Computing System**

The Cisco Unified Computing System is a next-generation data center platform that unites compute, network, and storage access. The platform, optimized for virtual environments, is designed using open industry-standard technologies and aims 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. It is an integrated, scalable, multi chassis platform in which all resources participate in a unified management domain.

The main components of Cisco Unified Computing System are:

- **Computing**—The system is based on an entirely new class of computing system that incorporates blade servers based on Intel Xeon E5-2600 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), Fibre Channel, Fibre Channel over Ethernet (FCoE). This provides customers with choice for storage access and investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.

The Cisco Unified Computing System is designed to deliver:

- A reduced Total Cost of Ownership (TCO) and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system which unifies the technology in the data center.
- Industry standards supported by a partner ecosystem of industry leaders.

### **Cisco UCS Manager**

Cisco UCS Manager provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System through 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.

### **Cisco UCS Fabric Interconnect**

The Cisco<sup>®</sup> UCS 6200 Series Fabric Interconnect is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco UCS 6200 Series offers line-rate, low-latency, lossless 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) and Fibre Channel functions.

The Cisco UCS 6200 Series provides the management and communication backbone for the Cisco UCS B-Series Blade Servers and Cisco UCS 5100 Series Blade Server Chassis. All chassis, and therefore all blades, attached to the Cisco UCS 6200 Series Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabric, the Cisco UCS 6200 Series provides both the LAN and SAN connectivity for all blades within its domain.

From a networking perspective, the Cisco UCS 6200 Series uses a cut-through architecture, supporting deterministic, low-latency, line-rate 10 Gigabit Ethernet on all ports, 1Tb switching capacity, 160 Gbps bandwidth per chassis, independent of packet size and enabled services. The product family supports Cisco low-latency, lossless 10 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over a lossless Ethernet fabric from a blade server through an interconnect. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

#### **Cisco UCS 6248UP Fabric Interconnect**

The Cisco UCS 6248UP 48-Port Fabric Interconnect is a one-rack-unit (1RU) 10 Gigabit Ethernet, FCoE and Fiber Channel switch offering up to 960-Gbps throughput and up to 48 ports. The switch has 32 1/10-Gbps fixed Ethernet, FCoE and FC ports and one expansion slot.

#### Figure 1 Cisco UCS 6248UP Fabric Interconnect

	81260	TANY TANG SANG TANG SANG HANG SANG SANG - CANG BANG DANG DANG BANG PANG DANG DANG	0	
	4.6.	[-]-]-]-]-]-]-]-] <b>2</b> [-]-]-]-]-]-]-]-] <b>2</b> [		
п	CISCO.			
	1.1	······································		
	a: 0	000000000000000000000000000000000000000		

# **Cisco UCS Fabric Extenders**

Fabric Extenders are zero-management, low-cost, low-power consuming devices that distribute the system's connectivity and management planes into rack and blade chassis to scale the system without complexity. Designed never to lose a packet, Cisco fabric extenders eliminate the need for top-of-rack Ethernet and Fibre Channel switches and management modules, dramatically reducing infrastructure cost per server.

#### **Cisco UCS 2232PP Fabric Extender**

The Cisco Nexus® 2000 Series Fabric Extenders comprise a category of data center products designed to simplify data center access architecture and operations. The Cisco Nexus 2000 Series uses the Cisco® Fabric Extender architecture to provide a highly scalable unified server-access platform across a range of 100 Megabit Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, unified fabric, copper and fiber connectivity, rack, and blade server environments. The platform is ideal to support today's traditional Gigabit Ethernet while allowing transparent migration to 10 Gigabit Ethernet, virtual machine-aware unified fabric technologies.

The Cisco Nexus 2000 Series Fabric Extenders behave as remote line cards for a parent Cisco Nexus switch or Fabric Interconnect. The fabric extenders are essentially extensions of the parent Cisco UCS Fabric Interconnect switch fabric, with the fabric extenders and the parent Cisco Nexus switch together forming a distributed modular system. This architecture enables physical topologies with the flexibility and benefits of both top-of-rack (ToR) and end-of-row (EoR) deployments.

Today's data centers must have massive scalability to manage the combination of an increasing number of servers and a higher demand for bandwidth from each server. The Cisco Nexus 2000 Series increases the scalability of the access layer to accommodate both sets of demands without increasing management points within the network.



cites	CRED	NEXUS IN	1947 1953	C FADRIC	0000		-	-	-	:::		1	1		:::				- 1	:::							2
	•		47	47		-	-	47	17		•	-	47			-	47	47	1			-				F	1
	+1	11	27	+1	Θ	÷ 2	43	43	8.5	0	13	42	11	63	0	22	03	43	42	Θ	÷1	t1	t I	+1	0	i.	3

# Cisco C220 M3 Rack Mount Servers

Building on the success of the Cisco UCS C220 M3 Rack Servers, the enterprise-class Cisco UCS C220 M3 server further extends the capabilities of the Cisco Unified Computing System portfolio in a 1-rack-unit (1RU) form factor. And with the addition of the Intel® Xeon® processor E5-2600 V2.





The Cisco UCS C220 M3 also offers up to 256 GB of RAM, eight drives or SSDs, and two 1GE LAN interfaces built into the motherboard, delivering outstanding levels of density and performance in a compact package.

# **Cisco UCS Blade Chassis**

The Cisco UCS 5100 Series Blade Server Chassis is a crucial building block of the Cisco Unified Computing System, delivering a scalable and flexible blade server chassis.

The Cisco UCS 5108 Blade Server Chassis, is six rack units (6RU) high and can mount in an industry-standard 19-inch rack. A single chassis can house up to eight half-width Cisco UCS B-Series Blade Servers and can accommodate both half-width and full-width blade form factors.

Four single-phase, hot-swappable power supplies are accessible from the front of the chassis. These power supplies are 92 percent efficient and can be configured to support non-redundant, N+ 1 redundant and grid-redundant configurations. The rear of the chassis contains eight hot-swappable fans, four power connectors (one per power supply), and two I/O bays for Cisco UCS 2204XP Fabric Extenders.

A passive mid-plane provides up to 40 Gbps of I/O bandwidth per server slot and up to 80 Gbps of I/O bandwidth for two slots. The chassis is capable of supporting future 40 Gigabit Ethernet standards. The Cisco UCS Blade Server Chassis is shown in Figure 4.



Figure 4 Cisco Blade Server Chassis (front and back view)

# **Cisco UCS Blade Servers**

Delivering performance, versatility and density without compromise, the Cisco UCS B200 M3 Blade Server addresses the broadest set of workloads, from IT and Web Infrastructure through distributed database.

Building on the success of the Cisco UCS B200 M2 blade servers, the enterprise-class Cisco UCS B200 M3 server, further extends the capabilities of Cisco's Unified Computing System portfolio in a half blade form factor. The Cisco UCS B200 M3 server harnesses the power and efficiency of the Intel Xeon E5-2600 V2 processor product family, up to 768 GB of RAM, 2 drives or SSDs and up to 2 x 20 GbE to deliver exceptional levels of performance, memory expandability and I/O throughput for nearly all applications. In addition, the Cisco UCS B200 M3 blade server offers a modern design that removes the need for redundant switching components in every chassis in favor of a simplified top of rack design, allowing more space for server resources, providing a density, power and performance advantage over previous generation servers. The Cisco UCS B200M3 Server is shown in Figure 5.

#### Figure 5 Cisco UCS B200 M3 Blade Server



# **Cisco Nexus 5548UP Switch**

The Cisco Nexus 5548UP is a 1RU 1 Gigabit and 10 Gigabit Ethernet switch offering up to 960 gigabits per second throughput and scaling up to 48 ports. It offers 32 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots. These slots have a combination of Ethernet/FCoE and native FC ports. The Cisco Nexus 5548UP switch is shown in Figure 6.



### **Cisco I/O Adapters**

Cisco UCS Blade Servers support various Converged Network Adapter (CNA) options. Cisco UCS Virtual Interface Card (VIC) 1240 is used in this EMC VSPEX solution.

The Cisco UCS Virtual Interface Card 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.



The Cisco UCS rack mount server has various Converged Network Adapters (CNA) options. The UCS 1225 Virtual Interface Card (VIC) option is used in this Cisco Validated Design.

A Cisco® innovation, the Cisco UCS Virtual Interface Card (VIC) 1225 is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers.

UCS 1225 VIC provides the capability to create multiple vNICs (up to 128) on the CNA. This allows complete I/O configurations to be provisioned in virtualized or non-virtualized environments using just-in-time provisioning, providing tremendous system flexibility and allowing consolidation of multiple physical adapters.

System security and manageability is improved by providing visibility and portability of network policies and security all the way to the virtual machines. Additional 1225 features like VM-FEX technology and pass-through switching, minimize implementation overhead and complexity.

#### Figure 8

Cisco UCS 1225 VIC



### **Nexus 1000v Virtual Switch**

Nexus 1000v is a virtual Ethernet switch with two components:

- Virtual Supervisor Module (VSM)—The control plane of the virtual switch that runs NX OS.
- Virtual Ethernet Module (VEM)—A virtual line card embedded into each VMware vSphere hypervisor host (ESXi).

Virtual Ethernet Modules across multiple ESXi hosts form a virtual Distributed Switch (vDS). Using the Cisco vDS VMware plug-in, the VIC provides a solution that is capable of discovering the Dynamic Ethernet interfaces and registering all of them as uplink interfaces for internal consumption of the vDS. The vDS component on each host discovers the number of uplink interfaces that it has and presents a switch to the virtual machines running on the host. All traffic from an interface on a virtual machine is sent to the corresponding port of the vDS switch. The traffic is then sent out to physical link of the host using the special uplink port-profile. This vDS implementation guarantees consistency of features and better integration of host virtualization with rest of the Ethernet fabric in the data center.



#### Figure 9 Nexus 1000v Virtual Distributed Switch Architecture

### **UCS 2.1 Singe Wire Management**

I

Cisco UCS Manager 2.1 supports an additional option to integrate the C-Series Rack-Mount Server with Cisco UCS Manager called "single-wire management". This option enables Cisco UCS Manager to manage the C-Series Rack-Mount Servers using a single 10 GE link for both management traffic and data traffic. When you use the single-wire management mode, one host facing port on the FEX is sufficient to manage one rack-mount server, instead of the two ports you will use in the Shared-LOM mode. Cisco VIC 1225, Cisco UCS 2232PP FEX and Single-Wire management feature of UCS 2.1 tremendously increases the scale of C-Series server manageability. By consuming as little as one port on the UCS Fabric Interconnect, you can manage up to 32 C-Series server using single-wire management feature.

# **UCS** Differentiators

Cisco's 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. Also, a pair of FIs can manage up to 40 chassis, each containing 8 blade servers. This gives enormous scaling on the management plane.
- 2. Unified fabric—In UCS, from blade server chassis or rack server fabric-extender to FI, there is a single Ethernet cable used for LAN, SAN and management traffic. This converged I/O results in reduced cables, SFPs and adapters reducing capital and operational expenses of overall solution.
- **3. Auto Discovery**—By simply inserting the blade server in the chassis or connecting rack server to the fabric extender, discovery and inventory of compute resource occurs automatically without any management intervention. The combination of unified fabric and auto-discovery enables the wire-once architecture of UCS, where compute capability of UCS can be extended 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 UCS Manager, it can be automatically classified to a given resource pool based on policies defined. This capability is useful in multi-tenant cloud computing. This CVD showcases the policy based resource classification of UCS Manager.
- 5. Combined Rack and Blade server management—UCS Manager 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 combinations of B and C series servers to demonstrate stateless and form-factor independent computing work load.
- 6. Model based management architecture—UCS Manager architecture and management database is model based and data driven. An open, standard based XML API is provided to operate on the management model. This enables easy and scalable integration of UCS Manager with other management system, such as VMware vCloud director, Microsoft System Center, and Citrix Cloud Platform.
- 7. Policies, Pools, Templates—The management approach in UCS Manager is based on defining policies, pools and templates, instead of cluttered configuration, which enables a simple, loosely coupled, data driven approach in managing compute, network and storage resources.
- 8. Loose referential integrity—In UCS Manager, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each-other. This provides great flexibility where different experts from different domains, such as network, storage, security, server and virtualization work together to accomplish a complex task.
- **9. Policy resolution**—In UCS Manager, a tree structure of organizational unit hierarchy can be created that mimics the real life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to another policy by name is resolved in the organization hierarchy with closest policy match. If no policy with specific name is found in the hierarchy of the root organization, then special policy named "default" is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibility to owners of different organizations.

- **10.** Service profiles and stateless computing—A service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.
- Built-in multi-tenancy support—The combination of policies, pools and templates, loose referential integrity, policy resolution in organization hierarchy and a service profiles based approach to compute resources makes UCS Manager inherently friendly to multi-tenant environment typically observed in private and public clouds.
- **12.** Extended Memory—The extended memory architecture of UCS servers allows up to 760 GB RAM per server allowing huge VM to physical server ratio required in many deployments, or allowing large memory operations required by certain architectures like Big-Data.
- **13.** 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 administrators' team. VM-FEX also off loads 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.
- 14. 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 UCS Manager by representing all system classes in one GUI panel.

# VMware vSphere 5.1

VMware vSphere 5.1 is a next-generation virtualization solution from VMware which builds upon vSphere5.0 and provides greater levels of scalability, security, and availability to virtualized environments. vSphere 5.1 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 5.1 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 Nexus 1000v 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 the network ports that have Layer 2 configurations, port access and security policies, monitoring features, and so on, that have been pre-defined by the network administrators; in the same way they need to plug in their physical servers to a previously-configured access switch. In this virtualized environment, the network port configuration/policies move with the virtual machines when the virtual machines are migrated to different server hardware.

# **EMC Storage Technologies and Benefits**

This document describes the steps required to deploy and configure a Cisco solution for EMC VSPEX with VMware architectures. This architecture has two variants:

- FC-variant of the solution, where EMC VNX series storage devices are attached to UCS FIs directly, accessing storage over Fibre Channel protocol.
- NFS-variant of the solution, where EMC VNX series storage devices are accessed from UCS through a pair of Nexus 5000 Series switches, accessing storage over NFS protocol.

The EMC VNX<sup>TM</sup> family is optimized for virtual applications delivering industry-leading innovation and enterprise capabilities for file, block, and object 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.

VNX series is designed to meet the high-performance, high-scalability requirements of midsize and large enterprises. The EMC VNX storage arrays are multi-protocol platform that can support the iSCSI, NFS, Fibre Channel, and CIFS protocols depending on the customer's specific needs. This solution was validated using NFS and FC for data storage of virtual machines and Fibre Channel for hypervisor SAN boot.

VNX series storage arrays have the following customer benefits:

- Next-generation unified storage, optimized for virtualized applications.
- Capacity optimization features including compression, deduplication, thin provisioning, and application-centric copies.
- High availability, designed to deliver five 9s availability.
- Multiprotocol support for file and block.
- Simplified management with EMC Unisphere<sup>™</sup> for a single management interface for all network-attached storage (NAS), storage area network (SAN), and replication needs.

# **Software Suites**

The following are the available EMC software suites:

- Remote Protection Suite—Protects data against localized failures, outages, and disasters.
- Application Protection Suite—Automates application copies and proves compliance.
- Security and Compliance Suite—Keeps data safe from changes, deletions, and malicious activity.

# Software Packs

Total Value Pack—Includes all protection software suites, and the Security and Compliance Suite. This is the available EMC protection software pack.

### **EMC** Avamar

EMC's Avamar® data deduplication technology seamlessly integrates into virtual environments, providing rapid backup and restoration capabilities. Avamar's deduplication results in vastly less data traversing the network, and greatly reduces the amount of data being backed up and stored; resulting in storage, bandwidth and operational savings.

The following are the two most common recovery requests used in backup and recovery:

• **File-level recovery**—Object-level recoveries account for the vast majority of user support requests. Common actions requiring file-level recovery are—individual users deleting files, applications requiring recoveries, and batch process-related erasures.

1

• **System recovery**—Although complete system recovery requests are less frequent in number than those for file-level recovery, this bare metal restore capability is vital to the enterprise. Some of the common root causes for full system recovery requests are viral infestation, registry corruption, or unidentifiable unrecoverable issues.

The Avamar System State protection functionality adds backup and recovery capabilities in both of these scenarios.

# **Architectural Overview**

This CVD focuses on the architecture for EMC VSPEX for VMware private cloud, targeted for mid-market segment, using VNX storage arrays. There are two variants of the architecture: FC-variant and NFS-variant. FC-variant of the architecture uses UCS 2.1(3a) with combined B-series and C-series servers with VNX5400 directly attached to UCS fabric interconnect. NFS-variant of the architecture uses UCS 2.1(3a) with B-series and C-series servers with VNX5600 or VNX5800 storage array attached to the Nexus 5548 switches. In both variants, the C220 M3 servers are connected with single-wire management feature. VMware vSphere 5.1 is used as server virtualization architecture. FC-variant of architecture show cases Cisco Nexus 1000v based virtual switches. However, either architecture can use any of the virtual switching components.

Table 1 lists the various hardware and software components which occupies different tiers of the Cisco solution for EMC VSPEX VMware architectures under test.

Vendor	Name	Version	Description	
Cisco	Cisco UCS B200M3 servers	2.1(3a)	Cisco UCS B200M3 Blade Servers (FC-vari- ant)	
Cisco	Cisco UCS 5108 Chassis	-	Cisco UCS Blade Server Chassis	
Cisco	Cisco VIC 1240	2.1(3a)	Cisco Virtual Interface Card (adapter) firmware	
Cisco	Cisco 2204XP Fabric Extender	2.1(3a)	Cisco UCS fabric extender firmware	
Cisco	Cisco UCS 6248UP Fabric Interconnect	5.0(3)N2(2.11)	Cisco UCS fabric inter- connect firmware	
Cisco	Cisco 2232PP Fabric Extender	5.0(3)N2(2.11.2)	Cisco UCS Fabric Extender	
Cisco	Cisco UCS C220M3	1.5(2) or later – CIMC	Cisco UCS C220M3	
	Servers	C220M3.1.5.2.23 - BIOS	Rack Servers	
		Cisco C220M3 rack servers		
Cisco	Cisco UCS 1240 VIC	2.1(3a)	Cisco UCS VIC adapter (FC-variant)	

#### Table 1 Hardware and Software Components of VMware Architectures

Vendor	Name	Version	Description			
Cisco	Cisco UCS Manager	2.1(3a)	Cisco UCS Manager software			
Cisco	Cisco Nexus 5548UP Switches	5.1(3)N1(1a)	Cisco Nexus 5000 series switches running NX-OS			
Cisco	Cisco nexus 1000v	4.2(1).SV2(2.1)	Cisco Nexus 1000v Virtual Switch (NFS-variant)			
EMC	EMC VNX5400	VNX Block OE 05.33	EMC VNX storage array (FC-variant)			
EMC	EMC VNX5600	VNX File OE 8.1	EMC VNX storage			
		VNX Block OE 05.33	array (NFS-variant)			
EMC	EMC VNX5800	VNX File OE 8.1	EMC VNX storage			
		VNX Block OE 05.33	array (NFS-variant)			
EMC	EMC Avamar	6.1 SP1	EMC data backup software			
EMC	Data Domain OS	5.2	EMC data domain operating system			
VMware	ESXi 5.1	5.1 build 799733	VMware Hypervisor			
VMware	vCenter Server	5.1 build 799731	VMware management			
Microsoft	Microsoft Windows Server 2012	Windows Server 2012 Datacenter	Operating system to host vCenter server			
Microsoft	Microsoft SQL server	2008 R2	Database server SQL R2 Enterprise edition for vCenter			

#### Table 1 Hardware and Software Components of VMware Architectures

1

Table 2 outlines the B200M3 or C220M3 server configuration (per server basis) across the two variants of VMware architectures.

#### Table 2 Server Configuration Details

Component	Capacity
Memory (RAM)	128GB (8 X 16GB DIMM)
Processor	2 x Intel® Xenon ® E5-2600 V2, CPUs 2.0 GHz, 8cores, 16 threads
Local storage	Cisco UCS RAID SAS 2008M-8i Mezzanine Card, With 2 x 67 GB slots for RAID 1 configuration each

Both the variants of architecture assume that there is an existing infrastructure/ management network available where a virtual machine hosting vCenter server and Windows Active Directory/ DNS server are present.

The required number of C or B series servers and storage array type change depending on number of virtual machines. Table 3 highlights the change in hardware components, as required by different scale. Typically, 50 reference Virtual Machines are deployed per server.

Components	VMware 300 VMs	VMware 600 VMs	VMware 1000 VMs
Servers	6 x Cisco C220M3 or	12 x Cisco B200M3 or	18 x Cisco B200M3 or
	B200M3 servers	C220M3 servers	C220M3 servers
Blade Server Chassis	1 x Cisco 5108 Blade	2 x Cisco 5108 Blade	3 x Cisco 5108 Blade
	Server Chassis	Server Chassis	Server Chassis
Storage	EMC VNX5400	EMC VNX5600	EMC VNX5800

#### Table 3 Hardware Components for Different Scale

Figure 10 and Figure 11 show a high level Cisco solution for EMC VSPEX VMware FC-variant and NFS-variant architectures respectively.





I



Following are the key design points of the architectures for mid-market segment:

- For smaller scale, storage array dedicated to a given UCS domain is preferable for simplicity, so VNX5400 storage is directly attached to the Cisco UCS FIs. For larger scales, multiple UCS domains may share a storage or multiple storage arrays; In this case, storage access through Cisco Nexus 5548UP is preferable, as shown in the NFS-variant architecture.
- Infrastructure network is on a separate 1GE network.
- Network redundancy is built-in by providing two switches, two storage controllers and redundant connectivity for data, storage, and infrastructure networking.

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 network. However, design does require accessibility of certain VLANs from the infrastructure network to reach the servers.

ESXi 5.1 is used as hypervisor operating system on each server and is installed on SAN LUNs in both the architectures. However, virtual machines' storage is accessed through FC or NFS protocols depending on the architecture. Typical load is 50 reference virtual machines per server.

# **Memory Configuration Guidelines**

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

### ESX/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 over commitment, 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 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 12 shows the use of memory settings parameters in the virtual machine.



Figure 12 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 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 per-virtual machine swap file that is created on the VMware Virtual Machine File System (VMFS) 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**

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

#### Table 4 Resources for a Single Virtual Machine

Following are the 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 GB of memory may consume about 100 MB of memory overhead, where a virtual machine with two virtual CPUs and 32GB of memory may consume approximately 500 MB 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 over commitment 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 over committing. 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 ESX/ESXi if physical memory comes under contention. Performance tests show that the balloon driver allows ESX/ESXi to reclaim memory, if required, with little to no impact to performance. Disabling the balloon driver forces ESX/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 the services have the resources they require while still allowing high consolidation of other virtual machines.

# **Storage Guidelines**

VSPEX architecture for VMware VMs for mid-market segment uses FC or NFS to access storage arrays. FC is used with smaller scale with VNX5400 storage array, while NFS is used with VNX5600 or VNX5800 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 VNX 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 VSPEX solution on vSphere NFS is a recommended option because of its simplicity in deployment.

For more information, see the VMware white paper Comparison of Storage Protocol Performance in VMware vSphere 5: http://www.vmware.com/files/pdf/perf\_vsphere\_storage\_protocols.pdf

### **Storage Best Practices**

Following are the 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. In this solution, the redundancy is comes from the "Fabric Failover" feature of the dynamic vNICs of Cisco UCS for NFS storage access.
- 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 NFS level as well as within the guest operating system. Use the vSphere Client when creating NFS datastores to be sure they are created aligned. When formatting volumes within the guest, Windows 2012 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 multi-tier application, you can expect each tier of application to have different I/O requirements. As a general recommendation, pay close attention to the amount of virtual machine disk files hosted on a single NFS volume. Over-subscription of the I/O resources can go unnoticed at first and slowly begin to degrade performance if not monitored proactively.

# **VSPEX VMware Memory Virtualization**

VMware vSphere 5.1 has a number of advanced features that help to maximize performance and overall resources utilization. This section describes the performance benefits of some of these features for the VSPEX deployment.

# **Memory Compression**

Memory over-commitment occurs when more memory is allocated to virtual machines than is physically present in a VMware ESXi host. Using sophisticated techniques, such as ballooning and transparent page sharing, ESXi is able to handle memory over-commitment without any performance degradation. However, if more memory than that is present on the server is being actively used, ESXi might resort to swapping out portions of a VM's memory.

For more details about Vsphere memory management concepts, see the VMware Vsphere Resource Management Guide at: http://www.VMware.com/files/pdf/mem\_mgmt\_perf\_Vsphere5.pdf

#### Virtual Networking

NFS-variant architecture demonstrates use and benefits of Nexus 1000v virtual switching technology. Each B200 M3 blade server and C220 M3 rack server has one physical adapter with two 10 GE links going to fabric A and fabric B for high availability. Cisco UCS VIC 1225 or 1240 presents four virtual Network Interface Cards (vNICs) to the hypervisor, two vNICs per fabric path. In FC-variant, the Cisco UCS VIC 1225 adapter also presents two virtual Host Bus Adapters (vHBAs) to the hypervisor, one per fabric path. The MAC addresses to these vNICs are assigned using MAC address pool defined on the UCS Manager. 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, switch (FI or FEX) failures, and in case of UCS, upstream switch failure (due to "End-Host-Mode" architecture).
- Enable PortFast on ESX/ESXi host uplinks—Failover events can cause spanning tree protocol recalculations that can set switch ports into a forwarding or blocked state to prevent a network loop. This process can cause temporary network disconnects. Cisco UCS Fabric Extenders are not really Ethernet switches, they are line cards to the Fabric Interconnect, and Cisco UCS Fabric Interconnects run in end-host-mode and avoid running Spanning Tree Protocol. Given this, there is no need to enable port-fast on the ESXi host uplinks. However, it is recommended that you enable

portfast on Cisco Nexus 5548UP switches or infrastructure switches that connect to Cisco UCS Fabric Interconnect uplinks for faster convergence of STP in the events of FI reboot or FI uplink flap.

• Jumbo MTU for vMotion and storage traffic—This practice is implemented in the architecture by configuring jumbo MTU end-to-end.

# **VSPEX VMware Storage Virtualization**

Disk provisioning on the EMC VNX series requires administrators to choose disks for each of the storage pools.

# **Storage Layout**

The architecture diagram in this section shows the physical disk layout. Disk provisioning on the VNX 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 13 shows storage architecture for 300 virtual machines on VNX5400 for FC-variant of architecture.



Figure 13 Storage Architecture for 300 VMs on EMC VNX5400

Figure 14 shows storage architecture for 600 virtual machines on VNX5600 for NFS-variant of architecture.



Figure 14 Storage Architecture for 600 VMs on EMC VNX5600

I

1

Figure 15 shows storage architecture for 1000 virtual machines on VNX5800 for NFS-variant of architecture.





Γ

Table provides the data stores size for various architectures shown in Figure 13, Figure 14, and Figure 15.

Parameter	300 VMs	600 VMs	1000 VMs
Storage Array	VNX5400	VNX5600	VNX5800
Disk capacity and type	600 GB SAS	600 GB SAS	600 GB SAS
Number of disks	110	220	360
RAID type	RAID 5 groups	RAID 5 groups	RAID 5 groups
Fast VP Config	6 x 200 GB Flash Drives	10 x 200 GB Flash Drives	16 x 200 GB Flash Drives
Hot spares	4 x 600 GB SAS	8 x 600 GB SAS	12 x 600 GB SAS
	1 x 200 GB Flash	1 x 200 GB Flash	1 x 200 GB Flash

#### Table 5 Datastores for Different Scale

The VNX family storage array 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**

NFS is a cluster file system that provides UDP based stateless storage protocol to access storage across multiple hosts over the network. Each virtual machine is encapsulated in a small set of files and NFS datastore mount points are used for the operating system partitioning and data partitioning.

It is preferable to deploy virtual machine files on shared storage to take advantage of VMware VMotion, VMware High Availability<sup>TM</sup> (HA), and VMware Distributed Resource Scheduler<sup>TM</sup> (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 (FC-variant)

All of these identifiers are defined in their respective identifier pools and the pool names are referred in the service profile template.

I

• Local disks are NOT used for booting. Boot policy in service profile template suggests host to boot from the storage devices using FC protocol for both architectures.

- Server pool is defined with automatic qualification policy and criteria. Rack servers are automatically put in the pool as and when they are fully discovered by UCS Manager. 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 UCS Manager, 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 and connect it to the Fabric Extenders. Let the new server be discovered by UCS Manager.
- Associate the service profile to the newly deployed rack 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 and rack servers can be added in the same server pool.

# **Network Availability Design - FC-Variant**

Figure 16 shows the logical layout of FC-variant architecture. The following are the key aspects of this solution:

- Mix of Cisco UCS B200 M3 and C220 M3 servers are used, managed by UCS Manager.
- Fabric A and Fabric B are used with host based FC multi-pathing for high availability
- EMC VNX5400 storage array is directly attached to UCS Fabric Interconnects
- Two 10GE links between FI and FEX provides enough bandwidth oversubscription for the SMB segment private cloud. The oversubscription can be reduced by adding more 10GE links between FI and FEX if needed by the VMs running on the ESXi hosts.
- Two vSwitches are used per host, as discussed in the Virtual Networking design section.

Storage is made highly available by deploying following practices:

- VNX storage arrays provide two Storage Processors (SPs): SP-A and SP-B
- Fabric Interconnects A and B are connected to each SP-A and SP-B.
- Port-channels or port-aggregation is not implemented or required in this architecture.
- Storage Processors are always in the active/active mode; if the target cannot be reached on SAN-A, server can access the LUNs through SAN-B and storage-processor inter-link.
- On hosts, boot order lists vHBA on both fabrics for high-availability.



#### Figure 16 Logical Layout of FC-Variant Architecture

# **Network Availability Design - NFS-Variant**

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

- Mix of Cisco UCS B200 M3 and C220 M3 servers are used, managed by UCS Manager
- · Cisco Nexus 1000v distributed virtual switch is used for virtual switching
- vNICs on fabric A and fabric B are used for NFS based access high-availability
- vPC is used between Nexus 5548UP and UCS FIs for high availability
- vPC and port-aggregation is used between Nexus 5548UP and VNX storage for high availability
- Two 10GE links between FI and FEX provides enough bandwidth oversubscription for the private cloud. The oversubscription can be reduced by adding more 10GE links between FI and FEX if needed by the VMs running on the ESXi hosts.

Storage is made highly available by deploying following practices:

• FC access for booting the hypervisor images in the NFS-variant of architecture is exactly same as the FC-variant. Only difference is – the VMs are stored on the NFS mount servers in the NFS-variant of architecture.

- VNX storage arrays provide two Storage Processors (SPs): SP-A and SP-B for FC and two Data Movers (DMs): DM-2 and DM-3 for NFS.
- Both Nexus 5548UP switches (A and B) are connected to both Storage Processors (over FC) and Data Movers (over Ethernet), however, a given FI connects to the same port on each SP. FI-A connects to "eth10" port of SP-A and SP-B, while FI-B connects to "eth11" port of SP-A and SP-B.
- vPC on Nexus 5548UP switches and port-aggregation on VNX storage arrays for high availability of NFS servers
- Data Movers are always in the active/stand-by mode; the L2 links are up on both DMs, LACP would be down on the stand-by DM.
- If a single link on port-channel fails, the other link would bear all the load. If the whole Data Mover fails, then the standby DM takes over the role of active DM.

Nexus 1000v VEM Nexus 10000 VEM VMware vSphere VMware vSphere ESXi5.5 Cluster Cisco UCS 5108 Chassis Cisco UCS 5108 Chassis Cisco UCS 6248 UF Cisco UCS 6248 UP N1K VSM Nexus 5548 UP - FabA Nexus 5548 UP – FabB Infra Network Virtual Ce 1 GE (Infra) 10 GE (Trunk, FCoE1 8 GE (FC) · · · · · · EMC VNX DM-2 EMC VNX DM-3 EMC VNX SP-B EMC VNX SP-A 10 GE Ethernet

Figure 17 Logical Layout of NFS-Variant Architecture

I

# 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 the end-points where the jumbo MTU needs to be configured:

- 1. Ethernet ports on VNX Storage Processors
- 2. System QoS classes in Nexus 5548UP switches
- 3. System QoS classes in UCS Manager
- 4. vNICS in service profiles
- 5. Nexus 1000v switch or vSwitches on the ESXi hosts
- 6. VM-Kernel ports used for vMotion and storage access on the ESXi hosts

# Sizing Guidelines

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

#### **Defining the Reference Workload**

To simplify the discussion, 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 characteristics shown in Table 4.

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

### Applying the Reference Workload

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

The reference architectures create a pool of resources sufficient to host a target number of reference virtual machines as described above. It is entirely possible that customer virtual machines may not exactly match the specifications above. In that case, you can say that a single specific customer virtual machine is the equivalent of some number of reference virtual machines, and assume that number of virtual machines have been used in the pool. You can continue to provision virtual machines from the pool of resources until it is exhausted. Consider these examples:

I

#### Example 1 Custom Built Application

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

Based on these numbers, following resources are needed from the resource pool:

- CPU resources for one VM
- Memory resources for two VMs
- Storage capacity for one  ${\tt V\!M}$
- IOPS for one VM

In this example, a single virtual machine uses the resources of two of the reference VMs. Once this VM is deployed, the solution's new capability would be 298 VMs.

#### Example 2 Point of Sale System

The database server for a customer's point-of-sale system needs to move into this virtual infrastructure. It is currently running on a physical system with four CPUs and 16GB of memory. It uses 200GB storage and generates 200 IOPS during an average busy cycle. The following resources that are needed from the resource pool to virtualize this application:

- CPUs of four reference VMs
- Memory of eight reference VMs
- Storage of two reference VMs
- IOPS of eight reference VMs

In this case the one virtual machine uses the resources of eight reference virtual machines. Once this VM is deployed, the solution's new capability would be 292 VMs.

#### Example 3 Web Server

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

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

- CPUs of two reference VMs
- Memory of four reference VMs
- Storage of one reference VMs
- IOPS of two reference VMs

In this case the virtual machine would use the resources of four reference virtual machines. Once this VM is deployed, the solution's new capability would be 296 VMs.

#### Example 4 Decision Support Database

The database server for a customer's decision support system needs to move into this virtual infrastructure. It is currently running on a physical system with 10 CPUs and 48GB of memory. It uses 5TB of storage and generates 700 IOPS during an average busy cycle. The following resources that are needed from the resource pool to virtualize this application:

- CPUs of ten reference VMs
- Memory of 24 reference VMs
- Storage of 52 reference VMs
- IOPS of 28 reference VMs

In this case the one virtual machine uses the resources of 52 reference virtual machines. If this was implemented on a resource pool for 300 virtual machines, there are 248 virtual machines of capability remaining in the pool.

# **Summary of Example**

The four examples show the flexibility of the resource pool model. In all the four cases the workloads simply reduce the number of available resources in the pool. If all four examples were implemented on the same virtual infrastructure, with an initial capacity of 300 virtual machines they can all be implemented, leaving the capacity of 236 reference virtual machines in the resource pool.

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

# VSPEX Configuration Guidelines

This sections provides the procedure to deploy the Cisco solution for EMC VSPEX VMware architecture.

Follow these steps to configure the Cisco solution for EMC VSPEX VMware architectures:

- 1. Pre-deployment tasks
- 2. Connect network cables
- 3. Configure Cisco Nexus 5548UP switches (NFS-variant only)
- 4. Prepare Cisco UCS FIs and configure Cisco UCS using UCS Manager
- 5. Configure data stores for ESXi images
- 6. Install VMware ESXi servers and vCenter infrastructure.
- 7. Install and configure vCenter server
- 8. Install Cisco Nexus 1000v VMS VM (NFS-variant only)
- 9. Configure storage for VM data stores, install and instantiate VMs through vCenter
- **10.** Test the installation

These steps are described in detail in the following sections.

# **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 Sheet, page 200 for reference during the deployment process.

Requirement	Description	Reference
Hardware	Cisco UCS B200M3 or C220M3 servers to host virtual machines	See the corresponding product documentation
	Cisco UCS 5108 Blade Server Chassis	-
	Cisco Nexus 2232PP Fabric Extender	-
	Cisco UCS 6248UP Fabric Inter- connect	
	VMware vSphere <sup>™</sup> 5.1 server to host virtual infrastructure servers	
	<b>Note</b> This requirement may be covered in the existing infrastructure	
	Cisco Nexus switches: Two Cisco Nexus 5548UP Switches for high availability	-
	EMC VNX storage: Multiproto- col storage array with the required disk layout as per archi- tecture requirements	

### Table 6 Customer Specific Configuration Data

Γ

Requirement	Description	Reference	
Software	Cisco Nexus 1000v VSM and VEM installation media	See the corresponding product documentation	
	VMware ESXi <sup>TM</sup> 5.1 installation media		
	VMware vCenter Server 5.1 in- stallation media		
	EMC VSI for VMware vSphere: Unified Storage Management – Product Guide		
	EMC VSI for VMware vSphere: Storage Viewer—Product Guide		
	Microsoft Windows Server 2012 installation media (suggested OS for VMware vCenter)		
	Microsoft SQL Server 2008 R2 SP1		
	<b>Note</b> This requirement may be covered in the existing infrastructure		
Licenses	VMware vCenter 5.1 license key	Consult your corre-	
	VMware ESXi 5.1 license keys	sponding vendor obtain license keys	
	Microsoft SQL Server license key		
	<b>Note</b> This requirement may be covered in the existing infrastructure		

1

Table 6 Customer Specific Configuration Data

# **Customer Configuration Data**

To reduce the onsite time, information such as IP addresses and hostnames should be assembled as part of the planning process.

The section Customer Configuration Data Sheet, page 200 provides tabulated record of relevant information (to be filled at the customer's end). This form can be expanded or contracted as required, and information may be added, modified, and recorded as the deployment progresses.

Additionally, complete the VNX Series Configuration Worksheet, available on the EMC online support website, to provide the most comprehensive array-specific information.

# **Connect Network Cables**

See the Cisco Nexus 5548UP, UCS FI, FEX, Blade server chassis, B-series and C-series server and EMC VNX 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.

# **Connectivity for FC-Variant:**

ſ

As shown in the following figure, there are four major cabling sections in this architecture:

- Cisco UCS Fabric Interconnects to EMX storage array Fibre Channel links (shown in yellow)
- Cisco Fabric Interconnects to Cisco UCS Fabric Extenders links (shown in blue)
- Cisco UCS Fabric Extenders to Cisco UCS C220 M3 Server links (shown in green)
- Infrastructure connectivity (not shown)

Figure 18

Detailed Connectivity Diagram of the FC-Variant Architecture



Figure 19 elaborates the detailed cable connectivity for the architecture.

Cable		Peer2			
ID	Peer1		VLAN	Mode	Description
A	FI-A, FC	SP-A,	Storage		
	2/9		VSAN	Applianœ	Directly attached storage on FI
В	FI-A, FC	SP-B,	Storage		
	2/10		VSAN	Appliance	Directly attached storage on FI
С	FI-B, FC	SP-B,	Storage		
	2/9		VSAN	Appliance	Directly attached storage on FI
D	FI-B, FC	Sp-A,	Storage		
	2/10		VSAN	Applianœ	Directly attached storage on FI
E, F	FI-A, Eth	FEX-A			FI/FEX20GE port-channel
	1/1, 1/2	uplinks	N/A	Server	connectivity
G,H	FI-A, Eth	FEX-B			FI/FEX20GE port-channel
	1/1, 1/2	uplinks	N/A	Server	connectivity
1		C220-			
	FEX-A,	M3 VIC		VNTag	Servertofabric A. VLANs are
	port 1	port 1	N/A	(internal)	allowed on per vNIC basis
J		C220-			
	FEX-B,	M3 VIC		VNTag	Servertofabric B. VLANs are
	port 1	port 2	N/A	(internal)	allowed on per vNIC basis
K,L	FI-A, Eth	5108			FI/FEX20GE port-channel
	1/3, 1/4	Chassis,	N/A	Server	connectivity
		FEX			
		2208			
		Left			
M,N		5108			
		Chassis,			
		FEX			FL/FFX202F and share 1
	FI-B, Eth	2208	01/0	Common	FI/FEX20GE port-channel
(not	1/3, 1/4	Right	N/A	Server	connectivity
(not	Eth 2/1,	Uplink switch			
shown)	2/2 on	switch			
	FI-Aand			Lindinda	Uplink to Infrastructure
	FI-B		All	Uplink	network

# Figure 19 Connectivity Details of FC-Variant Architecture

1

# **Connectivity for NFS-Variant**

As shown in the following figure, there are four major cabling sections in this architecture:

- Cisco UCS Fabric Interconnects to EMC storage array 10G Ethernet links (shown in yellow)
- Cisco UCS Fabric Interconnects to Cisco UCS Fabric Extenders links (shown in blue)
- Cisco UCS Fabric Extenders to Cisco UCS C220 M3 Server links (shown in green)
- Infrastructure connectivity (not shown)



Figure 20 Detailed Connectivity Diagram of the NFS-Variant Architecture

Figure 21 elaborates the detailed cable connectivity for the architecture.

Γ

Cable		Peer2					
ID	Peer1		VLAN	Mode	Description		
A	FI-A, Eth	DM-2,		Access			
	1/5	A1/0	Storage	(on N5k)	N5k to storage Data Mover		
В	FI-A, Eth	DM-3,		Access			
	1/6	B1/0	Storage	(on N5k)	N5k to storage Data Mover		
С	FI-B, Eth	DM-2,		Access			
	1/5	A1/1	Storage	(on N5k)	N5k to storage Data Mover		
D	FI-B, Eth	DM-3,		Access			
	1/6	B1/1	Storage	(on N5k)	N5k to storage Data Mover		
E,F	Eth 1/15,	Eth 1/15,					
	Eth 1/16	Eth 1/16					
	on N5k-A	on N5k-B	All	Trunk	vPCpeer-links between N5ks		
G	N5k-A,	FI-A, Eth			N5k vPCmember port, FLPC		
	Eth 1/3	1/13			memberport		
Н	N5k-A,	FI-B, Eth			N5k vPCmember port, FLPC		
	Eth 1/4	1/13	All	Trunk	memberport		
1	N5k-B, Eth 1/3	FI-A, Eth	All	Trunk	N5k vPCmember port, FI PC member port		
	-	1/14					
J	N5k-B,	FI-B, Eth			N5k vPCmember port, FI PC		
	Eth 1/4	1/14	All	Trunk	memberport		
K,L	FI-A, Eth	FEX-A		Server			
	1/1, 1/2	uplinks	N/A	(on FI)	FL/IOM links		
M,N	FI-B, Eth	FEX-B		Server			
	1/1, 1/2	uplinks	N/A	(on FI)	FI/IOM links		

Figure 21 Ethernet Cable Connectivity Details of NFS-Variant Architecture

1

# Figure 22 FC Cable Connectivity Details for NFS-Variant Architecture

Cable		Peer2		
ID	Peer1		VSAN	Description
0	N5k-A,	SP-A,	Storage	
	FC 1/31	0/0	VSAN	N5k to storage SP, crisscrossed
Р	N5k-A,	SP-B,	Storage	
	FC 1/32	0/0	VSAN	N5k to storage SP, crisscrossed
Q	N5k-B,	SP-A,	Storage	
	FC 1/31	0/1	VSAN	N5k to storage SP, crisscrossed
R	N5k-B,	SP-A,	Storage	
	FC 1/32	0/1	VSAN	N5k to storage SP, crisscrossed
S	N5k-A,	FI-A,	Storage	
	FC1/29	FC1/29	VSAN	N5k to FI straight cables
Т	N5k-A,	FI-A,	Storage	N5k to FI straight cables
	FC1/30	FC1/30	VSAN	
U	N5k-B,	FI-B,	Storage	N5k to FI straight cables
	FC1/29	FC1/29	VSAN	
$\vee$	N5k-B,	FI-B,	Storage	
	FC1/30	FC1/30	VSAN	N5k to FI straight cables

By connecting all the cables as outlined above, and you would be ready to configure Cisco Nexus 5548UP Switch, EMC VNX Series Storage Array and Cisco UCS Managaer.

# **Configuring Cisco Nexus Switches**

This section explains switch configuration needed for the Cisco solution for EMC VSPEX VMware architectures. For information on configuring password, and management connectivity, see *Cisco Nexus* 5000 Series Configuration Guide.

### **Configure Global VLANs and VSANs**

Figure 23 shows how to configure VLAN on a switch.

Figure 23	Creating	VL	AN
i igaio Eo	orouting		

```
UCS-N5k-Fabl# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UCS-N5k-Fabl(config)# vlan 40
UCS-N5k-Fabl(config-vlan)# name Storage
UCS-N5k-Fabl(config-vlan)# exit
UCS-N5k-Fabl(config)# exit
UCS-N5k-Fabl#__
```

Following VLANs in Table 7 need to be configured on both switches A and B in addition to your application specific VLANs:

VLAN Name	Description		
Storage	VLAN to access storage array from the servers over NFS		
vMotion	VLAN for virtual machine vMotion		
Infra	Management VLAN for vSphere servers to reach vCenter management plane		
VM-Data	VLAN for the virtual machine (applica- tion) traffic (can be multiple VLANs)		

Table 7 Configured VLANS on Switch A and B

For actual VLAN IDs of your deployment, see Customer Configuration Data Sheet, page 200. We have used one VSAN in this solution. Table 8 gives the VSAN name and the description.

Table 8 Configured VSAN To Access Storage Array

VSAN Name	Description
Storage	VSAN to access storage array from the servers over fibre channel

For actual VSAN ID of your deployment, see Customer Configuration Data Sheet, page 200. Figure 24 and Figure 25 show the creation of VSAN and assigning VSAN to the fibre channel interface.

Figure 24 Creating VSAN	
	U.
UCS-N5k-FabA# configure terminal	н.
Enter configuration commands, one per line. End with CNTL/2.	I.
UCS-N5k-FabA(config)# vsan database	I.
UCS-N5k-Fabl(config-vsan-db)# vsan 10	I.
UCS-N5k-FabA(config-vsan-db)# vsan 10 interface fc 1/29	I.
UCS-N5k-FabA(config-vsan-db)# vsan 10 interface fc 1/30	1
UCS-N5k-FabA(config-vsan-db)# vsan 10 interface fc 1/31	
UCS-N5k-FabA(config-vsan-db)# vsan 10 interface fc 1/32	
UCS-N5k-Fabl(config-vsan-db)# end	
UCS-N5k-Fabl#	

After creating the VSAN. VSAN membership is assigned, and the peer interfaces on the links need to be configured properly, a healthy fibre channel port is shown in Figure 25.

1

UCS-N5k-Fa vsan 1 int fc1/27	erfaces			ip						
vsan 10 in fc1/29		s: fc	1/30		fc1/31		fc1	/32		
vsan 4079(	evfp_is	olated_	vsan) in	terface	s:					
vsan 4094(	isolate	d_vsan)	interfa	ices:						
UCS-N5k-Fa	bl# sho	w inter	face fc1	./29-32	brief					
Interface	Vsan		Admin Trunk Mode	Status		SFP		Oper Speed (Gbps)	Port Channel	-
fc1/29	10	 F	 on	up		 ຣພl	 F	8		
fc1/30	10	F	on	up		swl	F	8		=
fc1/31	10	F	on	up		swl	F	8		
	10	F	on	up		swl	F	8		
UCS-N5k-Fa	bA#									-

Figure 25 Assigned VSAN Membership

~ 4

It is also crucial to enable NPIV feature on the Cisco Nexus 5548UP switches. Figure 26 show how to enable NPIV feature on Nexus 5548UP switches.

#### Figure 26 Enabling Npiv Feature On Cisco Nexus Switches

UCS-N5k-Fabl# configure terminal	-
Enter configuration commands, one per line. End with CNTL/2.	-
UCS-N5k-Fabl(config)# feature npiv	
UCS-N5k-Fabl(config)#	

#### **Configuring Virtual Port Channel (vPC)**

Virtual port-channel effectively enables two physical switches to behave like a single virtual switch, and port-channel can be formed across the two physical switches. Following are the steps to enable vPC:

- 1. Enable LACP feature on both switches.
- 2. Enable vPC feature on both switches.
- 3. Configure a unique vPC domain ID, identical on both switches.
- 4. Configure mutual management IP addresses on both the switches and configure peer-gateway as shown in Figure 27.

# Figure 27 Configuring Peer-Gateway



5. Configure port-channel on the inter-switch links. Configuration for these ports is shown in Figure 28. Ensure that "vpc peer-link" is configured on this port-channel.

#### Figure 28 Configured VPC Peer-link on Port-Channel



- **6.** Add ports with LACP protocol on the port-channel using "channel-group 1 mode active" command under the interface sub-command.
- 7. Verify vPC status using show vPC command. Successful vPC configuration is shown in Figure 29.



Figure 29 Window Showing Successful vPC Configuration

#### **Configuring Port-Channels Connected to Cisco UCS Fabric Interconnects**

Interfaces connected to the fabric interconnects need to be in the trunk mode. Storage, vMotion, infra, and application VLANs are allowed on this port. From the switch side, interfaces connected to Cisco UCS FI-A and Cisco UCS FI-B are in a vPC, and from the FI side the links connected to Cisco Nexus 5548UP A and B switches are in LACP port-channels. Ensure that you give a right description for each port and port-channel on the switch for better diagnosis in case of any problem. Figure 30 shows the configuration commands.

I

- 0 - X 🗗 10.29.180.3 - PuTTY UCS-N5k-Fabl# show running-config interface port-channel 18-19 Command: show running-config interface port-channel18-19 Time: Thu Aug 30 11:26:00 2012 ersion 5.0(3)N1(1b) interface port-channel18 description to FI-A switchport mode trunk vpc 18 switchport trunk allowed vlan 1,40-41,45 interface port-channel19 description to FI-B switchport mode trunk vpc 19 switchport trunk allowed vlan 1,40-41,45 UCS-N5k-Fabl# show running-config interface ethernet 1/18-19 Command: show running-config interface Ethernet1/18-19 Time: Thu Aug 30 11:26:15 2012 version 5.0(3)N1(1b) interface Ethernet1/18 description vpc port-channel switchport mode trunk switchport trunk allowed vlan 1,40-41,45 channel-group 18 mode active interface Ethernet1/19 description vpc port-channel switchport mode trunk switchport trunk allowed vlan 1,40-41,45 channel-group 19 mode active ICS-N5k-FabA#

#### Figure 30 Port-channel Configuration

#### **Configuring Storage Connectivity**

From each switch one link connects to each storage processor on the VNX storage array. A virtual port-channel is created for the two links connected to a single storage processor, but connected to two different switches. In this example configuration, links connected to the storage processor A (SP-A) of VNX storage array are connected to Ethernet port 1/26 on both the switches and links connected to the storage processor B (SP-B) are connected to Ethernet port 1/25 on both the switches. A virtual port-channel (id 26) is created for the Ethernet port 1/26 on both the switches and another virtual port-channel (id 25) is created for the Ethernet port 1/25 on both the switches.



The ports are in the access mode since only storage VLAN is required on these ports.

Figure 31 shows the configuration on the port-channels and interfaces.

ළු 10.6.116.40 - PuTTY	- • ×
<pre>!Command: show running-config interface port-channel25-26 !Time: Tue Sep 3 18:48:35 2013</pre>	۸ ۱
version 5.0(3)N2(1)	
interface port-channel25 description to VNX5600-DM2 untagged cos 5 vpc 25 switchport access vlan 40	
interface port-channel26 description to VNX5600-DM3 untagged cos 5 vpc 26 switchport access vlan 40	
l4al2-nexus5k-2(config-if)# show running-config interface ethernet 1/5-6	
Command: show running-config interface Ethernet1/5-6 Time: Tue Sep 3 18:48:40 2013	
version 5.0(3)N2(1)	
interface Ethernet1/5 description to VNX5600-DM2-1 switchport access vlan 40 channel-group 25 mode active	
interface Ethernet1/6 description to VNX5600-DM3-1 switchport access vlan 40 channel-group 26 mode active	E
14a12-nexus5k-2(config-if)#	

#### Figure 31 Configuration of Port-channel and Interfaces

#### **Configuring Ports Connected To Infrastructure Network**

Port connected to infrastructure network need to be in trunk mode, and they require at least infrastructure VLAN, N1k control and packet VLANs at the minimum. You may require enabling more VLANs as required by your application domain. For example, Windows virtual machines may need to access to active directory / DNS servers deployed in the infrastructure network. You may also want to enable port-channels and virtual port-channels for high availability of infrastructure network.

#### **Verify VLAN and Port-channel Configuration**

At this point of time, all ports and port-channels are configured with necessary VLANs, switchport mode and vPC configuration. Validate this configuration using the "show vlan", "show port-channel summary" and "show vpc" commands as shown in Figure 32.

1



The ports will be "up" only after the peer devices are configured properly, so you should revisit this subsection after configuring the EMC VNX storage array and Cisco UCS fabric interconnects.

UCS-N5k-FabA# show	vlan id 40-45		
VLAN Name		Status	Ports
40 Storage 41 vMotion 45 VM-DATA VLAN Name  Remote SPAN VLANs		active active active Status	Pol, Pol8, Pol9, Po25, Po26 Pol, Pol8, Po19 Pol, Po18, Po19 Ports
Primary Secondary  UCS-N5k-FabA# _	Туре 	Ports	

Figure 32 Validating Created Port-Channels with VLANs

**show vlan** command can be restricted to a given VLAN or set of VLANs as shown in Figure 32. Ensure that on both switches, all required VLANs are in "active" status and right set of ports and port-channels are part of the necessary VLANs.

Port-channel configuration can be verified using "show port-channel summary" command. Figure 33 shows the expected output of this command.

UCS-N Flags	I - Indi s - Susp S - Swit	P Vidual H	- Up in po - Hot-stan - Module-r - Routed	rt-channel (me dby (LACP only	
Group	Port- Channel	Туре	Protocol	Member Ports	
1 18 19	Po1 (SU) Po18 (SU) Po19 (SU)	Eth Eth Eth	LACP LACP LACP LACP	Eth1/1(P) Eth1/18(P) Eth1/19(P)	Eth1/2(P)
25 26	Po25(SD) Po26(SU) (Sk-Fabl#	Eth Eth	LACP LACP	Eth1/25(P) Eth1/26(P)	

#### Figure 33 Verifying Port-Channel Configuration

In this example, port-channel 1 is the vPC peer-link port-channel, port-channels 25 and 26 are connected to the storage arrays and port-channels 18 and 19 are connected to the Cisco UCS FI A and B. Make sure that the state of the member ports of each port-channel is "P" (Up in port-channel).



The port may not show "up" if the peer ports are not configured properly.

Common reasons for port-channel port being down are:

• Port-channel protocol mis-match across the peers (LACP v/s none)

Inconsistencies across two vPC peer switches. Use "show vpc consistency-parameters {global | interface {port-channel | port} <id> command to diagnose such inconsistencies.

vPC status can be verified using "show vpc" command. Example output is shown in Figure 34.



UCS-N5k-Fabl# show vpc	
Legend:	
(*) - local vPC is down, forwarding via vPC peer-lin	nk
, , arran in an array are and y has no part an	
vPC domain id : 101	
Peer status : peer adjacency formed ok	
vPC keep-alive status : peer is alive	
Configuration consistency status: success	
Per-vlan consistency status : success	
Type-2 consistency status : success	
vPC role : primary, operational secondary	
Number of vPCs configured : 4	
Peer Gateway : Enabled	
Dual-active excluded VL&Ns : -	
Graceful Consistency Check : Enabled	
vPC Peer-link status	
id Port Status Active vlans	
1 Pol up 1,40-41	
vPC status	
id Port Status Consistency Reason Act	tive vlans
18 Po18 up success success 1,4	40-41
19 Po19 up success success 1,4	40-41
25 Po25 up success success 40	
26 Po26 down* success success -	
UCS-N5k-Fabl#	

Ensure that the vPC peer status is "peer adjacency formed ok" and all the port-channels, including the peer-link port-channel status are "up", except one of the two port-channels connected to the storage array as explained before.

# **Configuring QoS**

The Cisco solution for the EMC VSPEX VMware architectures require MTU to be set at 9216 (jumbo frames) for efficient storage and vMotion traffic. MTU configuration on Cisco Nexus 5000 fall under global QoS configuration. You may need to configure additional QoS parameters as needed by the applications. For more information on the QoS configuration, see *Cisco Nexus 5000 Series Configuration Guide*.

To configure jumbo MTU on the Cisco Nexus 5000 series switches, follow these steps on both switch A and B:

I

- 1. Create a policy map named "jumbo-mtu".
- 2. As we are not creating any specific QoS classification, set 9216 MTU on the default class.

- **3.** Configure the system level service policy to the "jumbo-mtu" under the global "system qos" sub-command.
- **4.** NFS traffic flowing from storage array to fabric interconnect need to be marked with Ethernet Class of Service (CoS) 5 for proper classification at the fabric interconnect. Use the "untagged cos 5" command at the port-channels connected to the storage arrays.

Figure 35 shows the exact Cisco Nexus CLI for the steps mentioned above.

Figure 35 Configuring MTU on Cisco Nexus Switches





Figure 35 shows the NX-OS interface range CLI to configure multiple interfaces at the same time.

# Prepare UCS FIs and configure UCS Manager

Configure UCS FIs and UCS Manager can be subdivided in to following segments:

- 1. Initial Configuration of Cisco UCS FIs, page 51
- 2. Configuration for Server Discovery, page 53
- 3. Upstream/ Global Network Configuration, page 58
- 4. Configure Identifier Pools, page 78
- 5. Configure Server Pool and Qualifying Policy, page 85
- 6. Configure Service Profile Template, page 91
- 7. Instantiate Service Profiles from the Service Profile Template, page 108

Following subsections provided details on each of the steps mentioned above.

# Initial Configuration of Cisco UCS Fls

At this point of time, the Cisco UCS FIs, FEX, and Blade Servers or Rack Servers must be mounted on the rack and appropriate cables must be connected. 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 the power supplies 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.

To perform initial FI configuration, follow these steps:

 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 UCS Manager Virtual IP address), as the initial configuration script walks you through the configuration. Save the configuration, which will take you to UCS Manager CLI login prompt.

#### Figure 36 Initial Configurations of Cisco UCS Fabric Interconnect

🗜 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 $(\lambda/B)$ []: $\lambda$
Enter the system name: VSPEX-FI
Physical Switch Mgmt0 IPv4 address : 10.65.121.226
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.65.121.1
Cluster IPv4 address : 10.65.121.228
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=VSFEX-FI Enforced Strong Password=yes Physical Switch Mgmt0 IP Address=10.65.121.226 Physical Switch Mgmt0 IP Netmask=255.255.255.0 Default Gateway=10.65.121.1
Cluster Enabled=yes Cluster IP Address=10.65.121.228 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 will prompt to just join the cluster. Only information you need to provide is the FI specific management IP address, subnet mask and default gateway. Save the configuration.

1



3. Once initial configurations on both FIs are completed, you can disconnect the serial console cable. Now, UCS Manager will be accessible through web interface (https://<ucsm-virtual-ip>/) or SSH. Connect to UCS Manager using SSH, and see HA status. As there is common device connected between two FIs (a rack server or blade server chassis), the status shows as "HA NOT READY", but you must see both FI A and FI B in "Up" state as shown Figure 38.





# **Configuration for Server Discovery**

All the Ethernet ports of FIs are unconfigured and shutdown by default. You need to classify these ports as server facing ports, directly attached storage array facing ports, and uplink ports.

To configure the ports for proper server auto-discovery, follow these steps:

To configure chassis discovery policy that specifies server side connectivity, using a web browser, access the UCS Manager from the management virtual IP address and download the Java applet to launch UCS Manager GUI. Click Equipment tab in the left pane, and then Policies tab in the right pane. In Chassis Discovery Policy, For Actions field choose 2 Link. Two links represent the two 10 GE links that are connected between FI and FEX per fabric. Also, change Link Grouping Preference to Port Channel for better bandwidth utilization and link level high-availability as shown in Figure 39. Save the changes.

	G     Image: New →     Pending Activities     Image: Description       >>     B     Equipment	cisi Equipmen
Equipment Servers LAN SAN VM Admin Filter: All	Main Topology View Fabric Interconnects Thermal Decommissioned Firmware Management Global Policies Autoconfig Policies Server Inheritance Policies Blade Server Discovery Policies SEL Policy Chassis Discovery Policy Action: 2 Link Link Grouping Preference: None  Port Channel Rack Server Discovery Policy Action: Immediate User Acknowledged Scrub Policy: not set> Power Policy Redundancy: Non Redundant  +1 Grid MAC Address Table Aging Aging Time: Never  Mode Default other Global Power Allocation Policy Save Changes	

Figure 39 Configuring Chassis Discovery Policy

Next, identify ports connected to the Chassis or FEX per FI basis. Click the Equipment tab, expand Fabric Interconnects, choose an FI, for example, Fabric Interconnect A, click Unconfigured Ethernet Ports, and select the two ports connected to the FEX-A. Right-click, and choose Configure as Server Port. Click Yes on the confirmation pop-up window.

1

#### Figure 40 Configuring Ethernet Ports as Server Ports

ault Summary 0 6 8 0	>> 📸 Equ	ipment 🕨 💷 Fabric	is   😧 🕕   📥 Per			III Fixed Module >		
uipment Servers LAN SAN VM Admin		ired Ethernet Por	ts					
Filter: All	A Filter	le Export 😸 Print						_
	Slot	Port ID	MAC	If Role	If Type	Overall Status	Administrativ	e 🛱
	1	1	54:7F:EE:AA:1	. Unconfigured	Physical	🕹 Admin Down	🕹 Disabled	-
- E Fabric Interconnects	1	2	54:7F:EE:AA:1	. Unconfigured		🕹 Admin Down	🕹 Disabled	Π
E Fabric Interconnect A (primary)	1	Enable			Physical	Admin Down	Disabled	1
Fixed Module	1	Disable			Physical	Admin Down	Disabled	
	1			-	Physical	V Sfp Not Pre	Disabled	1
	1	Configure a:	s Server Port	-	Physical	V Sfp Not Pre	Disabled	1
Monitoring Ethernet Ports	1	Configure a:	s Uplink Port	-	Physical	V Sfp Not Pre	Disabled	- =
Server Ports	1	Configure a	s FCoE Storage Port	-	Physical	V Sfp Not Pre	Disabled	
Storage EC Ports	1		-	-	Physical	V Sfp Not Pre	Disabled	-
Unconfigured Ethernet Ports	1	Configure a:	s Appliance Port		Physical	Sfp Not Pre	Disabled	
Port 1	1	Unconfigure		-	Physical	Sfp Not Pre	Disabled	1
Port 2	1	Сору		Ctrl+C	Physical	Sfp Not Pre	Disabled	1
	1				Physical	Sfp Not Pre	Disabled	-
	1	Copy XML		Ctrl+L	Physical	Sfp Not Pre	Disabled	-
Port 5	1	Delete		Ctrl+D	Physical	Admin Down	Disabled	-
	-	16	54:7F:EE:AA:1	. Unconfigured	Physical	Admin Down	Disabled	-

**3**. Repeat step 2 for the other FI as well.

4. Once server ports are configured on both FIs, the Chassis or FEX auto-discovery gets started. In case of FEX, after the deep discovery of FEX is complete, you will see two Fabric Extenders in the **Equipment** tab with overall status shown as Operable.



#### Figure 41 Overall Status of FEX After Auto-Discovery

Similarly, if server ports are connected to the chassis, you will see that the chassis is fully discovered, with all its IOMs, fans, power supplies and so on.

ſ



Figure 42 Overall Status of Chassis After Auto-Discovery

1

**5.** After the Chassis and FEX auto-discovery, the Blade Server and Rack Server auto-discovery will get started respectively. As and when the servers are discovered, you will see them getting added in the **Equipment** tab with overall status shown as Unassociated and availability state as Available, and discovery state as Complete.



#### Figure 43 Overall Status of Rack Servers After Discovery

Similarly, a Blade Server's status is shown in Figure 44.



#### Figure 44 Overall Status of Blade Servers After Discovery

6. Once all the servers are discovered, you can see the summary of all of them by choosing Equipment tab > Rack-Mounts > Servers as shown below.

I

ult Summary	G 🔘 🗅 New	- 🛛 Options 🛛 🚱	🔁 🛛 🛆 Pendin	g Activities 🛛 🚺 Exit											
0 8 0 4	>> 👬 Equipmen	t 🕨 🐲 Rack-Mounts 🕨	Servers												
ment Servers LAN SAN VM Admin	Servers														
	🛋 Filter 👄 Exp	ort 😹 Print													
Filter: All	Name	Overall Status	PID	Model	User Label	Cores	Memory	Adapters	NICs	HBAs	Operability	Power State	Assoc State	Pr	Fault Su
9	Server 1	Unassociated	UCSC-C220	Cisco UCS C220 M3	1	16	262144	1	0	0	1 Operable	I Off	Vone	1	N/A
Equipment	Server 2	Unassociated	UCSC-C220	Cisco UCS C220 M3		16	262144	1	0	0	1 Operable	Off	None		N/A
- New York Chassis	Server 3	Unassociated	UCSC-C220	Cisco UCS C220 M3		16	262144	1	0	0	1 Operable	Off	None		N/A
Rack-Mounts	Server 4	Unassociated	UCSC-C220	Cisco UCS C220 M3		16	262144	1	0	0	1 Operable	Off	None		N/A

#### Figure 45 Summary of Rack Servers After the Discovery

Or, in case of Blade Servers, you can see the summary by choosing **Equipment** tab > **Chassis** > **Chassis** <id> > **Servers**.

Figure 46 Summary of Blade Servers After the Discovery

Fault Summary	V		1	ew 👻 😧 Qptions 🛛 😧 🚺 🛕 Pe						
		N VM Admin	Servers ± = 4	Filter 👄 Export 🎉 Print						
	r: Al	•	Name	Overall Status	PID	Model	Serial	Operability	Power State	Assoc State
			Serve	r 1 Unassociated	UC58-8200-M3	Cisco UCS B200 M3	FCH164670FW	1 Operable	Off	None
Equipment			- Serve		UCSB-8200-M3	Cisco UCS B200 M3	FCH16277191	1 Operable	Off	None
🖃 🥡 Chassis			- Serve	r 3 🖡 Unassociated	UCSB-B200-M3	Cisco UCS B200 M3	FCH16487356	1 Operable	4 Off	None
E SP Cha			Serve	r 4 Unassociated	UCSB-8200-M3	Cisco UCS B200 M3	FCH16467MKC	1 Operable	Off	None
	IO Modules PSUs Servers Server 1 Server 2 Server 3 Server 4									

# **Upstream/ Global Network Configuration**

This subsection lists a few upstream/ global network configuration:

- **1.** Move to FC switching mode (FC-variant only)
- **2**. Uplink VLAN configuration
- 3. Uplink VSAN configuration (NFS-variant only)
- 4. Appliance VSAN configuration (FC-variant only)
- 5. Configure uplink ports
- 6. Configure universal ports as FC ports
- 7. Configure FC uplink ports (NFS-variant only)
- 8. Configure FC appliance ports (FC-variant only)
- **9.** Configure FC Zoning policies (FC-variant only)
- 10. Configure QoS classes and QoS policy for jumbo MTU

To configure upstream/ global network, follow these steps:

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



Figure 47 Setting FC Switching Mode on Fabric A for FC-Variant

2. (FC-variant only) You might see a warning message that Fabric Interconnects need to be restarted as a result of this action. Click **Yes**. Both the FIs will 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 in a production environment.

**3.** From the LAN tab, expand LAN > LAN Cloud, and right-click on VLANs, and choose Create VLANs.

I

1

🛕 Cisco Unified Computing System Manager - VSPE	X-FI					
Fault Summary	6			Pending A	ctivities 🛛 🧿	<u>E</u> xit
0 0 0 0 0 Equipment Server LAN AN VM Admin	>> ELAN		loud > 📑 VLANs Print	;		
Filter: All	Name	ID	Туре	Transport	Native	VLAN Sha
± =	📃 VLAN de	1	Lan	Ether	Yes	None
Fabric A     Fabric B     Gos System Class     LAN Pin Groups     Threshold Policies	< Details				III	
Appliance: Show Navigator	General		ons VLAN Group	Membership Fa	1	
Create VLANs     C	Actio	0				Name: tive VLAN: vork Type:

Figure 48 Creating VLANs

**4.** Enter the name of the VLAN and assign the VLAN ID. Keep the VLAN as default with the option Common/Global.

	Figure 49	VLAN Details for Creating VLAN		
🛕 Create VLANs			100.00	
Create VL	_ANs			0
	refix: <b>vSphereMgm</b> D lame: <not set=""></not>	t		
		al O Fabric A O Fabric B O Both Fabrics Configured Differently		
You are creating	global VLANs that map	to the same VLAN IDs in all available fabrics.		
Enter the range VLAN IDs: 1	e of VLAN IDs.(e.g. "20	009-2019", "29,35,40-45", "23", "23,34-45")		
Sharing Type:	None OPrimary	<ul> <li>Isolated</li> </ul>		
			Check Overlap	OK Cancel

Γ

- 5. Click Ok and deploy the VLAN. Repeat this steps for vSphereMgmt, VM-Data and vMotion VLANs. For NFS-variant, create the Storage VLAN.
- 6. (NFS-variant only) NFS-variant of the architecture uses NFS for VM data access, but still uses FC SAN boot for the hypervisors. In the SAN tab, expand SAN Cloud, and right-click on VSANs. Choose Create VSAN.

	Figure 50	Creating VSAN	for N	FS	S-Variant	
ſ	A Cisco Unified Computing	System Manager - VSP	EX-FI			
	Fault Summary		1	G	) 💿 💷 New 🔪 🏹 Options   🚱 🕕	Pending Activities
	0 0	0 0		>	> 🚍 SAN 🕨 🍊 Storage Cloud 🕨 🚍 VSANs	;
	Equipment Servers LAN SA	N VM Admin		ſ	¥SANs 	
	Filter: All	-		ľ	Name	ID
	± =			l	□= VSANs	
	SAN			II	VSAN default (1)	1
	SAN Cloud			I	Fabric A	
	Fabric A     Fabric B			Ш	VSANs	
	SAN Pin Groups			II	E-B Fabric B	
				II	VSANs	
	USANs	now Navigator		l		
	Policies Cr	reate VSAN		l		
	🗄 📈 Traffic Monitoring Se	essions				

7. (NFS-variant only) Enter a VSAN name in the Name field and provide VSAN ID and its corresponding FCoE VLAN ID. FCoE VLAN ID should not have conflict with any of the VLANs configured before. Keep the FC zoning disabled (default setting).

1

Figure 51 VSAN Details fo	r Creating VSAN
🚔 Create ¥SAN	×
Create VSAN	0
Name: Storage	
FC Zoning Settings FC Zoning:  Disabled  Enabled Do NOT enable local zoning if fabric interconnect is co Common/Global  Fabric A  Fabric B  Both	
You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.	A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.
	OK Cancel

I

Γ

8. (FC-variant only) Click the SAN tab, and expand Storage Cloud, and right-click on VSANs. Choose Create Storage VSAN.

🛕 Cisco Unifie	ed Computing	System Ma	nager - VSPE	K-FI	12 C 8 8 8 8	
Fault Summa	ary V			1	Ġ 🍥 🗳 New 🔪 🏹 Optio	ns 🛛 😮 🚯 🗋 🖾 Pending Activities
0	0	0	0		>> 🗐 SAN 🕨 🙆 Storage Cl	oud 🕨 🧮 VSANs
	rvers LAN SA	N VM Ad	min		VSANs	t 😸 Print
± =	· <u>· · · · · · · · · · · · · · · · · · </u>			Ш	Name	ID
	I Cloud				VSAN default (1)	1
+	Fabric A Fabric B				Contraction of the second seco	
 ⊕ ∰ Polic	≡lvs Sh ties Cr	ow Navigat eate Storag essions				

Figure 52 Creating Storage VSAN for FC-Variant

**9.** (FC-variant) Enter the VSAN name in the Name field, 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 before.

1

i iguic co				
A Create Storage VSAN		-		X
Create Storage VS	AN			0
Name: Storage FC Zoning Settings FC Zoning: Disabled • E Do NOT enable zoning for this upstream switch that has zoning	VSAN if the fabric interco			
<ul> <li>Common/Global          Fabric A     </li> <li>You are creating a global VSAN I         the same VSAN ID in all available     </li> </ul>	<ul> <li>Fabric B Both Fa</li> <li>that maps to</li> </ul>	brics Configured Differentl	to carry FCoE traffic and can be	
Enter the VSAN ID that maps to VSAN ID: 10	this VSAN.	Enter the VLAN ID th	hat maps to this VSAN.	
			ОК	Cancel

Figure 53 VSAN Details for Creating Storage VSAN

10. To configure Uplink ports connected to the infrastructure network, click the Equipment tab, expand Fabric Interconnects, choose a particular FI, expand Expansion Module 2 (this may vary depending on which port you have chosen as uplink port), right-click on the Ethernet port, and choose Configure as Uplink Port. Repeat this step for all the uplink ports on each FI.

Γ



#### Figure 54 Configuring Ethernet Ports as Uplink Ports

Cisco UCS 6248UP Fabric Interconnects have Universal Ports. The physical ports are 10G Ethernet ports by default, but can be converted in to Fibre-Channel ports as well. We need the FC connectivity to EMC VNX storage array at least for SAN boot. For that, some of the ports need to be converted to FC ports. We can convert ports from expansion module into FC port. For that, click Equipment tab, expand Fabric Interconnects and click Fabric Interconnect A. In the right pane, click Configure Unified Ports. Click Yes, in the warning window.

📩 Cisco Unified Computing System Manager - VSI	SPEX-FI	×
Fault Summary	🕻 🕝 💿 💷 New - 🔀 Options 🛛 🚱 💼 Pending Activities 🛛 🖸 Exit	սիսիս
		cisco
0 8 0 10	0 >> 🛱 Equipment > 🚥 Fabric Interconnects > 🚥 Fabric Interconnect A (primary)	primary)
Equipment Servers LAN SAN VM Admin	General Physical Ports Fans PSUs Physical Display FSM Faults Events Statistics	
Filter: Al	Fault Summary Physical Display	-
± =		
Equipment		
🖻 🖏 Chassis	Status 🗧 Up 🛄 Admin Down 📕 Fail 🔛 Link Down	
E Chassis 1	Aurilation & Burnha	
E B Fans	Overall Status:   Operable  Properties	
⊡- IO Modules ⊕- IO Module 1	Thermal: 1 Ok Name: A	
IO Module 1	Ethernet Mode: End Host Product Name: Cisco LICE 6248UP	
B- B PSUs	FC Mode: End Host FOUNDAME: Else Cost Statement Vendor: Else Cos Systems, Inc. PID: UCS-FI-6248UP	
ervers		
Rack-Mounts	rectors a second s	
E - FEX	Available Memory: 13.815 (GB) Total Memory: 16.232 (GB)	
E-Servers	Part Details 😵	=
Server 1	- Internal Fabric Manager	
Server 2	Local Storage Information	
B- Server 3	Configure Unified Ports	
E Server 4		
Eabric Interconnects		
Fabric Interconnect A (primary)	The Configure Unified Ports wizard allows you to change the port mode from Ethernet to Fibre Channel or FC to Ethernet. Changing the port mode on either module causes an interruption in data traffic because changes to the fixed module	
E Fixed Module	require a reboot of the fabric interconnect and changes on an expansion module require a reboot of that module.	
Port 1		
Port 1	Are you sure you want to launch this wizard and reboot the modules associated with any reconfigured ports?	
Port 4		
	Set striemer side-Host Hode Door loader version Valuatory advice xxy	
	Kernel Version: 5.0(3)N2(2.11)	
	Set FC End-Host Wode System Version: 5.0(3)N2(2.11)	
	Bet PL End-Hoot Hode Package Version: 2.1(1)A	
	Set FC Switching Mode	
	Startup Kernel Version: 5.0(3)N2(2.11)	
	Activate Firmuare	
Port 13	Save Changes Reset Valu	ues
۰ III ۲		

# Figure 55 Configuring Ethernet Ports as FC Ports for Storage Connectivity

I

Γ

12. In the Configure Unified Ports wizard, click Configure Expansion Module Ports.

	Figure 5	6 Configuring Expansion Mo	dule Ports				
Configure	Unified Ports	1 0 m 2 pm 1 0 1	- Bre	×			
U	Unified Computing System Manager						
	ure Fixed Mo	ne no anno anno		C			
Instructions The position of the slider determines the type of the ports. All the ports to the left of the slider are Ethernet ports (Blue), while the ports to the right are Fibre Channel ports (Purple). By default, Ethernet ports are Unconfigured and FC ports are Uplink ports. Right click on a port to change its type (Server, Uplink, Appliance, etc.)							
	The position of the s All the ports to the le By default, Ethernet	oft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ	t click on a port to change its type (Server, Uplink, App	bliance, etc.)			
Port	The position of the s All the ports to the le By default, Ethernet Transport	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership		liance, etc.)			
Port	The position of the si All the ports to the le By default, Ethernet Transport ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2	The position of the s All the ports to the le By default, Ethernet Transport ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3	The position of the s All the ports to the le By default, Ethernet Transport ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether	aft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5 ort 6	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Appliance Storage	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5 ort 6 ort 7	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Appliance Storage Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 2 ort 3 ort 4 ort 5 ort 5 ort 6 ort 7 ort 8	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Member Server Port Channel Member Appliance Storage Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5 ort 5 ort 5 ort 6 ort 7 ort 8 ort 9	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 3 ort 4 ort 5 ort 4 ort 5 ort 6 ort 7 ort 6 ort 7 ort 9 ort 10	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Member Server Port Channel Member Appliance Storage Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 3 ort 4 ort 5 ort 5 ort 6 ort 7 ort 6 ort 7 ort 9 ort 9 ort 10 ort 11	The position of the s All the ports to the le By default, Ethernet ether ether ether ether ether ether ether ether ether ether ether ether ether ether ether ether ether ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5 ort 6 ort 7 ort 8 ort 7 ort 8 ort 9 ort 10 ort 11 ort 12	The position of the s All the ports to the le By default, Ethernet ether	aft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Appliance Storage Unconfigured Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port ort 1 ort 2 ort 3 ort 4 ort 5 ort 6 ort 7 ort 6 ort 7 ort 8 ort 9 ort 10 ort 10 ort 11 ort 12 ort 13	The position of the s All the ports to the le By default, Ethernet ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port Port 1 Port 2 Port 3 Port 4 Port 5 Port 5 Port 5 Port 6 Port 7 Port 10 Port 10 Port 11 Port 12 Port 13 Port 14	The position of the s All the ports to the le By default, Ethernet ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App				
Port Port 1 Port 2 Port 2 Port 3 Port 4 Port 5 Port 5 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 10 Port 11 Port 12 Port 13 Port 14 Port 15	The position of the s All the ports to the le By default, Ethernet ether	eft of the slider are Ethernet ports (Blue), while the ports to ports are Unconfigured and FC ports are Uplink ports. Righ If Role or Port Channel Membership Server Port Channel Member Server Port Channel Member Server Port Channel Member Server Port Channel Member Appliance Storage Appliance Storage Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured	t click on a port to change its type (Server, Uplink, App Desired If Role	Niance, etc.)			

1

Move the slider to the middle of the bar as shown in Figure 57. Make sure that the ports 2/9 to 2/15 are showing as FC Uplink. Click Finish. A warning message window pops up to restart FIs. Click OK.

#### Figure 57 Verifying FC Upink on Ports 9 to 15 A Configure Unified Ports **Unified Computing System Manager Configure Expansion Module Ports** 0 Instructions The position of the slider determines the type of the ports. All the ports to the left of the slider are Ethernet ports (Blue), while the ports to the right are Fibre Channel ports (Purple). By default, Ethernet ports are Unconfigured and FC ports are Uplink ports. Right click on a port to change its type (Server, Uplink, Appliance, etc.) Port If Role or Port Channel Membership Desired If Role Transport Unconfigured Port 7 ether sthe Port 9 Inconfigured Port 9 FC Uplink ether Unconfigured Port 10 FC Uplink ether Unconfigured Port 11 ether FC Uplink Unconfigured Port 12 ether Unconfigured FC Uplink Ξ Port 13 ether Unconfigured FC Uplink Port 14 ether Unconfigured FC Uplink FC Uplink Port 15 ether Unconfigured Up 📕 Admin Down 📕 Fail 🔜 Link Down Configure Fixed Module Ports Configure Expansion Module Ports Finish Cancel

14. Once the FI is rebooted, repeat steps 12, 13 and 14 on FI-B.

ſ

15. (NFS-variant only) Click the SAN tab, expand SAN Cloud > Fabric A > Uplink FC Interfaces, and choose the FC interface. Change the VSAN to the Storage VSAN that was created in steps 6 and 7 and click Save Changes.

🚖 Cisco Unified Computing System Manager - VSPEX-FI	
Fault Summary	alı Ci
	FC Interface 2/
Equipment Servers LAN SAN /M Admin General Faults Events	
Filter: All	
E Encide Interface ID: 1 Slot ID: 2 Fabric ID: A	
□ Isable Interface User Label:	
Port Type: Physical Network Type: San	
C Port Channels     Transport Type: Fc Role: Network	
Locale: External     Port: svs/switch-A/slot-2/switch-fc/port-1	
C Interface 2/1     VSAN: Fabric dual/vsan Storage (10)     Fill Pattern: C Idle C Arbff	
Creating and the second s	
- Cinterface 2/5	
FC Interface 2/6	
	1
Save Changes	Reset Values

Figure 58 Selecting Storage VSAN for NFS-Variant

16. (FC-variant only) Physical FC ports further need to be classified as FC storage ports for directly attached storage array. Click the Equipment tab, expand Fabric Interconnect > Fabric Interconnect A > Expansion Module 2 > FC Ports and select each of the FC port and on the right plane, click Configure as FC Storage port.





**17.** (FC-variant only) Make sure that the port are up. From the VSAN drop down list, select the Storage VSAN configured in steps 9 and 10, and click **Save Changes**.

A Cisco Unified Computing System Manager - VSPEX-FI	
Fault Summary	alja CISI
0 9 0 7 >> 🛱 Equipment > 🧰 Fabric Interconnects > 📷 Fabric Interconnect A (primary) > 🏧 Expansion Module 2 > 📲 FC Ports > 📲 FC Port S	
Equipment       Servers       LAN       SAN       VM       Admin         Filter:       All       Image: Servers       Fault       Statistics         Image: Servers       Fault       Image: Servers       Fault       Statistics         Image: Servers       Fault       Image: Servers       Fault       Statistics         Image: Servers       Fault       Summary       Image: Servers       Image: Servers       Physical Display         Image: Servers       Fault       Summary       Image: Servers       Image: Ser	
FC Port 13     FC Port 14     FC Port 15     FC Port 15     FC Port 16     F	Reset Values

# Figure 60 Selecting Storage VSAN for FC-Variant

18. (FC-variant only) At this point of time, EMC VNX storage array will do Fibre Channel flogi into the FIs. Using the WWPN of the VNX storage array, we can carve out the zoning policy on the FI. Use SSH connection to the UCS Manager Virtual IP address, and issue connect nxos a command. In the read-only NX-OS shell, issue show flogi database command and note down the WWPN of the storage array.

I

Figu	ıre 61	Port Name (I	NWPN) of the Storage Array			
₽ 10.65.121.228 - I	PuTTY					
The copyrights owned by other license. Certs the GNU General Lesser General such license : http://www.ope	perating http://ww 2002-201 s to cert c third p ain compo al Public l Public is avails ensource.	System (NX sw.cisco.co 2, Cisco S 2 ain works barties and 5 and to 5 License (L 1 License (L 2 ble at 5 org/licens 5 org/licens	m/tac ystems, Inc. All rights is contained in this softway used and distributed und his software are licensed GPL) version 2.0 or the ( GPL) Version 2.1. A copy es/gp1-2.0.php and es/lgp1-2.1.php	re are der d under GNU		
INTERFACE	VSAN	FCID	PORT NAME	NODE NAME		
	10 10		50:06:01:64:3e:a0:65:0a 50:06:01:65:3e:a0:65:0a			
Total number of flogi = 2. VSPEX-FI-A(nxos)# VSPEX-FI-A(nxos)# VSPEX-FI-A(nxos)#						

**19.** (FC-variant only) In UCS Manager GUI, click the **SAN** tab, expand **SAN** > **Policies** > **root**, and right-click the Storage connection policies, and choose **Create Storage Connection Policy**.

1
ult Summary		Ġ 🔘 🗉 New 🖌 🌛 Opt	tions 🛛 🕜 🔒 🖾 Pendina
$\otimes$ $\nabla$ $\triangle$		1	
0 0 0	0	>> 🗮 SAN 🕨 🚿 Policies 🕨	🛕 root 🔸 🚿 Storage Conn
uipment Servers LAN SAN VM Admin		Storage Connection Poli	
		🛨 🖃 🕰 Filter 👄 Exp	ort 😸 Print
Filter: All		Name	Description
= SAN			
SAN Cloud			
Storage Cloud			
Policies			
S Default vHBA Behavior			
😥 🛒 Fibre Channel Adapter Policies			
🗐 SAN Connectivity Policies			
🔊 Storage Connection Policies			
Threshold Policies	Storage	e Connection Policies	
vHBA Templates	Create	Storage Connection Policy	1
⊕ ∰ Pools	_		

Figure 62 Creating Storage Connection Policy

**20.** (FC-variant only) Enter the name Fabric-A in the name field and optional description. Choose Single Initiator Multiple Targets as the Zoning Type. Click to add a new FC Target Endpoint.

Γ

Create Storage C		×
Create Sto	rage Connection Policy	0
(	Fabric-A	
	zones for fabric A	
Zoning Type:	None Single Initiator Single Target Single Initiator Multiple Targets	
FC Target		
	> Export 😓 Print	
WWPN	Path VSAN	
	15.	
	-	
	ОК	Cancel

Figure 63 Details for Creating Storage Connection Policy for FC-Variant

1

**21.** (FC-variant only) Copy the WWPN from the **show flogi database** output from step 18 and paste it in the WWPN field. Provide optional description, click the radio button **Path A** and for VSAN choose **Storage VSAN** from the drop-down list.



## 22. (FC-variant only) Similarly, add the second FC target endpoint for fabric A and click OK.

ſ

Name: Fabric-A				
Description: zones for fabric	c A		_	
oning Type: O None O Sir		Single Target 💿 Single In	itiator Multiple Targets	
FC Target Endpoints	igio iniciacor .		actor matche rangets	
🔍 Filter 👄 Export 🍪 Print	:			
WWPN	Path	VSAN	E.	
50:06:01:65:3E:A0:65:0A	A	Storage		
50:06:01:64:3E:A0:65:0A	A	Storage		
			<b>E</b>	
			1	
			<b>1</b>	
			+	

Figure 65 Adding Second FC Target Endpoint for Fabric A

1

**23.** (FC-variant only) Repeat steps 18 to 22 for Fabric B as well. The end result should look similar to Figure 66.

#### 🚔 Cisco Unified Computing System Manager - VSPEX-FI Fault Summary 🕻 🌀 🌑 🖪 New 🚽 🛃 Options 🛛 🚱 🕕 Pending Activities 🛛 💽 Exit $\otimes$ ◬ V Δ >> 🚍 SAN + 🚿 Policies + 🛕 root + 🚿 Storage Connection Policies 0 0 0 0 Storage Connection Policies Equipment Servers LAN SAN VM Admin 🛨 😑 🔍 Filter 👄 Export 🍪 Print Filter: All • WWPN Name Description ± = 🖃 🚍 SAN 50:06:01:6D:3E:A0:65:0A E Fc Target Endpoint SAN Cloud E Fc Target Endpoint 50:06:01:6C:3E:A0:65:0A Fabric-A zones for fabric A S Policies E Fc Target Endpoint 50:06:01:65:3E:A0:65:0A SAN Cloud 🗱 Fc Target Endpoint 50:06:01:64:3E:A0:65:0A 🖻 🛕 root S Default vHBA Behavior Fibre Channel Adapter Policies SAN Connectivity Policies • S 🕀 🚿 Threshold Policies

Figure 66 FC Target Endpoints on Fabric A and Fabric B

24. The next global configuration task is QoS configuration. Click the LAN tab, expand LAN > LAN Cloud, and choose QoS System Class. Check the check box next to Platinum for setting the priority, and set MTU to 9216. Keep other configuration as default and save the configuration.

#### Figure 67 Configuring QoS

I

wit Summary	🕄 🔘 🗳 New 🗸	Option:	s   🕜 🕻	Pending Ac	ivities 🛛 🗿 Exit					
0 8 0 4	>> 🗐 LAN + 🔿 LAN Cloud + 🍟 QoS System Class							👬 QoS System Clas		
uipment Servers LAN 5AN VM Admin	General Events F	SM							_	
Filter: All	Priority	Enabled	CoS	Packet Drop	Weight		Weight (%)	мти		Multicast Optimized
	Platinum	<b>V</b>	5		10	•	50	9216	•	
= LAN	Gold		4		9	•	N/A	normal	•	
E-C LAN Cloud	Silver		2	<b>V</b>	8	-	N/A	normal	•	
Habric B	Bronze		1	<b>V</b>	7	•	N/A	normal	•	
QoS System Class	Best Effort		Any		5	•	25	normal	•	
Internal LAN	Fibre Channel		3		5	-	25	fc	•	N/A
Internal Fabric A      Internal Fabric B										
Policies										
Appliances										
E An Cloud										

25. From the LAN tab, expand LAN > Policies > root, and choose Create QoS Policy.



**26.** Create a QoS policy with name jumboMTU and for the Priority field choose **Platinum** from the drop-down list. Click **OK** to save the configuration.

# **Configure Identifier Pools**

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

To configure pools mentioned above, follow these steps:

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



#### Figure 69 Creating UUID Suffix Pool

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

Figure 70 Details for Creating UUID Suffix Pool

	_
mputing System Manage	2
Define Name and Description	
Name: VSPEX-UUIDs Description: UUID Pool for VSPEX project Prefix: O Derived O other	
Assignment Order:   Default  Sequential  Prev Next > Finish Cancel	٦
2	efine Name and Description

3. Click to **H** add UUID block.

I

Figure 71 Add	ling UUID Block	ſ		
Create UUID Suffix Pool				×
Unified C	omput	ing Syst	em Man	agei
Create UUID Suffix Pool	Add UUID	Blocks		0
<ol> <li><u>√ Define Name and</u> <u>Description</u></li> <li><u>√ Add UUID Blocks</u></li> </ol>	Name	From	То	
		E Add	Delete	
		< Prev	Next > Finish	Cancel

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

I

1

#### Figure 72 Specifying Block Size

A Create a Block of UUID Suffixes	x
Create a Block of UUID Suffixes	9
1	
From: 600D-0000000001 Size: 20	
ОК	Cancel

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

🛕 Cisco Unified Computing System Manager - VSPI	EX-FI
Fault Summary	G ● ■ New - Q Options 0 0
Equipment Serves LAN S/N VM Admin	MAC Pools
	Name
Propulates     Policies     Policies     Policies     Pools     Pools     Pools     Pools     MAC Pools	
Bub-Organ Traffic Monitoring Sub-Organ	

#### Figure 73 Creating MAC Pool

7. Enter the name and description for MAC pool and click Next.

#### Figure 74 Details for Creating MAC Pool

I



Figure 75

8.	Click	E Add	to add MAC pool block.
----	-------	-------	------------------------

Adding MAC Address

Create MAC Pool	omput	ting Syst	tem Man	age
Create MAC Pool 1. √Set MAC Pool Name	Add MAC	Addresses		0
2. √ <u>Add MAC Addresses</u>	Name	From	То	<b>F</b>
		E Add	Delete	•
		< Prev	Next > Finish	Cancel

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

1

#### Figure 76 Specifying MAC Address Block

A Create a Block of MAC Addresses	Color 1	×
Create a Block of MAC Addresses		٢
First MAC Address: 00:25:85 60:0D:00 To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:85:xx:xx:xx	Size:	30 丈
	ОК	Cancel

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

Fault Summa	ry V	Δ		Ġ 🏐 🖬 New 🔹 隆
0	0	0	0	>> 🗮 SAN 🕨 🌚 Pools
Equipment Se	rvers LAN	AN VM Admir	ו	WWxN Pools
Filt	er: All		-	🛨 🖃 🕰 Filter 👄
веl				Name
		ols ols- izz Show I	Navigator WWxN Poo	
		Create	** **XIV P00	

### Figure 77 Creating WWxN Pool

- **12.** Enter name, and description for WWxN and choose **3 Ports per Node** from the drop-down list for max ports.
- **13.** Click **Hadd** to add a block of WWxN IDs.



Γ

Create WWxN Pool	Computi	ing Systen	n Manage	r
Create WWxN Pool 1. √Define Name and	Add WWN	Blocks		0
2. √ <u>Add WWN Blocks</u>	Name	From	То	-
		Add <	ev Next > Finish	Cancel

14. Enter first WWN IDs and sufficiently large number of block size. Click OK and Finish.

#### Figure 79 Specifying WWxN Block Size



15. Next 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 > IP Pool ext-mgmt, and click the Create Block of IP addresses link in the right pane.



#### Figure 80 Creating IP Address Block

**16.** Enter the initial IP address, size of the pool, default gateway and subnet mask. Click **OK** to deploy the configuration. IP addresses will be assigned to various Rack-Mount server CIMC management access from this block.

🛕 Create Bloc	k of IP Addresses	-	-	
Create a	a Block of IP Addresses			0
From:	10.65.121.231 T	Size:	0	8
Subnet Mask:	255.255.255.0	Default Gateway:	10.65.121.1	
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0	
				OK Cancel

#### Figure 81 Specifying the IP address Block Size

# **Configure Server Pool and Qualifying Policy**

ſ

Creation and policy based auto-population of server pool can be sub-divided into the following tasks:

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

Follow these steps to complete the three tasks mentioned above:

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

Fault Summ	ary 📅	A A		🎯 🌕 🛄 Ne
_ ○	8			>> 🥪 Server
	ervers LAN SAN	J VM Admin	d	• - 4
• •			11	Name
	vice Profiles vice Profile Templa	ates		
· · · · · · · · · · · · · · · · · · ·	🔛 UUID Suf	Server Pools Create Server Pool		_
🗄 🚮 Sch	edules	create server Poor		J

1

Figure 82 Creating Server Pools

- 2. Enter the name of the server pool in the Name field, and click Next.
- Figure 83 Entering Details in the Create Server Pool Wizard

Create Server Pool Unified	Computing System Manager
Create Server Pool 1. √Set Name and	Set Name and Description
Description 2. D <sub>Add Servers</sub>	Name: USPEX-Servers

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

Unified C	Computing System Manager	
e Server Pool 1. √ <u>Set Name and Description</u> 2. √ <b>Add Servers</b>	Add Servers	
100 201102	Servers Pooled Servers	
	Ch       Slo       Ra       Us       PID       Ad       Ad       Serial       Corr       II       Corr       III       Corr       III       Corr       III       Corr       III       Corr       III       Corr       IIII       Corr       IIII       Corr       IIII       Corr       IIII       Corr       IIIII       Corr       IIIII       Corr       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	. Ad Se Co
	Details for rack-unit-1 Details	
	Model:         UCSC-C220-M35         Model:	

### Figure 84 Adding Servers in the Create Server Pool Wizard

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

Γ



Figure 85 Creating Server Pool Policy Qualification

5. Enter a name for the server policy qualification criterion in the Name field. In the left pane under Actions choose **Create Memory Qualifications**.

	licy Qualificat	ion								
ming										
Name: Min-Memory										
escription: Minimum memory crite										
is server pool policy qualification will ap	ply to new or re-discovere	d servers. Existing se	rvers are n	ot qualified	l until the	ey are re-discover	red			
Actions	Qualifications									
Create Adapter Qualifications	🛨 🖃 🕰 Filter 🛋	Export 😸 Print								
Create Chassis/Server Oualifications	Name	Max	Model	From	То	Architecture	Speed	Stepping	Power Group	R.
Create Memory Qualifications										*
Create Storage Qualifications										
create storage Qualitications										
Create Server PID Qualifications										
Create Server PID Qualifications Create Power Group Qualifications										
Create Server PID Qualifications Create Power Group Qualifications										
Create Server PID Qualifications										

**Creating Memory Qualification** 

Figure 86

I

**6.** Set the minimum RAM capacity as 64GB RAM for the pool qualification criterion. Click **OK** twice to create the qualification.

**Note** This is just an example criterion, you can choose a criterion that suites your requirement.

#### Figure 87 Specifying Minimum RAM Capacity for Memory Qualification

Create Memory Qualifications	×
Create Memory Qualifications	0
Clock (MHz): Unspecified select Latency (ns): Unspecified select Min Cap (MB): Unspecified select Minx Cap (MB): Unspecified select 65536 Width: Unspecified select Units: Unspecified select	
OK	Cancel

7. From the Servers tab, expand Servers > Policies > root, right-click on Server Pool Policies and choose Create Server Pool Policy.



Figure 88 Creating Server Pool Policy

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

🛕 Create Sen	ver Pool Policy	×
Create	Server Pool Policy	0
	VSPEX-Servers	
	Policy for VSPEX server pool classification	
Target Pool:	UServer Pool VSPEX-Ser ▼	
Qualification:	Min-Memory	
	0	
		OK Cancel

#### Figure 89 Details for Creating Server Pool Policy

**9.** If you go back to the server pool created in step 1 above and click the **Servers** tab on right pane, you will see that all the compute resources that meet the qualification criteria are dynamically added to the server pool. Figure 90 shows the screen capture taken from the FC-variant of the architecture, where combination of Cisco UCS B200M3 Blade Servers and Cisco UCS C220M3 Rack Servers are used to share the workload. This architecture showcases the form-factor independent architecture with unified managed using UCS Manager.

#### Figure 90 Qualified Compute Resources Automatically Added to the Server Pool

ault Summary	G 🔘 🖬 New - 📝	Options 0	0   🛆		rities 🛛 🚺 Ex	ř.		
0 0 0 0	>> 🥪 Servers 🕨 🚱 Po	ools 🕨 Å root	· 🥪 Serv	ver Pools 🕨	Server Poo	VSPEX-Servers	Server Pool VS	PEX-Ser
quipment Servers LAN SAN VM Admin	General Servers Fault							
Filter: Al	Name	Chassis ID	1	Rack ID	Assigned	Assigned To	Reason	
Servers		r 1		1	No		Dynamically Added(org-root/pooling-policy-VSPEX-Serve	··· *
- Service Profiles	- Rack-Mount Serve	r 2		2	No		Dynamically Added(org-root/pooling-policy-VSPEX-Serve	
Service Profile Templates		1	1		No		Dynamically Added(org-root/pooling-policy-VSPEX-Serve	
😥 📆 Policies		1	2		No		Dynamically Added(org-root/pooling-policy-VSPEX-Serve	
Pools     A root     Server Pools     Server Pool     Server Pool     Server Pool	Server 1/3	1	3		No		Dynamically Added(org-root/pooling-policy-VSPEX-Serve	h
⊕-∰ Schedules								

# **Configure Service Profile Template**

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

To create service profile template, follow these steps:

 From the Servers tab. Expand Servers > Service Profile Templates, right-click on service profile templates and choose Create Service Profile Template.



Figure 91 Creating Service Profile Template

2. Enter the service profile template name in the name field, keep the type as **Initial Template**, and choose **UUID pool** for UUID assignment.

Figure 92	Creating Service Profile Template - Entering Details
🌲 Create Service Profile Template	
Unified C	Computing System Manager
Create Service Profile Template	Identify Service Profile Template You must enter a name for the service profile template and specify the template type. You can also specify how a UUD will be assigned to this template and enter a description.   Name: VSPEX-Service-Profile   The template will be created in the following organization. Its name must be unique within this organization.   Where: org-root   The template will be created in the following organization. Its name must be unique within this organization.   Type: Initial Template   UDD will be assigned to the server associated with the service generated by this template.   UUID Assignment: SPEX-UUDS(20/20)   UUID will be assigned from the selected pool.   The UUID will be assigned from the selected pool.   The available/total UUIDs are displayed after the pool name.   Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.
	<prev next=""> Finish Cancel</prev>

I

Γ

**3.** Click the **Expert** radio button for configure LAN connectivity. Click to create a vNIC.

	Figure 93	Creating Service	Profile Template - LA	N Configuration Detai	ls	
A Create Service Profile Template						×
Unified	Comput	ing System	Manager			
Create Service Profile Template 1. √ <u>Identify Service Profile</u>	Networking	cify LAN configuration information.				0
Template 2. √ Networking 3. □ Storage 4. □ Zoning 5. □ vNIC/vHBA Placement	Dynamic vNIC Conner	ction Policy: Select a Policy to use (no D	ynamic vNIC Policy by defa 💌	Create Dynamic vNIC Connection Policy		
6. Server Boot Order     7. Maintenance Policy     8. Server Assignment     9. Operational Policies		would you like to configure LAN con the or more vNICs that the server should		No vNICs 🕜 Use Connectivity Policy		
	Name	MAC Address	Fabric ID	Native VLAN	-	
	Click Add to specify on	e or more iSCSI vNICs that the server s	Toelet Add Modfy		v	
	Name	Overlay vNIC Name	ISCSI Adapter Policy	MAC Address		
			🚹 Add 👕 Delete 📲 Modify			
				< Prev	Vext > Finish	Cancel

4. Create a system vNIC for fabric A. Enter system-A as the vNIC name, choose the MAC pool created in section D, click the radio button fabric A for fabric ID, check the check boxes vMotion and vSphereMgmt VLANs with vSphereMgmt as native VLAN. For MTU enter 9000, for Adapter Policy field, choose VMware and choose jumboMTU for the QoS Policy field.

I

1

system-A		Address
IC Template:	MAC	Address Assignment: VSPEX-MACs(30/30)
	±	Create MAC Pool
ate vNIC Template	The	MAC address will be automatically assigned from the selected pool.
o: 💽 Fabric A 🔿 Fabric B 🥅	Enable Failover	r
Ns		
lect Name		Native VLAN
Storage		<u> </u>
VM-Data		0
vMotion		C
▼ vSphereMgmt		©
		C V
vSphereMgmt		C V
vSphereMgmt eate VLAN TU: 9000		C V
vSphereMgmt eate VLAN ITU: 9000	value in the On	
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same		S System Class
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of		S System Class oS Policy.
vSphereMgmt eate VLAN ITU: 9000 ning sure that the MTU has the same sponding to the Egress priority of pup: <not set=""></not>	the selected Q	<u>S System Class</u> oS Policy. in Group
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of up: <not set=""></not>	the selected Q	S System Class oS Policy.
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of pup: <not set=""></not>	the selected Q	<u>S System Class</u> oS Policy. in Group
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of up: <not set="">  r Performance Profile</not>	the selected Q	S System Class oS Policy. in Group
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of up: <not set=""> ational Parameters cr Performance Profile Adapter Policy: VMWa</not>	the selected Qo Create LAN Pi	S System Class oS Policy. in Group
	the selected Q Create LAN Pi re re	S System Class oS Policy. in Group Create Ethernet Adapter Policy
vSphereMgmt eate VLAN TU: 9000 ning sure that the MTU has the same sponding to the Egress priority of up: <not set=""> ational Parameters cr Performance Profile Adapter Policy: VMWa</not>	the selected Q Create LAN Pi re re mtu	S System Class oS Policy. in Group

Figure 94 Creating a System vNIC

5. Similarly, create one more vNIC with exact same properties on fabric B.

ſ

**6.** (NFS-variant only) Create two more vNICs similar to steps 3, 4 and 5 for NFS server access. Enter the names Storage-A and Storage-B for vNICs on fabric A and B respectively, choose only Storage VLAN and mark it as native VLAN and choose **VMware** and **jumboMTU** for adapter policy and QoS policy respectively.

7. Finally, create a vNIC for VM data traffic. Enter **data-A** for vNIC name, same MAC address pool name, **Fabric A** for Fabric ID, **VM-Data** as native VLAN, and **VMware** as adapter policy.

1

🚔 Create vNIC		X
Create vNIC		0
Name: data-A Use villC Template:	MAC Address MAC Address Assignment: VSPEX-MACs(30/30)  Create MAC Pool The MAC address will be automatically assigned from the selected pool.	
Fabric II : 💽 Fabric A 🕜 Fabric B 🕅 Enable	e Failover	
VLANs		
Select Name	Native VLAN	
default Storage		
VM-Data		
🛨 Create VLAN		
MTU: 1500		
Pin Group: <not set=""> 💌 🚹 Creat</not>	te LAN Pin Group	
Operational Parameters		
Adapter Performance Profile		
Adapter Policy: VMWare		
Dynamic vNIC Connection Policy: <not set=""></not>	Create Dynamic vNIC Connection Policy	
QoS Policy: <not set=""></not>	Create QoS Policy	
Network Control Policy: <not set=""></not>	Create Network Control Policy	
		OK Cancel

Figure 95 Creating vNIC for VM Data Traffic

**8.** Similarly, create one more vNIC for Fabric B for VM data traffic. Table 9 summarizes all the vNICs created on the service profile.

vNIC Name	MAC address assignment	VLANs	Native VLAN	Fabric	MTU	Adapter Policy	QoS Policy
System-A	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	А	9000	VMware	jumboMTU
System-B	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	В	9000	VMware	jumboMTU
Storage-A*	MAC pool	Storage	Storage	А	9000	VMware	jumboMTU
Storage-B*	MAC pool	Storage	Storage	В	9000	VMware	jumboMTU
Data-A	MAC pool	VM-Data	VM-Data	А	1500	VMware	-
Data-B	MAC pool	VM-Data	VM-Data	В	1500	VMware	-

# Table 9Summary of all the vNICs created on the service profile

\*Storage vNICs are created for NFS-variant only

Γ

**9.** In the Storage window, click the **Expert** radio button for SAN connectivity and choose the option VSPEX-WWNs for WWNN pool from the drop-down list. Click to add vHBA.

Figure 96

Create Service Profile Template					
Unified (	Computing	System	Manager		
Create Service Profile Template 1. √Identify Service Profile	Storage Optionally specify disk po	olicies and SAN confi	guration information.		(
Template 2. √Networking 3. X Storage 4. 2 Joning 5. VNIC/VHBA Placement 6. Server Boot Order 7. Maintenance Policy 8. Server Assignment	Select a local disk configuration poli Local Storage: Select Local Stor	rage Policy to use 📃 💌	If nothing is selected, the default i policy will be assigned to this servi		
9. Operational Policies	A server is identified on a SAN by it profile. World Wide Node Name WWNN Assignment: VSPEX-WW The WWNN will be assigned from	/Ns(100/100) m the selected pool. derived from this pool as	(WWNN). Specify how the system sho	uld assign a WWNN to the server associated v	with this
	Name		WWPN		<b>P</b>
			Dele 🛃 Add 👔 Modfy		
	•		m		,
				<pre>Prev Next &gt; Finis</pre>	h Cancel

**Creating Service Profile Template - Storage Configuration Details** 

1

**10.** Enter the vHBA name as vHBA-A in the Name field, Choose the WWPN assignment as **Derived** from the drop-down list, click the **A** radio button for Fabric ID, choose VSAN as **Storage VSAN** from the drop-down list, and choose the Adapter policy as **VMWare**. Click **OK** to deploy the vHBA.

eate vHBA		
Name: vHBA-A	world Wide Port Name	
• vHBA Template:	WWPN Assignment: Derived	
Create vHBA Template	Create WWPN Pool If you select a WWxN Pool for the World Wide Node Name, the WWPN will be derived from that pool. If you did not select a WWxN Pool for the World Wide Node Name, the WWPN assigned by the manufacturer will be used. Note: When a manifacturer assigned WWPN is used, the WWPN will not be migrated if the service profile is moved to a new server.	
Fabric ID:  A B Select VSAN: Storage Pin Group: <not set=""></not>	Create VSAN     Create SAN Pin Group	
Persistent Binding:		
lax Data Field Size: 2048		
Operational Parameters	8	
apter Performance Profile		
dapter Policy: VMWare	eate Fibre Channel Adapter Policy	
QoS Policy: <not set=""> 🔻 🛨 Cri</not>	eate QoS Policy	

Figure 97 Creating vHBA on Fabric A

I

Γ

- **11**. Repeat step 11 for vHBA-B on fabric B, keep all the configuration same as fabric A.
- **12.** For FC-variant of the solution, in the **Zoning** window, click to create a vHBA initiator group.

Figure 98	Creating Service Profile	e Template - Zoning Deta	ails
A Create Service Profile Template	an an far an a Barran far the feature of	(me	
Unified C	Computing Syste	em Manager	
Create Service Profile Template          1.        Identify Service Profile         Template       2.         2.        Vetworking         3.        Storage         4.        Zoning         5.        VIC/VHBA Placement	Zoning Specify zoning information Zoning configuration involves the following steps: 1. Select vHBA Initiator(s) (vHBAs are created on 2. Select vHBA Initiator Group(s) 3. Add selected Initiator(s) to selected Initiator Gr		
6. Server Boot Order     7. Maintenance Policy     8. Server Assignment	Select vHBA Initiators	Select vHBA Initiator Groups	
9. Operational Policies	VHBA-A VHBA-B >> Add To >>		Storage Connection Policy Name
	•	III	
			< Prev Next > Finish

1

**13.** (FC-variant only) Enter SAN-A in the Name field of Create vHBA Initiator Group window, and choose **Fabric-A** zoning policy from the drop-down list and click **OK**.

100

Figure 99	Creat	ting vHBA Initiator Gr	oup for FC-Variant	
Create vHBA Initiator Group	_			
Create vHBA Initia	tor Grou	р		(
vHBA Initiator Group				
Name: SAN-A				
Description:			_	
Charles Consulting Dallary To	hule A			
Storage Connection Policy: Fa	Dric-A		reate Storage Connection Policy	
	- D-1			
Global Storage Connectio		er org is assigned to this vHBA	initiator group	
Properties	acy defined und	er org is assigned to this vriba	nicator group.	
Storage Connection Policy	: Fabric-A			
	zones for fabr	ic A		
Zoning Type	: Single Initiato	r Multiple Targets		
FC Target Endpoints				
🕰 Filter 👄 Export 😸 P	rint			
WWPN	Path	VSAN		
50:06:01:64:3E:A0:65:0A	A	Storage	<u>^</u>	
50:06:01:65:3E:A0:65:0A	A	Storage		
				OK Cancel

I

Γ

**14.** (FC-variant) Repeat steps 14 and 15 for the zoning on fabric B. Now choose **vHBA-A** from the list of initiators and **SAN-A** from the initiator-group, and click to add initiator to the selected initiator group.



**15.** Repeat step 16 for fabric B as well. The end result should look like Figure 101. Click **Next** and choose the default configuration on the vNIC/vHBA Placement window.

Create Service Profile Template  I. Videntify Service Profile  Template  Create Service Profile  Coning Configuration involves the following steps:  Sectify the Thistor(s) (videa are created on storage page)  Sectify the Thistor(s) (videa are created on storage)  Se	Create Service Profile Template	Computing System Mana	ger
e	Create Service Profile Template 1. √ <u>Identify Service Profile</u> <u>Template</u> 2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. □ <u>vtNIC/tHBA Placement</u> 6. □ <u>Server Boot Order</u> 7. □ <u>Maintenance Policy</u> 8. □ <u>Server Assignment</u>	Zoning Specify zoning information Zoning configuration involves the following steps: 1. Select vHBA Initiator(s) (vHBAs are created on storage page) 2. Select vHBA Initiator Group(s) 3. Add selected Initiator Group(s) Select vHBA Initiator Name VHBA-A VHBA-B Solution Select vHBA Initiator Select vHBA Initiator	or Groups Storage Connection Policy Name Fobric-B : Initiator vHBA-B Fabric-A : Initiator vHBA-A
		•	

Figure 101 Window Showing vHBAs Added to the Initiator Group

- **16.** For the NFS-variant of the solution, choose the default configuration in Zoning and vNIC/vHBA Placement window. Click **Next**.
- For both the architectures, in the Server Boot Order window, choose Create a Specific Boot Policy from the drop-down list. Choose the option Add CD-ROM as the first boot order choice. Choose vHBA-A as the next choice, and provide a name vHBA-A. Click the radio button Primary for Type and click OK.

ſ

ger		25
ger		
1 2		e e Cancel Primary
C A	t SAN Boot	d SAN Boot

18. Similarly, choose vHBA-B as the next (secondary) choice to boot from SAN. Once both the vHBAs are added, make sure that the check boxes Reboot on Boot Order Change and Enforce vNIC/vHBA name are checked. Click Add SAN Boot Target under the vHBAs, and click Add San Boot Target to SAN primary.

1

Figure 1	-		get to SAN Prim	_		
Create Service Profile Template 1. √ Identify Service Profile Template 2. √ Networking 3. √ Scrage 4. √ Zoning 5. √ <u>vNIC/VHBA Placement</u>	Server Boot Order Optionally specify the boot Select a boot policy. Boot Policy: Create a Specific Boot F	t policy for this s				(
6. √ <u>Server Boot Order</u> 7. □ <u>Maintenance Policy</u> 8. □ <u>Server Assignment</u> 9. □ <u>Operational Policies</u>	Local Devices Add Local Disk. Add CD-ROM Add Floppy VNICs VNIC data-A	8	If Enforce vNIC/vHBA/iSCSI	loes not indicate a ices within the sam I Name is selected (HBAs/ISCSI are sel	boot order presence. e device class (LAN/Storage/ISCSI and the vNIC/vHBA/ISCSI does no ected if they exist, otherwise the	ot exist, a config erro
	VNIC data-B VNIC system-A VNIC system-B		Name CD-ROM Storage Storage	Order 1 2	VNIC/VHBA/ISCSI VNIC	Type
	VHBAs VHBA VHBA-A VHBA VHBA-B Add San Boot Target To Add San Boot Target To Sol San Boot Target To		SAN secondary		vHBA-B	Secondary

Provide target WWPN of the VNX storage device (which can be obtained using show flogi database NX-OS CLI command executed under connect nxos {alb} shell as described in the previous subsection). Keep the target as Primary.

Figure 104 Adding SAN Boot Target as Primary

ſ

🛕 Add SAN Boot Ta	rget	×
Add SAN B	oot Target	0
Boot Target LUN:	0	
	50:06:01:64:3E:A0:65:0A	
Туре:	Primary O Secondary	
0		
		OK Cancel

20. Repeat step 21 for the fabric B as well. The end result will look like Figure 105.

Figure	105 Server Boot Ord	er After the Configuratio	on is Com	plete	
Unified (	Computing Sys	stem Manage	r		
Create Service Profile Template 1. √ <u>Identify Service Profile</u> <u>Template</u> 2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. √ <u>vNIC/vHBA Placement</u>	Server Boot Order Optionally specify the boot policy f Select a boot policy. Boot Policy: Create a Specific Boot P	for this service profile template.			
<ol> <li>✓ Server Boot Order</li> <li>Maintenance Policy</li> <li>B Server Assignment</li> <li>Operational Policies</li> </ol>	Local Devices  Add Local Disk.  Add CD-ROM  Add Floppy  VNICs  VNICs VNIC data-A	Boot Order      Reboot on Boot Order Change:     Enforce vNIC/VHBA/ISCSI Name:      WARNINGS:      The type (primary/secondary) does     The effective order of boot devices      If is not selected, the vNICs/VHBA     The selected, the vNICs/VHBA     The selected, the vNICs/VHBA	inot indicate a bo within the same is selected an As/ISCSI are select	device class (LAN/Storage/iSC nd the vNIC/vHBA/iSCSI does	not exist, a config
	VNIC data-B				
	vNIC system-A	Name	Order	VNIC/VHBA/ISCSI VNIC	Туре
	white system-b	CD-ROM	1		
		E-Storage	2		
	vHBAs	SAN primary		vHBA-A	Primary
		SAN Target prima	ry		Primary
	vHBA vHBA-A	🖻 🛒 SAN secondary		<b>vHBA-B</b>	Secondary
	Add SAN Boot Target	SAN Target prima	ry		Primary
	iSCSI vNICs  Set Boot Parameters	8			
				🔺 Move Up 🔍 Move Dowr	Delete

**21.** Click **Next** to go to the Maintenance Policy window. Keep all the fields at default and click **Next** to continue to Server Assignment window. For Pool Assignment, choose the Server Pool created in the previous sub-section. Click **Next**.

1

Figure 106 Creating Service Profile Template - Configuring Server Assignment A Create Service Profile Template Unified **Computing System Manager** Server Assignment Create Service Profile Template Optionally specify a server pool for this service profile template. ✓<u>Identify Service Profile</u> Template You can select a server pool you want to associate with this service profile template. 2. VNetworking 3. √<u>Storage</u> ✓<u>Zoning</u> 🕂 Create Server Pool Pool Assignment: VSPEX-Servers -5. √<u>vNIC/vHBA Placement</u> 6. √<u>Server Boot Order</u> Select the power state to be applied when this 7. √<u>Maintenance Policy</u> profile is associated with the server. 8. VServer Assignment 💿 Up 🕥 Down 9. Operational Policies The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list. Server Pool Qualification: <not set> -Restrict Migration:

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

Figure 107 Creating Service Profile Template - Restore Default Settings for Operational Policy

Create Service Profile Template	omputing System Manager	×
Create Service Profile Template 1. √Identify Service Profile	Operational Policies Optionally specify information that affects how the system operates.	0
2. √ <u>Networking</u>	BIOS Configuration	8
3. √ <u>Storage</u> 4. √ <u>Zoning</u>	External IPMI Management Configuration	8
5. √ <u>vNIC/vHBA Placement</u> 6. √ <u>Server Boot Order</u>	Management IP Address	۲
7. ✓ <u>Maintenance Policy</u>	Monitoring Configuration (Thresholds)	8
<ol> <li>✓ <u>Server Assignment</u></li> <li>✓ <u>Operational Policies</u></li> </ol>	Power Control Policy Configuration	8
	Scrub Policy	8
	<prev next=""> Finish</prev>	Cancel

I

# Instantiate Service Profiles from the Service Profile Template

As a final step to configure UCS Manager, we need to instantiate service profiles from the service profile template created in "Configure Service Profile Template" section on page 91. Follow these steps to instantiate service profiles from the service profile template:

 From the Servers tab, expand Servers > Service profiles > root, and click the Create Service Profile from Template link in the right pane.



Figure 108 Creating Service Profile from Template

**2.** Providing the naming prefix, number of service profiles to be instantiated and choose the service profile template from the drop-down list. Refer to the sizing guidelines for the number of servers needed for your deployment.
A Create Service Profiles From Template	X
Create Service Profiles From Template	0
Naming Prefix: <b>VSPEX-Server</b> -	
Number: 4	
Service Profile Template: Service Template VSPEX-Service-Profile	
OK (	Cancel

#### Figure 109 Details for Creating Service Profiles

3. There are four service profiles are created in this example.

#### Figure 110 Window Showing All the Service Profiles Created from the Template



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

I



5. Eventually, all the four servers will be associated – you can see the summary by clicking **Servers** in the **Equipment** tab.





#### Figure 111 Status Details Of Service Profiles



We have not yet carved out specific data-store to install ESXi hypervisor OS image on the VNX storage array. We needed 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**

This section provides necessary steps to create FC accessible data-stores for the ESXi boot image per server basis. This can be done in three steps:

- 1. Configure Storage Pool, page 111
- 2. Register Hosts, page 114
- **3.** Configure Storage Groups, page 122

### **Configure Storage Pool**

To create storage pool and carve boot LUNs per server basis, follow these steps:

 Connect to EMC VNX Unisphere GUI, click the Storage tab. Choose Storage Configuration > Storage Pools. Click the Pools tab, in the Pools window, choose Create.

EMC Unisphere				_	Po	ool LUN	🖌 Sear	ch
< >	🔠 Dashboard	System	👕 Stora	ige 👔 H	losts 🛛 🧃	🖁 Data Prote	ection 🛛 🐐	Settings
<u>VNX5300-VSPEX</u> > <u>Storage</u> > <u>Storag</u>	<u>e Configuration</u> > Stora	age Pools						
Pools RAID Groups								
Pools							274.	<u>)</u>
Tilter for RAID	Type All 💌							
Name 🔺 FAST Cache State	RAID Type Drive Type	Total Capa	Free Capa	Allocated (	%Consum	Subscribed	%Subscrib	%Full
0 Selected Create Delete Pr	operties Defragmen	t						0 items

Figure 113 Creating Storage Pools in EMC Unisphere

2. Choose the RAID Configuration as RAID5 (4 + 1) from the drop-down list for performance. Click the **Manual** radio button, and click **Select** to manually select 5 SAS disks to create the storage pool.

Storage Pool Parame	eters -				
Storage Pool Type: 🚺	• Pool	RAID Group	,		
	Sched	luled Auto-Tie	ring		
Storage Pool ID:	3				~
Storage Pool Name:	Pool 3				
Extreme Performan					
RAID Configuration		umber of Flash	n Disks		
RAID5 (4+1)	✓ 0		~		
Performance					
RAID Configuration	Nu	mber of SAS	Disks		
RAID5 (4+1) Distribution Extreme Performance Performance	: 366.90	(Recommend 06 GB (12.03% 038 GB (87.97	6)		
Distribution Extreme Performance Performance Disks	: 366.90 : 2684.0	06 GB (12.03% 038 GB (87.97	6) %) ks		
Distribution Extreme Performance	: 366.90 : 2684.0	06 GB (12.03% 038 GB (87.97	6) %)	Total Raw Capacit	y: 3050.944
Distribution Extreme Performance Performance Disks	: 366.90 : 2684.0	06 GB (12.03% 038 GB (87.97	6) %) ks	Total Raw Capacit	y: 3050.944 State
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di	: 366.90 : 2684.0 wer Savin	06 GB (12.03%) 038 GB (87.97 038 GB (87.97 04 Eliaible Dis 04 Capacity 91.727 GB	6) %) <u>Select</u> Drive Type SATA Flash	Model SS160510 CL	State Unbound
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9	06 GB (12.03%) 038 GB (87.97 Dag Eligible Dis Capacity 91.727 GB 91.727 GB	6) %) <u>Select</u> Drive Type SATA Flash SATA Flash	Model SS160510 CL SS160510 CL	State Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8	06 GB (12.03%) 038 GB (87.97 038 GB (87.97 04 Eliaible Dis 05 05 05 05 05 05 05 05 05 05 05 05 05	6) %) Select Drive Type SATA Flash SATA Flash SATA Flash SATA Flash	Model SS160510 CL SS160510 CL SS160510 CL	State Unbound Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Por Manual Disk Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8 isk 7	06 GB (12.039) 038 GB (87.97 038 GB (87.97 04 Eligible Dis 05 05 05 05 05 05 05 05 05 05 05 05 05	6) %) Select Drive Type SATA Flash SATA Flash SATA Flash SATA Flash SATA Flash	Model SS160510 CL SS160510 CL SS160510 CL SS160510 CL	State Unbound Unbound Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Por Manual Disk Bus 0 Enclosure 7 Di Bus 0 Enclosure 7 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8 isk 7 isk 6	Capacity 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB	6) %) <u>Select</u> Drive Type SATA Flash SATA Flash SATA Flash SATA Flash SATA Flash SAS	Model SS160510 CL SS160510 CL SS160510 CL SS160510 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di Bus 1 Enclosure 1 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8 isk 8 isk 8 isk 7 isk 6 isk 5	06 GB (12.03%) 038 GB (87.97) 038 GB (87.97) 04 Eliaible Dis 05 04 Eliaible Dis 05 04 Capacity 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 536.808 GB	6) %) <u>Select</u> Drive Type SATA Flash SATA Flash SATA Flash SATA Flash SATA Flash SAS SAS	Model SS160510 CL SS160510 CL SS160510 CL SS160510 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di Bus 1 Enclosure 1 Di Bus 1 Enclosure 1 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8 isk 7 isk 6 isk 7 isk 6 isk 5 isk 4	06 GB (12.03%) 038 GB (87.97) 038 GB (87.97) 04 Eliaible Dis Capacity 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 536.808 GB 536.808 GB	6) %) Select Drive Type SATA Flash SATA Flash SATA Flash SATA Flash SATA Flash SAS SAS SAS	Model SS160510 CL SS160510 CL SS160510 CL SS160510 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound
Distribution Extreme Performance Performance Disks Automatic Use Pou Manual Disk Bus 0 Enclosure 7 Di Bus 1 Enclosure 1 Di	: 366.90 : 2684.0 wer Savin isk 10 isk 9 isk 8 isk 7 isk 6 isk 5 isk 4 isk 3	06 GB (12.03%) 038 GB (87.97) 038 GB (87.97) 04 Eliaible Dis 05 04 Eliaible Dis 05 04 Capacity 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 91.727 GB 536.808 GB	6) %) <u>Select</u> Drive Type SATA Flash SATA Flash SATA Flash SATA Flash SATA Flash SAS SAS	Model SS160510 CL SS160510 CL SS160510 CL SS160510 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound Unbound

1

Figure 114 Details for Creating Storage Pools

3. From the newly created RAID group, right-click and choose Create LUN.

Pools											2	74.3	Ģ
Y, Filte	er for	RA	ID Type All	*									
Name 🔺	FAST Cache	State	RAID Type	Drive Type	Total Capa	Free Capa	Allocated (	%Consum	Subscribed	%Subscrib	%Full Thre	Auto-Tierin.	.M
🎁 Pool O	On	Ready	RAID5	SAS	2146 434 Create LU		374.229		1,156.755	53.892	70	Scheduled	
					Expand								
					Delete								
					Analyzer	>	1						
					<u>A</u> uto-Tieri	ng >							
					Properties								
<													

### Figure 115 Creating LUN from Created RAID Group

4. Choose 5 for Number of LUNs to create, with 50 GB User Capacity each. Make sure the **thin provisioning** check box is checked.

	Pool      RAID Group				
Storage Pool Type:					
RAID Type:	RAID5: Distributed Parity (High Throughput)				
Storage Pool for new LUN:	Pool 0 <u>N</u> ew				
✓ Thin User Capacity 50	GB				
LUN ID: 0	Number of LUNs to create: 5				
LUN Name					
LUN Name       Name					
-	0				
O Name					

### Figure 116 Details for Creating LUN

ſ

#### **Register Hosts**

After the service profiles are associated in UCS Manager, the vHBAs will do flogi in the network and the SAN initiators will be identified by the VNX storage array. To register the hosts identified by the WWPN of the server, follow these steps:

(NFS-variant only) For NFS-variant of the solution, the storage connectivity is through Nexus 5000 switches. In that case, the FC zoning must be configured manually on Nexus 5548UP switches. In contrast to this, in case of FC-variant architecture, where storage is attached to FIs, FC zoning is taken care by UCS Manager implicitly.

To configure zoning on Nexus 5548 UP switches, follow these steps:

1. Login to the Nexus 5548UP switch A and configure a zoneset for SAN fabric A. You need to create one zone for each ESXi host, containing WWPN of SP-A and SP-B of VNX storage and WWPN of the vHBA on fabric A of the ESXi server. WWPN list is available from UCS Manager as shown in step 7. Entire zoneset configuration looks like Figure 117. Activate the zoneset in the storage VSAN after the zoneset is configured completely.

Figure 117 Zoneset Configuration on Cisco Nexus 5548UP Switch

UCS-N5k-Fabl# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UCS-N5k-Fabl(config)# zoneset name V250-Fabric-A vsan 10
UCS-N5k-FabA(config-zoneset)# zone name V250-ESXHost1-fc0
UCS-N5k-Fabk(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:0e
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabl(config-zoneset) # zone name V250-ESXHost2-fc0
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:1d
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02 UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabk(config-zoneset)# zone name V250-ESXHost3-fc0
UCS-NSk-FabA(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:1c
UCS-N5k-Fabk(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabk(config-zoneset-zone)# exit
UCS-N5k-FabA(config-zoneset)# zone name V250-ESXHost4-fc0
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:1b
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabl(config-zoneset) # zone name V250-ESXHost5-fc0
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:1a
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabl(config-zoneset) # zone name V250-ESXHost6-fc0
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:09
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabl(config-zoneset)# zone name V250-ESXHost7-fc0
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:08
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabl(config-zoneset) # zone name V250-ESXHost8-fc0
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:07 UCS-N5k-FabA(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02 UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabk(config-zoneset)# zone name V250-ESXHost9-fc0
UCS-N5k-Fabk(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:06
UCS-N5k-Fabk(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-FabA(config-zoneset-zone) # exit
UCS-N5k-Fabk(config-zoneset) # zone name V250-ESXHost10-fc0
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 20:00:00:25:b5:66:dd:05
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 50:06:01:64:3e:a0:52:02
UCS-N5k-FabA(config-zoneset-zone)# member pwwn 50:06:01:6c:3e:a0:52:02
UCS-N5k-Fabl(config-zoneset-zone)# exit
UCS-N5k-Fabk(config-zoneset)# exit
UCS-N5k-Fabl(config)# zoneset activate name V250-Fabric-1 vsan 10
Zoneset activation initiated. check zone status
UCS-N5k-Fabl(config)#

**2.** (NFS-variant only) Validate the successful activation of zoneset by issuing **show zoneset brief** command.

Γ

UCS-N5k-FabA# show zoneset brief
zoneset name V250-Fabric-A vsan 10
zone V250-ESXHost1-fc0
zone V250-ESXHost2-fc0
zone V250-ESXHost3-fc0
zone V250-ESXHost4-fc0
zone V250-ESXHost5-fc0
zone V250-ESXHost6-fc0
zone V250-ESXHost7-fc0
zone V250-ESXHost8-fc0
zone V250-ESXHost9-fc0
zone V250-ESXHost10-fc0
UCS-N5k-FabA#

Figure 118 Running show zoneset brief Command for Fabric A

**3.** (NFS-variant only) Similarly, on Nexus 5548UP switch B, create a zoneset for fabric B and include vHBAs on fabric B on the servers. Zoneset on fabric B looks like Figure 119.





4. (NFS-variant only) To further validate zoneset configuration across entire SAN fabric, SSH to UCS FI-A, issue connect nxos command, and run show npv flogi-table. It should list all ten FLogI sessions, one from each vHBA on fabric A in storage VSAN.

TAC support: Copyright (c) The copyright owned by othe license. Cert the GNU Gener Lesser Genera such license http://www.op http://www.op	perating Sy http://www. 2002-2012/ s to certa: r third par ain compone al Public I l Public L: is availab! ensource.or ensource.or	ystem (NX-OS) Software .cisco.com/tac , Cisco Systems, Inc. Al. in works contained in th: cties and used and distr ents of this software are License (GPL) version 2.0 icense (LGPL) Version 2.0	is software are ibuted under e licensed under ) or the GNU 1. A copy of each	
SERVER INTERFACE VSA E	N FCID	PORT NAME	NODE NAME	EXTERNAL INTERFAC
vfc769 10 vfc823 10 vfc877 10 vfc931 10 vfc1011 10 vfc1065 10 vfc1119 10 vfc1173 10 vfc1227 10 vfc1281 10 Total number V250-UCS-Å(nx	0x5c0003 0x5c0004 0x5c0005 0x5c0006 0x5c0007 0x5c0009 0x5c0008 0x5c0008 0x5c000b of flogi =	20:00:00:25:b5:66:dd:1d 20:00:00:25:b5:66:dd:1c 20:00:00:25:b5:66:dd:1b 20:00:00:25:b5:66:dd:06 20:00:00:25:b5:66:dd:07 20:00:00:25:b5:66:dd:08 20:00:00:25:b5:66:dd:09 20:00:00:25:b5:66:dd:05 20:00:00:25:b5:66:dd:1a	20:00:00:25:b5:60:0d:0e 20:00:00:25:b5:60:0d:0d 20:00:00:25:b5:60:0d:0c 20:00:00:25:b5:60:0d:0b 20:00:00:25:b5:60:0d:06 20:00:00:25:b5:60:0d:07 20:00:00:25:b5:60:0d:08 20:00:00:25:b5:60:0d:08 20:00:00:25:b5:60:0d:08 20:00:00:25:b5:60:0d:08	fc2/2 fc2/1 fc2/2 fc2/1 fc2/1 fc2/1 fc2/2 fc2/2 fc2/2 fc2/1

Figure 120 Running show nvp flogi-table to List All the FLogI Sessions

**5.** (NFS-variant only) Similarly, the **show flogi database** command on Nexus 5548UP switch should show 14 FLogI sessions: 10 from B200 M3 vHBAs, 2 from FI-A's FC ports, and 2 from VNX storage array's SP-A and SP-B FC ports. Similarly, verify the FLogI entries on SAN fabric B.

Γ

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
c1/29	 10	0x5c0000	20:41:00:0d:ec:f7:04:00	20:0a:00:0d:ec:f7:04:
c1/29	10	0x5c0002	20:00:00:25:b5:66:dd:0e	20:00:00:25:b5:60:0d:
c1/29	10	0x5c0004	20:00:00:25:b5:66:dd:1c	20:00:00:25:b5:60:0d:
c1/29	10	0x5c0006	20:00:00:25:b5:66:dd:06	20:00:00:25:b5:60:0d:
c1/29	10	0x5c0007	20:00:00:25:b5:66:dd:07	20:00:00:25:b5:60:0d:
c1/29	10	0x5c000a	20:00:00:25:b5:66:dd:05	20:00:00:25:b5:60:0d:
c1/30	10	0x5c0001	20:42:00:0d:ec:f7:04:00	20:0a:00:0d:ec:f7:04:
c1/30	10	0x5c0003	20:00:00:25:b5:66:dd:1d	20:00:00:25:b5:60:0d:
c1/30	10	0x5c0005	20:00:00:25:b5:66:dd:1b	20:00:00:25:b5:60:0d:
c1/30	10	0x5c0008	20:00:00:25:b5:66:dd:09	20:00:00:25:b5:60:0d:
c1/30	10	0x5c0009	20:00:00:25:b5:66:dd:08	20:00:00:25:b5:60:0d:
c1/30	10	0x5c000b	20:00:00:25:b5:66:dd:1a	20:00:00:25:b5:60:0d:
c1/31	10	0x5c00ef	50:06:01:64:3e:a0:52:02	50:06:01:60:be:a0:52:
c1/32	10	0x5c01ef	50:06:01:6c:3e:a0:52:02	50:06:01:60:be:a0:52:

Figure 121 Running show flogi database Command on Cisco Nexus 5548UP

1

6. In the Unisphere GUI, click the **Hosts** tab, and click **Initiators**. Choose the first unregistered initiator and click **Register**.

the late of the										
Initiators										274, 🝺
Y, Fi	Iter for Connection Status All	~								
Status	Initiator Name	▼ SP Port	Host N	Host I	Storag	Regist	Logge	Failov	Туре	Protocol Attrib
<ul> <li></li> </ul>	50:06:01:60:C7:20:35:8C:50:06:01:69:47:20:35:8C	B-2	Celer	10.65	~filest	Yes	Yes	4	Host	Fibre
×	50:06:01:60:C7:20:35:8C:50:06:01:68:47:20:35:8C	A-2	Celer	10.65	~filest	Yes	Yes	4	Host	Fibre
<ul> <li></li> </ul>	50:06:01:60:C7:20:35:8C:50:06:01:61:47:20:35:8C	B-3	Celer	10.65	~filest	Yes	Yes	4	Host	Fibre
<u> </u>	50:06:01:60:C7:20:35:8C:50:06:01:60:47:20:35:8C	A-3	Celer	10.65	~filest	Yes	Yes	4	Host	Fibre
<u>^</u>	20:00:00:25:B5:60:0D:5C:20:00:00:25:B5:60:0D:5E	A-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:85:60:0D:5C:20:00:00:25:85:60:0D:5D	B-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:4C:20:00:00:25:B5:60:0D:4E	A-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:4C:20:00:00:25:B5:60:0D:4D	B-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:3C:20:00:00:25:B5:60:0D:3E	A-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:3C:20:00:00:25:B5:60:0D:3D	B-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
<u> </u>	20:00:00:25:B5:60:0D:2C:20:00:00:25:B5:60:0D:2E	A-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:2C:20:00:00:25:B5:60:0D:2D	B-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
<u> </u>	20:00:00:25:85:60:0D:0C:20:00:00:25:85:60:0D:0E	A-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre
4	20:00:00:25:B5:60:0D:0C:20:00:00:25:B5:60:0D:0D	B-4	UNKN	UNKN	~man	No	Yes	4	Host	Fibre

From the UCS Manager GUI, click the Servers tab, expand Servers > Service Profiles > root > Service profile (a specific service-profile), and click vHBAs. This will list the WWPN identities. Using this IDs, you can associate WWPN to the server.



#### Figure 123 WWPN Identities of vHBAs in Cisco UCS Manager GUI

8. In the Register Initiator Record wizard, choose the Initiator Type as **CLARiiON/VNX** and Failover Mode as **failovermode 4** from the drop-down lists respectively. Click the **New Host** radio button, enter the hostname and (future) management IP address of the host. Click **OK**.

I

Figure 124

Initiator Information WWN/IQN: 20:00:00:25:85:60:0D:4C:20:00:00:25:	85:60:0D:4E
SP - port: A-4 (Fibre)	
nitiator Type: CLARiiON/VNX 🛛 🗹	ailover Mode: //e-Active mode(ALUA)-failovermode 4
Host Agent Information	Existing Host     Selected Host
Host Name: VSPEX-Server-1 P Address: 10.65.121.239	Browse Host

**Registering Initiator Record - Part 1** 

**9.** Choose the second vHBA's WWPN from the same server, click **Register** and now, click the **Existing Host** radio button. Click **Browse Host** to manually select the host.

1

1

Figure 125 Registering Initiator Record - Part 2

Register Initiator Record	ALL CAMPA-	-	-		-	×
Initiator Information       WWN/IQN:       20:00:00:25:8       SP - port:       B-4 (Fibre)		0:25:85:60:0D:4D				
Initiator Type: CLARiiO Host Agent Informati New Host Host Name:		Failover Mod	e: /e-Active m Existing Ho: Browse Host	st ]	)-failovermo	
IP Address:				<u>о</u> к	<u>C</u> ancel	Help

**10.** Choose the previously registered host, and click **OK**.

	VNX5300-VSPEX - Con	nectivity status		
	Host Name	IP Address	OS Name	
	20:00:00:25:B5:6		Unknown VNX On	
٢	VSPEX-Server-1	10.65.121.239	Unknown	
			<u>O</u> K <u>C</u> ance	l <u>H</u> elp

Figure 126 Choosing Registered Host for EMC VNX Connectivity

11. Repeat these steps for all the servers in the group. End result looks like Figure 127.

Figure 127 Initiator Window Showing All the Hosts with Initiator Names

EMC Un	isphere						Poo	LUN		▼ Se	arch		Advanced 👾 🍹
< >	↑ 🗊 VNX5300-VSPEX 🗹 🔠 Dashboard 📲	System	🗊 Storage 📲		losts		Data P	otectio	n 🦸	💲 Set	tings	👩 Supp	and a second
<u>VNX5300</u>	<u> -VSPEX</u> > <u>Hosts</u> > Initiators												
Initiators	1									3	72.	0	Wizards
Ϋ.	Filter for Connection Status All	~											Storage Assignment Wizard for Blo
Status	Initiator Name	SP Port	Host Name	*	Host	Stora	Regi	Logg	Failo	Туре	Proto	Attri	Hypervisor Information Configuration Failover Wizard
<ul> <li>Image: A second s</li></ul>	50:06:01:60:C7:20:35:8C:50:06:01:69:47:20:35:8C	B-2	Celerra_VNX5300		10.6	~file	Yes	Yes	4	Host	Fibre		
<b>~</b>	50:06:01:60:C7:20:35:8C:50:06:01:60:47:20:35:8C	A-3	Celerra_VNX5300		10.6	~file	Yes	Yes	4	Host	Fibre		Host Management
<ul> <li>Image: A second s</li></ul>	50:06:01:60:C7:20:35:8C:50:06:01:68:47:20:35:8C	A-2	Celerra_VNX5300		10.6	~file	Yes	Yes	4	Host	Fibre		Allocate LUNs for File Storage
<u> </u>	50:06:01:60:C7:20:35:8C:50:06:01:61:47:20:35:8C	B-3	Celerra VNX5300	-	10.6	~file	Yes	Yes	4	Host	Fibre		Connect Host
1	20:00:00:25:B5:60:0D:4C:20:00:00:25:B5:60:0D:4E	A-4	VSPEX-Server-1	-)	10.6	~ma	Yes	Yes	4	Host	Fibre		Update All Hosts
1	20:00:00:25:B5:60:0D:4C:20:00:00:25:B5:60:0D:4D	B-4	VSPEX-Server-1		10.6	~ma	Yes	Yes	4	Host	Fibre		
<u> </u>	20:00:00:25:B5:60:0D:5C:20:00:00:25:B5:60:0D:5D	B-4	VSPEX-Server-2		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:B5:60:0D:5C:20:00:00:25:B5:60:0D:5E	A-4	VSPEX-Server-2		10.6	~ma	Yes	Yes	4	Host	Fibre		
1	20:00:00:25:B5:60:0D:2C:20:00:00:25:B5:60:0D:2E	A-4	VSPEX-Server-3		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:B5:60:0D:2C:20:00:00:25:B5:60:0D:2D	B-4	VSPEX-Server-3		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:B5:60:0D:3C:20:00:00:25:B5:60:0D:3E	A-4	VSPEX-Server-4		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:B5:60:0D:3C:20:00:00:25:B5:60:0D:3D	B-4	VSPEX-Server-4		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:B5:60:0D:0C:20:00:00:25:B5:60:0D:0E	A-4	VSPEX-Server-5		10.6	~ma	Yes	Yes	4	Host	Fibre		
4	20:00:00:25:85:60:0D:0C:20:00:00:25:85:60:0D:0D	B-4	VSPEX-Server-5		10.6	~ma	Yes	Yes	4	Host	Fibre		

ſ

#### **Configure Storage Groups**

At this point, hosts as well as the LUNs are created on the VNX storage array, we need to create storage groups to assign access to LUNs for various hosts. A Boot LUN will be dedicated to a specific server. Follow these steps to configure storage groups:

1

1. Click the **Hosts** tab in the EMC Unisphere GUI, click **Storage Groups**. Click **Create** to create a new storage group.

#### Figure 128 Creating a Storage Group

EMC Unisphere	Pool LUN Search
< > 🁔 🗊 VNX5300-VSPEX 🗹 🔠 Dashboard 📲 System	🗊 Storage 📕 Hosts 👔 Data Protection 🏾 🌼 Settings 🛛 📀 St
<u>VNX5300-VSPEX</u> > <u>Hosts</u> > Storage Groups	
Storage Groups	S 😵 🔧 📴
Filter for	
Storage Group Name	WWN
Arilestorage	60:06:01:60:00:00:00:00:00:00:00:00:00:00:00:00:
0 Selected Create Delete Properties Connect LUNs Connect	osts 1 items

2. Enter a name to the storage group name in the Name field.

Figure 129	Name the Storage	e Group
------------	------------------	---------

📴 VNX5400-VSPEX - Cre	ate Storage Group 🛛 🗖 🗙					
Storage System:	VNX5400-VSPEX					
Storage Group Name:	VSPEX-Server-1					
<u>O</u> K <u>A</u> ppl	y <u>C</u> ancel <u>H</u> elp					

**3.** You will see the success message after the creation of new storage group. The system prompts to create LUNs and connect hosts. Click **Yes**.

	Figure 130	Successful Com	pletion of Storage	group Creation
--	------------	----------------	--------------------	----------------

🚑 Con	firm: VNX5300-VSPEX - Create Storage Group
2	Results from call to create storage group:Success
	Do you wish to add LUNs or connect hosts?
	Do you wish to continue?
	Yes No

4. From the LUNs tab, select a LUN and click Add.

Show LUNs: Not Available LUNs Name MetaLUNs	in other Storage (		pacity	Drive Type	^
		50			
	0		.000 GB	SAS	
	2		.000 GB	SAS	
- S LUN 3	3		.000 GB	SAS	~
Selected LUNs	ID	Capacity	Drive Typ	e Host LL	IN ID
Name					
nane					<u>R</u> emove

#### Figure 131 Adding LUNs to the Storage Group

5. Click the **Hosts** tab, and choose a server to add on the storage group. Click **OK** to deploy the storage group.

Γ

VNX5300-VSPEX - VSPE General LUNs Host		age Group Proper	ties		X
Show Hosts: Not con Select Hosts Filter For:	nnected 💌				
Available Hosts			Hosts to be Connect	ed	
Name	IP Address OS	Туре	Name	IP Address OS	Туре
VSPEX-Server-2 VSPEX-Server-5 VSPEX-Server-3 VSPEX-Server-4 VSPEX-Server-1	10.65.12 10.65.12 10.65.12	Fibre Fibre Fibre	)		
< : <u>R</u> efresh	:	>	٢	#	>
			<u>O</u> K <u>Apply</u>	Cancel	Help

Figure 132 Adding Host to the Storage Group

6.Repeat these steps for all the five servers. The end result looks like Figure 133.

#### Figure 133 Storage Group Showing All the Servers Added

Now, we have end-to-end FC storage access from servers in UCS to the specific boot LUN on the VNX storage devices. We are ready to install ESXi images on the server.

# Install ESXi Servers and vCenter Infrastructure

Follow these steps to install ESXi image on Cisco UCS servers:

1. From UCS Manager GUI, click the **Servers** tab, expand **Servers** > **Service Profiles** > **root**, and select a particular service profile. Click KVM Console in the right pane of the window.



2. Once the Java pallet of KVM is launched, click the Virtual Media tab and click Add Image. A window appears to select an ISO image. Browse through the local directory structure and select ISO image of the ESXi 5.1 hypervisor installer media.

#### Cisco Virtualization Solution for EMC VSPEX with VMware vSphere 5.1 Solution for up to 1000 Virtual Machines

I

Help Boot Server 🛛 🛃 S	Shutdown Se	rver 🧕 Reset					
Console Propert	ies						
Virtual Media							
lient View							
Mapped	Read Only	Drive				Γ	Exit
		🚽 A: - Floppy				1	Create Image
	V	🙆 D: - CD/DVD				ſ	Add Image
							Remove Image
						Î	Details <b>±</b>
ails							
arget Drive	Mapped	То	Read Bytes	Write Bytes	Duration		
rtual CD/DVD	Not map	ped					USB Reset
emovable Disk	Not map	ped					

# Figure 135 Adding an ISO Image of the ESXi 5.1 Hypervisor Installer Media

1

**3.** When the ISO image shows up in the list, check the Mapped check box and click **Reset** to reset the server.

/ VSPEX-Server-1 le Help Boot Server 📑 S	(Rack -4) - KVM Console	<u>ר</u>				
VM Console Properti	es	<i>,</i>				
VM Virtual Media						
Client View						
Mapped F	Read Only Drive					Exit
	🗖 🛛 🛃 A: - Floppy					Create Image
	🗹 🛛 🖄 D: - CD/DVD					
	🔽 🛃 Y:\ISO\VMw	are\ESXI5.1\RTM79	9733\VMware-Vi	Mvisor-Installer-5.1.0	-799733.x86_64.iso	Add Image
						Remove Image
						Details ±
1						
					<u> </u>	
Details						
Target Drive	Mapped To	Road Bytes	Write Bytes	Duration	<u></u>	
Virtual CD/DVD	P:\ISO\VMware\ESXi5	.1 0	0	00:00:14		USB Reset
Removable Disk	Not mapped				_	
Floppy	Not mapped					

## Figure 136 Mapping the ISO Image and Resetting the Server

4. Click **OK** in the Reset Server warning message window.



Reset Se	erver 🛛 🔀
	You have selected the <b>Reset</b> 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 <b>Cancel</b> then select the <b>Boot Server</b> action. If you are certain that you want to continue with the <b>Reset</b> operation, click <b>OK</b> .
	Cancel

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

Γ

Figure 138	Selecting Resetting Option
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 C 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

6. Click the **KVM** tab to see how ESXi boot media is booted from the virtual CD-ROM drive.

At this point of time, ESXi installation media would boot from the virtual disk mounted on the KVM. Follow the steps to install ESXi 5.1 hypervisor on the boot LUN. Make sure that you select the boot LUN and not the local disk. You can select all the default parameters or parameters settings as per your requirements.

1

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

#### Figure 139 Selecting Adapters for Default Management Network Connection

🌲 / VSPEX-Server-3 (Rack -2) - KVM	1 Console	
File View Macros Tools Help		
📣 Boot Server 🛛 🔩 Shutdown Server	S Reset	
KVM Console Properties		
KVM Virtual Media		
Configure Management N	ietwork Network	Adapters
Network Adapters VLAN (optional)	vmic0 (	90:25:b5:60:0d:07)
IP Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	connectio are used	ters listed here provide the default network on to and from this host. When two or more adapters , connections will be fault-tolerant and outgoing will be load-balanced.
	Network Adapters Select the adapters for this host's default man connection. Use two or more adapters for fault load-balancing.	
	Device Hune         Hur due c         Lubri (MA hdd cool)           [X] venic0         N/A (00:25:b5:60:0d:07)           [X] venic1         N/A (00:25:b5:60:0d:17)           [J] venic2         N/A (00:25:b5:60:0d:18)           [] venic3         N/A (00:25:b5:60:0d:18)           [] venic3         N/A (00:25:b5:60:0d:18)           [] venic3         N/A (00:25:b5:60:0d:16)	Connected () Connected Connected Connected Connected Connected Connected Connected Connected Connected
	<pre><b>CD&gt;</b> View Details <b><space></space></b> Toggle Selected</pre>	<pre><enter> OK <esc> Cance1</esc></enter></pre>



ſ

Easiest way to figure out which vmnic adapter should be used for the vSphere management purpose, you can identify the vmnic by MAC address. The MAC addresses of the vNICs (vmnic's) are summarized in UCS Manager GUI as show in Figure 140. Click the **Servers** tab, expand **Servers** > **Service Profiles** > **root**, and select a particular service profile and click **vNICs**. The vNIC names and MAC addresses are listed in the right pane of the window.

Cisco Unified Computing System Manager - VSPEX-F	L							_ 0
Fault Summary	🕄 🏐 🗳 Ne	w 👻 🛃 Options 🛛 🚱 🛛	🛚 🛛 🛆 Pending Ar	tivities 0 Exit				
	>> Servers	Service Profiles * 🙏 ro	ot 🕴 🚟 Service Pro	file VSPEX-Server-3			-	
Equipmen: Servers AN SAN VM Admin	Network FSM	m			-			
Filter: All	Actions		Dynamic	vNIC Connection I	Policy			
± =	😷 Change	Dynamic vNIC Connection Poli	cy Nothing	Selected				
E	📜 🦉 Modify v	NIC/vHBA Placement		BA Placement Poli				
🖃 🚚 Service Profiles					-7			
⊡ - A root			Nothing	Selected				
VSPEX-Server-1			LAN Con	ectivity Policy				
E SPEX-Server-3								
				LAN Connectivity Poli		-		
				ectivity Policy Instan				
			+ Crea	te LAN Connectivity P	Policy			
·····································								
	VNICS							
III VIIC ISCSI-Overlay-B	🛃 Filter 👄 Exp	oort 🖂 Print						
		1.4-				1		
	Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Ę
SPEX-Server-4	- VNIC data-A			5	A	Any	1	-
Sub-Organizations     Service Profile Templates	- VNIC data-B			6	B	Any	1	
Policies		Dv 00:25:85:60:0D:08 3		3	A	Any	1	_
		00-25-85-60-00-18 4	· · · · ·	4	8	Any	1	
Schedules		A 00:25:85:60:0D:07 1		1	A	Any	1	_
_	-I vNIC system	-B 00:25:85:60:0D:17 2		2	В	Any	1	

Figure 140 vNIC Names and Their MAC Addresses are Shown in the vNICs Area

7. Repeat the ESXi installation steps for all the four servers.

# VMware vCenter Server Deployment

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

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

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

http://kb.vmware.com/selfservice/microsites/search.do?language=en\_US&cmd=displayKC&externalId =2032885

The following steps provide high level configuration procedure 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, then we need to directly connect 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. To ensure that adequate space is available on the vCenter and vSphere, Update Manager installation drive, see *vSphere Installation and Setup Guide*.

3. Install vCenter server

Install vCenter by using the VMware VIMSetup 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 VMware vCenter**

I

Follow these steps to configure cluster, HA, and DRS on 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.** Check the check boxes Turn On vShpere HA and Turn On vSphere DRS, as shown in Figure 141.
  - c. Click OK, to save changes.

Prew Cluster Wizard Cluster Features What features do you want	to enable for this cluster?
Cluster Features vSphere DRS Power Management vSphere HA Virtual Machine Options VM Monitoring VMware EVC VM Swapfile Location Ready to Complete	Name         VSPEX-Cluster         Cluster Features         Select the features you would like to use with this cluster.         ✓         Turn On vSphere HA         vSphere HA detects failures and provides rapid recovery for the virtual machines running within a cluster. 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, groups, and virtual machines.         vSphere DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies.         vSphere DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing.
Help	≤Back Next ≥ Cancel

1

Figure 141 Configuring HA and DRS on Cluster

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

🛃 ¥SPEX - vSphere Client							
File Edit View Inventory Administra	ation Plug-ins Help						
💽 💽 🏠 Home 🕨 🛃 Inve	ventory 👂 🎁 Hosts and C	lusters				Search Inventory	Q
II & & II & N	4						
- 🚱 VSPEX	VSPEX-Cluster						
VSPEX-DC  VSPEX-Cluster	Getting Started Summa	ry Virtual Machines	Hosts DRS	Resource Allocation	Performance Tas	sks & Events 🛛 Alarms 🔪 Permissio	ns Maps F 🕁 🕨
10.65.121.231 10.65.121.232					Nam	e or State contains: 👻	Clear
10.65.121.233	Name	State	Status	% CPU	% Memory	Memory Size C	PU Count   1
10.65.121.234	10.65.121.233	Connected	🔔 Warning	0	1	262084.60 MB	2
	10.65.121.234	Connected	🔔 Warning	0	1	262084.60 MB	2
	10.65.121.232	Connected	🔔 Warning	0	1	262084.40 MB	2
	10.65.121.231	Connected	🤼 Warning	0	1	262084.50 MB	2
	•						•
🚰 Tasks 🞯 Alarms					E	Evaluation Mode: 45 days remaining	Administrator //

Figure 142 Adding ESXi Hosts to the Cluster

# **Virtual Networking Configuration**

I

In UCS Manager service profile, we created six vNICs per server for NFS-variant and four vNICs per server for FC-variant. This shows up as six or four network adapters or vmnics in ESXi server. You can see these adapters in the vCenter by choosing **Home > Inventory > Hosts and Clusters**, select a particular server, click the **Configuration** tab in the right pane of the window, and click **Network Adapters**.

VSPEX - vSphere Client							
File Edit View Inventory Administra	ition Plug-ins Help						
🖸 🔝 🏠 Home 🕨 🛃 Inve	entory 🔹 🛐 Hosts and	Clusters				🖅 🔹 Search Invent	ory 🤇
II	۹.						
B 🚱 VSPEX	VSPEX-Cluster						
VSPEX-DC     VSPEX-Cluster	Getting Started Summ	ary Virtual Mach	ines Hosts DRS	Resource Allocation	Performance Tasks	& Events Alarms Per	rmissions Maps F d
10.65.121.231 10.65.121.232					Name o	r State contains: +	Clear
10.65.121.233	Name	State	Status	% CPU	% Memory	Memory Size	CPU Count
10.65.121.234	10.65.121.233	Connected	🔥 Warning	0	1	262084.60 MB	2
	10.65.121.234	Connected	🔔 Warning	0	1	262084.60 MB	2
	10.65.121.232	Connected	🔥 Warning	0	1	262084.40 MB	2
	10.65.121.231	Connected	🔼 Warning	0	1	262084.50 MB	2
	•						
🗂 Tasks 🙊 Alarms					Eva	aluation Mode: 45 days rem	aining Administrator

Figure 143 Network Adapter Showing vmnics in ESXi Server

1

Table 10 shows UCS Manager service profile and vSphere vmnic per ESXi host basis:

UCS Manager vNIC Names	vSphere VM NIC Names	MAC Address	Uplink Port-Profile*
System-A	vmnic0		system-uplink
System-B	vmnic1		system-uplink
Storage-A*	vmnic2		storage-uplink
Storage-B*	vmnic3		storage-uplink
Data-A	vmnic4		data-uplink
Data-B	vmnic5		data-uplink

#### Table 10 Service Profile vNIC and vSphere vmnic Relations

\*Applicable for the NFS-variant of the solution only.

We are show casing two different approaches for the virtual networking layer of this architecture:

- 1. VMware vSphere native virtual switching in FC-variant of architecture
- 2. Cisco Nexus 1000v virtual switching in NFS-variant of architecture

Note

You can use either virtual switching strategy with any variant of architecture. This section focuses on the vSphere native virtual switching. See "Install and configure Nexus 1000v" section on page 149.

We need to create two native vSwitches for virtual network configuration as follows:

- 1. vSwitch0—Standard, default vSwitch for management and vMotion traffic.
- 2. vSwitch1—For VM data traffic.

Each vSwitch listed will have two vmnics, one on each fabric for load balancing and high-availability. Also, for vMotion, jumbo MTU needs to be configured in virtual network.

Follow these steps to configure the two vSwitches:

In the vSphere client, choose Home > Inventory > Hosts and Clusters. In the Hosts and Clusters window, click the Configuration tab on the right pane of the window. Click Networking in the Hardware area. Click Properties to see the details of vSwitch0.



Figure 144 Viewing Details of vSwitch0

2. Select vSwitch in the vSwitch0 Properties window, and click Edit.

Switch0 Properties			_ 🗆 X
Ports Network Adapters			
Configuration Summary	vSphere Standard Switch Properties		-
vSwitch 120 Ports	Number of Ports:	120	
VITUAL WALL AND A CONTRACT AND	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	<b>_</b>
		Close	Help

Figure 145 Editing vSwitch0 Properties

**3.** Click the **General** tab of the vSwitch0 Properties window, change the MTU in the Advanced Properties area to 9000.

Γ

Figure 146	Setting Jumbo MTU			
🚱 vSwitch0 Properti	es			×
VSphere Standard Number of Ports:	Traffic Shaping NIC Teaming Switch Properties 120 ot take effect until the system	•		
		ОК	Cancel	Help

1

4. Click the **NIC Teaming** tab in the vSwitch0 Properties window. Select the adapter under Standby Adapters and click **Move up** to get it under Active Adapters, and click **OK**.

oad Balancing.						
	p.	Route based on the orig	Route based on the originating virtual port ID			
Network Failov	er Detection:	Link status only				
Notify Switche	s:	Yes				
ailback:		Yes				
ailover Order	:					
vmnic0	10000 Full	10.65.121.1-10.65.121.127	Move Down			
Name	ate in the order	Networks	Move Up			
Active Adap		10.65.121.1-10.65.121.127	Move Down			
Standby Ad	anters					
wnnic1	10000 Full	10.65.121.1-10.65.121.127				
Unuseu aua						
Unused Ada	-					
Unused ada	•					
<b>Unused Ada</b> Adapter Deta	-					
-Adapter Deta	-	thernet NIC				
-Adapter Deta	ails	thernet NIC				
-Adapter Deta Cisco System	ails					
-Adapter Deta Cisco System Name:	ails	vmnic1				

Figure 147 Moving Standby Adapter to Active Adapter

I

Γ

5. In the vSwitch0 configuration window, click the **Ports** tab, and click **Add**.

ts Network Adapters				
Configuration	Summary	- VSphere Standard Switch Propertie		
🗊 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	

Figure 148 Adding Ports to vSwitch0

**6.** Click the **VMKernel** radio button in the Connection Types area and click **Next** in the Add Network Wizard window.

1

dd Network Wizard		_ 🗆
Connection Type Networking hardware c	an 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 > C	ancel

# Figure 149 Specifying Connection Type

7. Enter vMotion in the Network Label field. Choose the VLAN ID from the drop-down list. The standard vSwitch0 carries both management and vMotion VLANs. Management traffic leaves vSwitch0 untagged using the native VLAN of the vNIC. The vMotion traffic must be tagged with the appropriate VLAN ID. Check the Use this port group for vMotion check box.

ſ

VMkernel - Connection S Use network labels to ic	ettings lentify VMkernel connections while managing your hosts and datacenters.	
Connection Type Connection Settings IP Settings Summary	Port Group Properties Network Label: VLAN ID (Optional):  VLAN ID (Optional):  Use this port group for vMotion  Use this port group for Fault Tolerance logging  Use this port group for management traffic	
	Network Type:	
	VMkemel Port	
	vMotion  VLAN ID: 42 Virtual Machine Port Group	
	VM Network	
	fe80::225:b5ff:fe60:d04	

Figure 150 Specifying Port Group Properties for Setting VMkernel Connection

1

8. Configure IP address and subnet mask for the vmkernel interface. Click Next and deploy the vmkernel.

Add Network Wizard VMkernel - IP Connecti Specify VMkernel IP s		_ 🗆 >
Connection Type Connection Settings IP Settings Summary	<ul> <li>Obtain IP settings automatically</li> <li>Use the following IP settings:         <ul> <li>IP Address:</li> <li>Subnet Mask:</li> <li>VMkernel Default Gateway:</li> <li>I0 . 65 . 121 . 1</li> <li>Edit</li> </ul> </li> </ul>	
	Preview: VMkemel Port vMotion 10.42.42.104   VLAN ID: 42 Virtual Machine Port Group VM Network VMkemel Port Management Network vmk0 : 10.65.121.234 fe80::225:b5ff:fe60:d04	
Help	< Back Next > Ca	ncel

Figure 151 Specifying IP Address and Subnet Mask for Setting VMkernel Connection

I

Γ

9. In the vSwitch0 properties window, select the newly created vMotion port group and click Edit.

ts Network Adapters		Port Properties		
onfiguration	Summary	Network Label:	vMotion	
vSwitch	120 Ports	VLAN ID:		
VM Network VM Network VMotion	Virtual Machine vMotion and IP		42	
Managemeni: Net	vMotion and IP	vMotion:	Enabled	
	Without and IP	Fault Tolerance Logging:	Disabled	
		Management Traffic:	Disabled	
		iSCSI Port Binding:	Disabled	
		NIC Settings		
		MAC Address:	00:50:56:60:58:c1	
		MTU:	1500	
		- IP Settings		
		IP Address:	10.42.42.104	
		Subnet Mask:	255.255.255.0	
				View Routing Table
		Effective Policies		
		Security		
		Promiscuous Mode:	Reject	
		MAC Address Changes:	Accept	
Add	Edit Remove	1		
A00	Eult Kelliove	Forged Transmits:	Accept	

Figure 152 Editing vMotion vSwitch0 to Set Jumbo MTU

1

- 10. Set the MTU to 9000 and click OK. Click Close.
- **11.** Repeat steps 1 to 13 for all the 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 issuing ping with IP's don't fragment.
| ~ #<br>~ #  | ^   |
|---|-----|
| ~ #   |     |
| ~ #   |     |
| ~ #   |     |
| ~ # vmkping 10.42.42.101 -d -s 8972   |     |
| PING 10.42.42.101 (10.42.42.101): 8972 data bytes   |     |
| 8980 bytes from 10.42.42.101: icmp_seq=0 ttl=64 time=0.279 ms   |     |
| 8980 bytes from 10.42.42.101: icmp_seq=1 ttl=64 time=0.274 ms   |     |
| 8980 bytes from 10.42.42.101: icmp_seq=2 ttl=64 time=0.272 ms   |     |
| 10.42.42.101 ping statistics<br>3 packets transmitted, 3 packets received, 0% packet loss<br>round-trip min/avg/max = 0.272/0.275/0.279 ms<br>~ # vmkping 10.42.42.102 -d -s 8972<br>PING 10.42.42.102 (10.42.42.102): 8972 data bytes<br>8980 bytes from 10.42.42.102: icmp_seq=0 ttl=64 time=0.362 ms<br>8980 bytes from 10.42.42.102: icmp_seq=1 ttl=64 time=0.247 ms<br>8980 bytes from 10.42.42.102: icmp_seq=2 ttl=64 time=0.242 ms |     |
| 10.42.42.102 ping statistics<br>3 packets transmitted, 3 packets received, 0% packet loss<br>round-trip min/avg/max = 0.242/0.284/0.362 ms<br>~ #   | E F |

Figure 153 Pinging the VMKernel Port with Jumbo MTU

In the vCenter GUI, choose Home > Inventory > Hosts and Clusters. In the Hosts and Clusters window, click the Configuration tab on the right pane of the window. Click Networking in the Hardware area. Click Add Networking.

ſ

🚱 VSPEX - vSphere Client			
File Edit View Inventory Administra	tion Phys.inc Help		
🖸 🖸 🏠 Home 🕨 👸 Inv	entory 🕨 🎁 Hosts and Clusters		Search Inventory
5 6 8 8 9 9 4			
C P VSPEX	10.65.121.234 ¥Mware E5Xi, 5.1.0, 799	733   Evaluation (58 days remaining)	
VSPEX-DC      VSPEX-Cluster	Getting Started Summary Virtual Mach	ines Performance Configuration Tasks & Events Alarms Permissions Maps 5	torage Views 🛛 Hardware Status 🔍 Update Manager 🛛 🕁 🛛
10.65.121.231	Hardware	View: vSphere Standard Switch vSphere Distributed Switch	4
10.65.121.232 10.65.121.233			
10.65.121.235	Processors Memory	Networking	Refresh Add Networking Properties
	Storage		
	Networking	Standard Switch: vSwitch0 Remove Properties	
	Storage Adapters	Virtual Machine Port Group Physical Adapters	
	Network Adapters	VM Network 2 wmic1 10000 Full VM kernel Port	
	Advanced Settings	C Management Network	
	Power Management	vmk0:10.65.121.234	
	Software	fe80::225:b5ff:fe60:d04	
	Licensed Features		
	Time Configuration	Standard Switch: iScsiBootvSwitch Remove Properties	
	DNS and Routing	VMkernel Port Physical Adapters	
	Authentication Services	vmk1 : 192.168.100.78	
1	Power Management		
	Virtual Machine Startup/Shutdown Virtual Machine Swapfile Location		
	Security Profile		
	Host Cache Configuration		

1

Figure 154 Add Networking in VMware vSphere Client

13. Click the Virtual Machine radio button in the Add Networking Wizard, click Next.

### Figure 155 Specifying the Connection Type

I

Γ

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

14. Select the two vmnics corresponding to the VM-Data vNICs by checking the check boxes and click Next.

Connection Type	Select which vSphere standard switch will vSphere standard switch using the unclair		affic for this connection. You may also create a new listed below.
Connection Settings Summary	Create a vSphere standard swi	•	Networks
onnary	Cisco Systems Inc Cisco V. C E		
	🔽 📟 vmnic4	10000 Full	None
	Vmnic5	10000 Full	None
	C Use vSwitch0	Speed	Networks
	Cisco Systems Inc Cisco VIC E	thernet NIC	
	🕅 📟 vmnic1	10000 Full	10.65.121.1-10.65.121.127
	🗐 📟 vmnic0	10000 Full	10.65.121.1-10.65.121.127
		Sneed	Naturovice
	Preview:		
	Virtual Machine Port Group	Physical Adapters Physical Adapters Vmnic4 Vmnic5	

15. Enter VM-Data in the Network Label field, and keep VLAN ID as None (0) to signify absence of VLAN tag. Click Next.

1

Add Network Wizard Virtual Machines - Conne Use network labels to ic	ection Settings lentify migration compatible connections common to two or more hosts.
Connection Type Network Access Connection Settings Summary	Port Group Properties       Network Label:       VLAN ID (Optional):         None (0)
	Preview: Virtual Machine Port Group VM-Data VM-Data Vmric5
Help	< Back Next > Cancel

Figure 157 Specifying Port Group Properties

16. Repeat steps 15 to 18 for all the ESXi hosts in the cluster.

# **Install and configure Nexus 1000v**

ſ

Cisco Nexus 1000v is a Cisco's NX-OS based virtual switch that replaces the native vSwitch in the VMware ESXi hosts by a virtual Distributed Switch (vDS). The control plane of Nexus 1000v switch is installed in a VMware Virtual Machine, and is known as Virtual Switching Module (VSM). VSM virtual machine (VSM VM) is available as a VMware OVF template. Following are the major steps to deploy Nexus 1000v architecture:

- 1. Install Nexus 1000v VSM VM
- 2. Connect Nexus 1000v VSM to VMware vCenter
- 3. Configure port-profiles in VSM and migrate vCenter networking to vDS

# Install Nexus 1000v VSM VM

**OVF** Template Details

As mentioned before, the Nexus 1000v VSM VM installation media is available as VMware virtual machine OVF template. The VSM VM must be deployed on the infrastructure network, and not on one of the VSPEX ESXi servers. Follow these steps to install VSM VM:

From the Hosts and Cluster tab in vCenter, choose the infrastructure ESX/ESXi host and click File
 > Deploy new Virtual Machine through OVF template. Choose Nexus 1000v VSM OVF, and click Next.

Figure 158 Deploy OVF Template - Verifying OVF Template Details

-		
Source OVF Template Details End User License Agreement	Product:	Nexus1000V-4.2.1.5V2.2.1
Name and Location Deployment Configuration	Version:	4.2(1)5V2(2.1)
Storage Disk Format	Vendor:	Cisco Systems Inc
Network Mapping	Publisher:	No certificate present
Properties	Described stress	114 4 105
Ready to Complete	Download size:	116.6 MB
	Size on disk:	Unknown (thin provisioned) 3.0 GB (thick provisioned)
	Description:	Cisco Nexus 1000V Virtual Supervisor Module

2. Select the datacenter where you want to install the VSM in next page

🛃 Deploy OYF Template Name and Location Specify a name and location for the deployed template Source Name: **OVF Template Details** Nexus1000V-1780-Primary End User License Agreement The name can contain up to 80 characters and it must be unique within the inventory folder. Name and Location Deployment Configuration Host / Cluster Inventory Location: Resource Pool 🖃 🛃 VSPEX-Infra1.vspex.com Disk Format € SPEX-FC Properties VSPEX-Infra Ready to Complete VSPEX-NFS +

**Deploy OVF Template - Specifying Inventory Location** 

Figure 159

I

3. For Configuration field, choose Manually Configure Nexus 1000v from the drop-down list.

Figure 160 Deploy OVF Template - Choosing Deployment Configuration

Deploy OVF Template	
Deployment Configuration Select a deployment configura	ation.
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Storage Disk Format Network Mapping Properties Ready to Complete	Configuration: Manually Configure Nexus 1000V Use this deployment option to manually configure the Nexus 1000V VSM without the use of the installer application or OVF Properties. If this option is selected, please ignore the properties section ahead.

4. Choose the host on which you want to install the N1k VSM VM.

Figure 161	Deploy OVF Template - Choosing the Host
🛃 Deploy OVF Template	
Host / Cluster On which host or cluster do	you want to run the deployed template?
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Host / Cluster Specific Host Resource Pool Storage Disk Format Network Mapping Properties Ready to Complete	VSPEX-Infra  192.168.1.7

1

5. Choose the datastore where the VM should be deployed. Click Next.

F Template Details		_	age for the virtua	al machine files:				
d User License Agreement me and Location	-	orage Profile:					-	71:0
loyment Configuration	Nam		Drive Type Non-SSD		Provisioned 197.85 GB	Free 1.90 GB	Туре	Thin Pr
e		Datastore_Infr Datastore_Infr			45.06 GB	4.69 GB		Suppor
at Japping		Datastore_Te	Non-SSD		239.67 GB	92.09 GB		Suppor
bing		datastore1	Non-SSD		971.00 MB	44.05 GB		Suppor
lete	6							
	•							
		Disable Storage DR						
	Sele	ct a datastore:						
	Nam	ie	Drive Type	Capacity Pr	ovisioned	Free	Туре	Thin Pro
	•							
	Comp	atibility:						
	Comp	Genome y :						

# Figure 162 Deploy OVF Template - Choosing the Datastore

I

Γ

**6.** Choose the destination Network for mapping the Source Network's Control, Management, and Packet VLANs to the management (infra) VLAN. Click **Next**.

Network Mapping What networks should the	deployed template use?	
Source OVF Template Details End User License Agreement	Map the networks used in this OVF	template to networks in your inventory
Name and Location	Source Networks	Destination Networks
Deployment Configuration	Control	Network mgmt
Host / Cluster	Management	Network mamt
<u>Storage</u> Disk Format	Packet	Network_mgmt
Network Mapping		
Properties Ready to Complete		
Ready to Complete		
	I Description:	
		ty between the Nexus 1000V VSM and VEMs. Please associate ds to the "packet vlan" configured in the VSM.
	Warping: Multiple course petworks	are mapped to the host network: Network mgmt

7. In the Properties window, configure Domain Id (a unique number across multiple N1k VSMs, if there are more than one), Administrator User Password, Management IP address and Management Subnet Mask as shown in Figure 164. Click Next.

1

Figure 164	Deploy OVF Template - Entering Details for the Deployment
Deploy OVF Template	
Properties Customize the software so	olution for this deployment.
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Storage Disk Format Network Mapping Properties Ready to Complete	a. VSM Domain ID         DomainId         Enter the Domain Id (1-4095).         Image: Comparing the password of the password         Password         Enter the password. Must contain at least one capital, one lowercase, one number.         Enter the password         Enter password         enter the password         ************************************
	Management Ip¥4Subnet Enter the Subnet Mask in the following form: 255.255.255.0 255 , 255 , 255 , 0

I

Γ

**8.** Verify the configuration, check the check box **Power on after deployment** and click **Finish** to complete the OVF deployment of VSM virtual machine.

Source OVF Template Details End User License Agreement	When you click Finish, the deploym	ent task will be started.	
Name and Location	Deployment settings: OVF file:	Z:\lab\software\Cisco\N1KV\Nexus1000v.4.2.1.SV2.2.1\V	
Deployment Configuration	Download size:	116.6 MB	
Storage	Size on disk:	3.0 GB	
<u>Disk Format</u> Network Mapping	Name:	Nexus1000V-1780-Primary	
Properties	Folder:	VSPEX-Infra	
Ready to Complete	Deployment Configuration:	Manually Configure Nexus 1000V	
	Host/Cluster:	192.168.1.7	
	Datastore:	Datastore_Template	
	Disk provisioning:	Thick Provision Lazy Zeroed	
	Network Mapping:	"Control" to "Network_mgmt"	
	Network Mapping:	"Management" to "Network_mgmt"	
	Network Mapping:	"Packet" to "Network_mgmt"	
	IP Allocation:	Fixed, IPv4	
	Property:	DomainId = 1780	
	Property:	ManagementIpV4 = 192.168.1.29	
	Property:	ManagementIpV4Subnet = 255.255.255.0	
	Property:	GatewayIpV4 = 192.168.1.1	
	Power on after deployment		

1

**9.** When VSM VM is powering up for the first time, click **Console** of the virtual machine in the vCenter and perform initial configuration of the VSM VM. During the OVF deployment, basic configuration information was already provided. Verify the details and press **no** if you don't want to change anything.



Figure 166 Verifying the Details in the Virtual Machine Console in vCenter

- **10.** Once initial configuration is complete, you would see the exec mode CLI and you can SSH to the VM.
- **11.** It is highly recommended that you deploy two VMs in HA mode for VSM. To deploy secondary VM, repeat steps 1 and 2. On step 3, for the configuration field, choose **Nexus 1000v Secondary** from the drop-down list.

#### Figure 167 Deploy OVF Template - Choosing Deployment Configuration for Secondary VM

ð	Deploy OVF Template	
	Deployment Configuration Select a deployment configu	ration.
ŧ	Source OVF Template Details End User License Agreement Name and Location Deployment Configuratior Host / Cluster Resource Pool Disk Format Properties Ready to Complete	Configuration: Nexus 1000V Secondary Use this deployment option to pair the Nexus 1000V VSM with a secondary VSM in a HA pair. If this option is selected, please only enter the selected properties as prompted in the Properties section ahead ignoring Property (c-e).

**12.** Repeat steps 4, 5 and 6 from the original VSM VM deployment. In the Properties window, give the same domain ID as the primary VSM VM domain ID and password. No need to provide IP address/ subnet mask, as secondary VM will take over the operations if primary fails.

Figure 168	Deploy OVF Template - Entering Details for the Secondary VM Deploym
Deploy OVF Template	
Properties Customize the software so	lution for this deployment.
Source OVF Template Details	
End User License Agreement Name and Location	a. VSM Domain ID
Deployment Configuration	DomainId
<u>Host / Cluster</u> <u>Storage</u>	Enter the Domain Id (1-4095).
<u>Disk Format</u> Network Mapping	
Properties	b. Nexus 1000V Admin User Password
Ready to Complete	Password
	Enter the password. Must contain at least one capital, one lowercase, one number. Enter password ************************************
	Confirm password *********
	c. Management IP Address
	ManagementIp¥4
	Enter the VSM IP in the following form: 192.168.0.10
	0.0.0
	d. Management IP Subnet Mask
	ManagementIp¥4Subnet
	Enter the Subnet Mask in the following form: 255.255.255.0
	0.0.0.0

13. For the other configurations in the wizard, follow the steps same as primary VSM VM configuration.

1

# **Connecting VSM to vCenter**

Once initial setup of VMS VM is completed, we need to add it as a plug-in/ extension in the vCenter:

- 1. Using the browser, access management IP address of the VSM VM.
- 2. Right-click the cisco\_nexus\_1000v\_extension.xml link and save it to a location on your local hard drive.



Figure 169 Save the Cisco Nexus Extension XML on your Local Drive

3. From the vCenter, click **Plug-ins** > **Manage Plug-ins**.



Figure 170 Managing Plug-ins in vCenter

4. Scroll to the bottom of Available Plug-ins, right-click in the empty space and choose New Plug-in.

Plug-ir	n Name	Vendor	Version	Status	Description
Insta	lled Plug-ins		-		
3	VMware vCenter Storage Mon	VMware Inc.	5.0	Enabled	Storage Monitoring and Reporting
3	vCenter Service Status	VMware, Inc.	5.0	Enabled	Displays the health status of vCenter services
3	vCenter Hardware Status	VMware, Inc.	5.0	Enabled	Displays the hardware status of hosts (CIM monitoring)
Availa	able Plug-ins				
3	Cisco-UCSM-079bea36-4bc8	Cisco Systems, I	1.0.0	Download and I	
3	Cisco-UCSM-2587e610-9fae	Cisco Systems, I	1.0.0	Download and I	
3	Cisco-UCSM-f9b83c9a-b6c8	Cisco Systems, I	1.0.0	Download and I	
		New Plug-in		)	

1

Figure 171 Creating a New Plug-in

- 5. Click **Browse**, choose the cisco\_nexus-1000v\_extension.xml file you just downloaded.
- 6. Click Register Plug-in.



Figure 172 Registering the Downloaded XML File as the New Plug-in

7. If you receive a certificate warning, click Ignore.

I

- 8. Click OK. The Plug-in Manager page appears showing the plug-in that was just added.
- 9. Now configure the SVS connection to the vCenter as shown in Figure 174.

#### Figure 173 Configuring SVS Connection



**10.** Validate the connection using **show svs connections** and make sure that the operational status is **connected** and sync status is **Complete** as shown in Figure 175.



```
N1k-VSM(config) # svs connection vspex
N1k-VSM(config-svs-conn)# remote ip address 10.29.150.166
N1k-VSM(config-svs-conn)# protocol vmware-vim
N1k-VSM(config-svs-conn)# vmware dvs datacenter-name vspex
N1k-VSM(config-svs-conn)# connect
N1k-VSM(config-svs-conn)# exit
N1k-VSM(config)# exit
N1k-VSM# show svs connections
connection vspex:
    ip address: 10.29.150.166
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: vspex
    admin:
    max-ports: 8192
    DVS uuid: 5c 03 21 50 ba e4 17 23-ad 02 05 ab 6e cb af 20
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 5.0.0 build-455964
    vc-uuid: 9D562753-5C78-4C08-973A-D67EA6023CB8
N1k-VSM#
```

**11.** You must create uplink port-profiles for the static vNICs of the service profile. Uplink port-profile is used to apply configuration on the uplink of the vDS, effectively the physical adapter of the ESXi server. Configure the system-uplink port-profile.

Figure 175 Configuring System-Uplink Port-profile



The system-uplink port-profile is applied to the system vNICs of the service profile. MTU 9000 is configured on uplink port-profile to enable jumbo frames. "channel-group auto mode on mac-pinning" is a very important configuration which 'pins' the VM vNICs to uplinks on the vDS. MAC pinning feature does static load balancing per vNIC basis. It also provides high-availability by moving the traffic to the alternate adapter when a given fabric is down.

**12.** Create storage-uplink port-profile as shown in Figure 176. The storage-uplink port-profile corresponds to the storage vNICs of the service profile.

Figure 176 Configuring Storage-Uplink Port-Profile



**13.** Create data-uplink port-profile as shown in Figure 177. The data-uplink port-profile corresponds to the data vNICs of the service profile.

	Figure 177	Configuring Data-Uplink Port-Profile	
.67 - PuTTY			



14. Once VSM is connected to the vCenter, it shows up as a virtual Distributed Switch in the vCenter's "Network" view as shown in Figure 179.



Figure 178 VSM Shown as Virtual Distributed Switch in vCenter

15. Add hosts to the vDS.

	- <b>ySphere Client</b> dministration Plug-ins Help 🚓 Inventory	vorking		Search Inventor
4022				
V100-vCenter.VSPEX.CO Vspex Vspex VIIk-VSM UIK	Add Host Manage Hosts New Port Group Manage Port Groups Edit Settings Migrate Virtual Machine Neto Alarm	Ctrl+Alt+N services either thi using ho machine to distrib machine	vSphere Distributed Switch? Distributed Switch acts as a single virtual switch associated hosts. This allows virtual machines to posistent network configuration as they migrate its.	tohnes Hots Taks 8 Events Alares Perressons
		Basic Ta	isks a host	Explore Further Learn more about vSphere Distributed Switches Learn how to set up a network with a

#### Figure 179 Adding Host to vDS

**16.** Select all the VSPEX ESXi hosts and add appropriate adapters using the uplink port-profiles created in the previous step. See Table 10 for vNICs to uplink port-profile mapping.

Γ



*Figure 180 Selecting Host and Adapters to Add to vDS* 

17. Do not migrate management VM kernel from the native vSwitch to vDS, click Next and then click Finish.

🛃 Add Host to vSphere Distributed Sw	vitch				
Network Connectivity Select port group to provide netwo	rk connectivity for the adapters (	on the vSphere distribu	uted switch.		
Select Host and Physical Adapters	🕕 Assign adapters to a desti	nation port group to m	igrate them. Ctrl+click to multi-s	elect.	
Network Connectivity	Host/Virtual adapter	Switch	Source port group	Destination port group	
Virtual Machine Networking Ready to Complete	□ □ 10.29.150.161     □ vmk0     □ □ 10.29.150.162	vSwitch0	Management Network	Do not migrate	
	vmk0	vSwitch0	Management Network	Do not migrate	
	vmk0	vSwitch0	Management Network	Do not migrate	
	ன vmk0	vSwitch0	Management Network	Do not migrate	
	Virtual adapter details				Assign port group
Help				< Back Next :	> Cancel

Figure 181 Selecting Port Groups for Network Connectivity

**18.** Verify that all the hosts are successfully added to the vDS.



Γ

V100-vCenter.VSPEX.COM - vSphere Client								
File Edit View Inventory Administration Plug-ins Help								
🖸 🗈 🔝 Home 🕨 👸 Inventory 🕨 🧕 Net	working					🔊 🗸 Se	arch Inventory	
V100-vCenter.VSPEX.COM	N1k-V5M							
vspex								70010
E 📂 N1k-VSM	Getting Started Sur	nmary Networks	Ports Configuratio	n Virtual Machines	Hosts Tasks & Events	Alarms Permission	15	
E C Nik-VSM						Name or St.	ate contains: 👻	
🔤 system-uplink 💁 Unused_Or_Quarantine_Uplink	Name	∠ State	VDS Status	Status	% CPU	% Memory	Memory Size	CPU Count
2 NFS	10.29.150.161	Connected	🕑 Up	Normal	6	2	65478.71 MB	2
🏯 Unused_Or_Quarantine_Veth	10.29.150.162	Connected	🥑 Up	Normal	0	3	65478.71 MB	2
M-DATA	10.29.150.163	Connected	📀 Up	Normal	7	2	65478.71 MB	2
VMotion     VM Network	10.29.150.164	Connected	📀 Up	Normal	6	2	65478.71 MB	2
M Network	-							

# **Configure Port-Profiles and Add Virtual Machines**

The last step of Nexus 1000v configuration and its integration with vCenter is creation of port-profiles and using them in the virtual machines in the vCenter. Note that this is possible only after carving out disk space for VMs on the storage array and deploying the VMs.

To configure port-profiles for VMs, follow these steps:

1. Create a port-profile for storage (NFS) access. Max-ports can be set to number of hosts you have in the architecture.

Figure 183 Creating a Port-Profile for NFS Storage Access

```
N1k-VSM(config) # port-profile type vethernet NFS
N1k-VSM(config-port-prof) # vmware port-group
N1k-VSM(config-port-prof) # switchport mode access
N1k-VSM(config-port-prof) # switchport access vlan 40
N1k-VSM(config-port-prof) # no shutdown
N1k-VSM(config-port-prof) # max-ports 5
N1k-VSM(config-port-prof) # description port-profile for NFS share access
N1k-VSM(config-port-prof) # state enabled
N1k-VSM(config-port-prof) # state enabled
N1k-VSM(config-port-prof) # exit
N1k-VSM(config-port-prof) # exit
```

2. Create a port-profile for vMotion traffic. Max-ports can be set to number of hosts you have in the architecture.

N1k-VSM(config) # port-profile type vethernet vMotion N1k-VSM(config-port-prof) # vmware port-group N1k-VSM(config-port-prof) # switchport mode access N1k-VSM(config-port-prof) # switchport access vlan 41 N1k-VSM(config-port-prof) # no shutdown N1k-VSM(config-port-prof) # max-ports 5 N1k-VSM(config-port-prof) # state enabled N1k-VSM(config-port-prof) # description port-profile for vMotion traffic N1k-VSM(config-port-prof) # description port-profile for vMotion traffic N1k-VSM(config-port-prof) # exit

Figure 184 Creating a Port-Profile for vMotion Traffic

**3.** Create port-profiles for the virtual machine data traffic used by various applications as per your needs. You can set max ports to appropriate values based on the number of VMs being configured. Following is a sample port-profile:



4. Once the port-profiles are configured, choose the Hosts and Clusters tab, choose the ESXi Host, click the Configuration tab, choose Networking, view vSphere Distributed Switch, and click the Manage Virtual Adapters... link.



Figure 186 Manage Virtual Adapters in vCenter

- 5. Click Add in the wizard, click New virtual adapter, and click Next.
- 6. Select VMKernel on the next dialog box.
- 7. Select port-profile NFS for the storage access, and click Next.
- 8. Configure IP address from the NFS subnet and configure subnet mask. Click **Next** and the **Finish** to deploy the vNIC.
- **9.** Similarly, add one more vmknic (VM Kernel NIC) for vMotion. When providing the port-profile name, make sure that you choose vMotion port-profile and check the check box **Use this virtual adapter for vMotion**.

- 10. Repeat creation of the two vmknic virtual adapters for all the ESXi hosts.
- **11.** Connectivity between all the vmknics can be tested by enabling SSH access to ESXi host, logging in to ESXi host using SSH and using **vmkping** command and ping to all vMotion IP addresses from each of the hosts. Similarly, all the hosts must be able to ping NFS share IP address.
- **12.** Once NFS share is reachable, the NFS datastore can be discovered and mounted through vCenter. Virtual machines can be deployed on these NFS datastore using the VM-Data port-profile for the network access.
- Verify the port-profile usage using show port-profile brief, show port-profile usage, or show port-profile name <name> command. Sample output is as shown in Figure 187.

Figure 187 Running show port-profile brief to Verify Port-Profile Usage

N1k-VSM# show port-profile brief								
				Child Profs				
ernet 1 ernet 1 ernet 1 ernet 1 ernet 1 ernet 1 ernet 1 ernet 1	4 1 5 3 5 5 4	4 0 5 3 5 4	4 0 12 100 12 12 12 4	0 0 0 0 0 0 0				
Prfls Prfls  4 0	Prfls			 E				
	ernet 1 rnet 1 rnet 1 ernet 1 rnet 1 rnet 1 rnet 1 ernet 1 Parent Child Prfls Prfls	ernet 1 4 rnet 1 1 rnet 1 1 rnet 1 5 ernet 1 3 rnet 1 5 rnet 1 5 ernet 1 5 Parent Child UsedBy Prfls Prfls Prfls	State         Items         Items           wernet         1         4         4           rnet         1         1         0           wernet         1         1         0           rnet         1         5         5           wernet         1         5         5           rnet         1         5         5           rnet         1         4         4           Parent         Child         UsedBy           Prfls         Prfls         Prfls           4         0         3	State         Items         Items         Intfs           wernet         1         4         4         4           rnet         1         1         0         0           wernet         1         1         0         0           wernet         1         5         5         12           wernet         1         4         4         4           Parent         1         4         4         4           Parent         Child         UsedBy         Prfls         Prfls           4         0         3         3         3         3				

By running the command **show port-profile name <uplink-port-profile-name>**, you can see the implicit creation of port-channels per ESXi host basis due to the "channel-group auto mode on mac-pinning" CLI configured under the port-profile. In addition to the Ethernet uplink ports, port-channels are also listed as assigned interfaces. Port-channel status can be further viewed/ validated using **show port-channel brief** command from VSM VM.

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

This subsection is divided in two subsections:

- 1. Configure VM Datastores for FC-Variant of the Solution, page 170
- 2. Configuring VM Datastore for the NFS-Variant of the Solution, page 180

#### **Configure VM Datastores for FC-Variant of the Solution**

See Figure 13 for Storage Architecture for 300 VMs on VNX 5400 to have a high-level overview of storage architecture. Follow these steps to configure the data store:

 Login to the EMC VMX Unisphere, and click the Storage tab. Click Storage Configuration > Storage Pools and click the Pools tab. Click Create.

	VNX5300	)-VSPEX 🔽	🛛 🔠 Das	hboard	System	Stora	ige 🔡 H	losts 🧃	😼 Data Prote	ection 🖌 🐐	Se Se
VX5300-VSF	<u>PEX</u> > <u>Stora</u>	<u>qe</u> > <u>Sto</u>	rage Configura	<u>tion</u> > Stora	age Pools						
ools RAID G	iroups										
Pools										273.	•
Y, Filte	r for	RA	ID Type All	>							
Name 🔺	FAST Cache	State	RAID Type	Drive Type	Total Capa	Free Capa	Allocated (	%Consum	Subscribed	%Subscrib	%F
🗿 Pool O	On	Ready	RAIDS	SAS	2146.434	1772.205	374.229		1,156.755	53.892	

# Figure 188 Creating Storage Pools

**2.** Create a new pool. Choose **Manual** for disk selections and choose 45 for the number of SAS disks and 2 for the number of Flash disks to create one pool.

Γ

Storage Pool Parameters -					
Storage Pool Type: 00 Poo	I 🔘 <u>R</u> AID Group				
Sch	eduled Auto-Tie	ring			
Storage Pool ID: 3					4
Storage Pool Name: Pool 3					
RAID1/0 (4+4)	Number of Flash 2 Number of SAS	~			
RAID5 (4+1)     Distribution     Extreme Performance : 183.     Performance : 2415	45 (Recommen 453 GB (0.75%) 56.343 GB (99.2	)			
Distribution Extreme Performance : 183. Performance : 2419 Disks	.453 GB (0.75%) 56.343 GB (99.2	) :5%) ks	Total Raw Capa	rcity: 24339.	79
Distribution Extreme Performance : 183. Performance : 2419 Disks Automatic Use Power Sa Manual	.453 GB (0.75%) 56.343 GB (99.2	) 25%) ks Select	otal Raw Capa	1	79
Distribution Extreme Performance : 183. Performance : 2419 Disks Manual Disk	453 GB (0.75%) 56.343 GB (99.2 vina Eligible Dis	) 25%) Select Drive Type	Model	State	
Distribution Extreme Performance : 183. Performance : 2419 Disks Manual Disk Bus 0 Enclosure 1 Disk 5	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB	) 25%) <u>Select</u> Drive Type SAS	Model STE60005 CL	State Unbound	^
Distribution Extreme Performance : 183. Performance : 2419 Disks Manual Disk	453 GB (0.75%) 56.343 GB (99.2 vina Eligible Dis	) 25%) Select Drive Type	Model	State Unbound Unbound	
Distribution Extreme Performance : 183. Performance : 2419 Disks Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 6 Bus 0 Enclosure 1 Disk 7	453 GB (0.75%) 56.343 GB (99.2 vina Eliaible Dis Capacity 536.808 GB 536.808 GB	) 25%) <u>Select</u> Drive Type SAS SAS	Model STE60005 CL STE60005 CL	State Unbound Unbound Unbound	^
Distribution Extreme Performance : 183. Performance : 2419 Disks Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 6	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB	) 25%) Select Drive Type SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound	^
Distribution Extreme Performance : 183. Performance : 2419 Disks Automatic Use Power Sa Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 6 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 7	453 GB (0.75%) 56.343 GB (99.2 vina Eliaible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) :5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound	^
Distribution Extreme Performance : 183. Performance : 2419 Disks Automatic Use Power Sa Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 8	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) :5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound	^
Distribution Extreme Performance : 183. Performance : 2413 Disks Automatic Use Power Sa Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 9 Bus 0 Enclosure 1 Disk 10 Bus 0 Enclosure 1 Disk 11 Bus 0 Enclosure 1 Disk 11 Bus 0 Enclosure 1 Disk 12	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) :5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound	^
Distribution Extreme Performance : 183. Performance : 2419 Disks Automatic Use Power Sa Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 6 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 9 Bus 0 Enclosure 1 Disk 10 Bus 0 Enclosure 1 Disk 11 Bus 0 Enclosure 1 Disk 11	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) :5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SA	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound Unbound	
Distribution Extreme Performance : 183. Performance : 2413 Disks Automatic Use Power Sa Manual Disk Bus 0 Enclosure 1 Disk 5 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 7 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 8 Bus 0 Enclosure 1 Disk 9 Bus 0 Enclosure 1 Disk 10 Bus 0 Enclosure 1 Disk 11 Bus 0 Enclosure 1 Disk 11 Bus 0 Enclosure 1 Disk 12	453 GB (0.75%) 56.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) :5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SA	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound Unbound Unbound	^

1

Figure 189 Details for Creating Storage Pool

- **3.** Repeat this step for 2 more times to create total of three pools for VM datastorage. For the third pool, you would add 20 SAS drives and 2 Flash drives (See Figure 13 for Storage Architecture for 300 VMs on VNX 5400).
- 4. Click Storage > LUNs. You will see 5 boot LUNs created for 5 hosts. Click Create to create the LUN for VM datastore.

MC Unisphere					Pool LUN	Search
> 🏠 🗐 VNX5300-VSPEX 💌	🔠 Dashboard 🛛	System	Stor.	age 👔 Hosts	📷 Data Protection	🌼 Settings
NX5300-VSPEX > Storage > LUNs						
JNs Folders						
LUNS					1	ટે 🍸 🔧 🔥 📀
Y Filter for Usage Al	L User LUNs 🛛 🔽 Fo	older All 🔽 S	Status All	~		
lame	ID	I	User Capa	Host Information		
LUN 0		0	50.000	VSPEX-Server-1		
LUN 1		1	50.000	VSPEX-Server-3		
LUN 2		2	50.000	VSPEX-Server-2		
LUN 3		з	50.000	VSPEX-Server-4		
LUN 4		4	50.000	VSPEX-Server-5		
<		::				>
Selected Create Delete Prop	erties Add to Stora	ge Group				Filtered: 5 of 5

#### Figure 190 Creating LUNs for VM Datastore

5. Click the **Pool** radio button for storage pool type, and choose the first VM data Pool ID from the drop-down list, which was created in step 2. Make sure to check the Thin check box for provisioning. Select User Capacity as 7 TB from the drop-down list and Number of LUNs to Create per pool as 2, and click **Apply**.

Γ

VNX5400-VSPEX - Create LUN
General Advanced
Storage Pool Properties
Storage Pool Type: <ul> <li><u>P</u>ool</li> <li><u>R</u>AID Group</li> </ul>
RAID Type: Mixed: Multi-tiered with mixed RAID types
Storage Pool for new LUN: Pool 3
Capacity           Available Capacity: 19365.249 GB         Consumed Capacity: 43.835 GB
Oversubscribed By:
LUN Properties
✓ Thin
User Capacity: 7 TB
LUN ID: 15 Number of LUNs to create: 2
LUN Name
O Name
Starting ID
Automatically assign LUN IDs as LUN Names
<u>A</u> pply <u>C</u> ancel <u>H</u> elp

Figure 191

Details for Creating LUN

**6.** Repeat step 5 for all the 3 pools in the system. Note that 3rd pool will have reduced LUN size of 2.2 TB.

1

7. Select all the newly created LUNs, and click Add to Storage Group.

Figure 192	Adding the Created LUN to Storage Group

Y. F	ilter for	r	Usage ALL U	ser LUNs 🛛 🔽						
Name	*	ID	State	Thin	User Capacity	Current Owner	Host Information	Initial	Additio	Tierin
LUN 1	5	15	Ready	On	7168.000	SP B		Highes		Auto
LUN 1	6	16	Ready	On	7168.000	SP A		Highes		Auto

**8.** Select all ESXi servers, and move them to the right side. This will allow all ESXi hosts to see the datastore, which is essential for the vMotion of VMs across the cluster.

📔 Add to selected Storage Groups	
Storage System VNX5300-VSPEX	
Select Storage Groups	
Available Storage Groups	Selected Storage Groups
Name	Name
VSPEX-Server-5	
😰 VSPEX-Server-1	
📴 VSPEX-Server-2	
📴 VSPEX-Server-3	
VSPEX-Server-4	
🛃 ~filestorage	
	<u>Q</u> K <u>C</u> ancel <u>H</u> elp

#### Figure 193 Moving Storage Groups to Selected Storage Groups

**9.** On the LUNs window, you will see the storage group (and hence host) access for LUNs as shown in Figure 194.

AC Unisphere			Pool LUN Search
> 🏠 🗊 v	NX5300-VSPEX 💌	🚟 Dashboard 📲 🤋	System 👔 Storage 🚦 Hosts 😱 Data Protection 🏾 🎇 Settings 📀
NX5300-VSPEX >	<u>Storage</u> > LUNs		
UNs Folders			
LUNs			
🝸 🗸 Filter for	Usage A	LL User LUNs 💽 Folde	er All 🔍 Status All
Name 🏾	ID State	User Capacity (GB)	Host Information
🛢 LUN 0	0 Ready	50.000	0 VSPEX-Server-1
LUN 1	1 Ready	50.000	0 VSPEX-Server-3
🚔 LUN 2	2 Ready	50.000	0 VSPEX-Server-2
🖺 LUN 3	3 Ready	50.000	0 VSPEX-Server-4
🖺 LUN 4	4 Ready	50.000	0 VSPEX-Server-5
🖺 LUN 5	5 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🖺 LUN 6	6 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🖺 LUN 7	7 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🖺 LUN 8	8 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🖺 LUN 9	9 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🖺 LUN 10	10 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
🛢 LUN 11	11 Ready	2141.336	6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5
	12 Ready		6 VSPEX-Server-4; VSPEX-Server-3; VSPEX-Server-2; VSPEX-Server-1; VSPEX-Server-5

Figure 194 Storage Group and Host Information

ſ

 login to vCenter GUI, select a particular host from the Hosts and Clusters view, click Configuration and then Storage. Click the Add Storage link.



1

11. Click the Disk/LUN radio button in the wizard, click Next.

### Figure 196 Choose the Storage Type

I

Γ

🛃 Add Storage	
Select Storage Type Specify if you want to forma	t a new volume or use a shared folder over the network.
Disk/LUN Select Disk/LUN File System Version Current Disk Layout Properties Formatting 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.             • Adding a datastore on Fibre Channel or iSCSI will add this datastore to all hosts that have access         to the storage media.
Help	< Back Next > Cancel

12. Select the DGC Fibre Channel Disk (...) from the list and click Next.

#### Figure 197

Selecting a LUN

Add Storage Select Disk/LUN Select a LUN to create a	datastore or expand the current one				
Disk/LUN Select Disk/LUN	Name, Identifier, Path ID, LUN, Capacit		Label c	•	Clear
File System Version	Name	Path ID	LUN 🛆	Drive Type	Capacity
Current Disk Layout Properties	Local LSI Disk (naa.64403a70b495e	vmhba0:C2:T0:L0	0	Non-SSD	184.40 GB
Formatting	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L3	3	Non-SSD	2.09 TB
Ready to Complete	DGC Fibro Channal Disk (naa.60060	vmhba1+C0+T1+L1	1	Non SSD	2.09 10
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L5	5	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L6	6	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L7	7	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L8	8	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L9	9	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L10	10	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L11	11	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L12	12	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L13	13	Non-SSD	2.09 TE
	DGC Fibre Channel Disk (naa.60060	vmhba1:C0:T1:L14	14	Non-SSD	2.09 TE
	•		_		1
Help			< Back	Next >	Cancel

1

# **13.** Enter the name of the first datastore as VM-DS1 and click **Next** and then **Finish**.

🛃 Add Storage				
<b>Properties</b> Specify the properties for th	e datatore			
Disk/LUN Select Disk/LUN File System Version Current Disk Layout Properties Formatting Ready to Complete	Enter a datastore name			
Help		<u>≤</u> Back	Next >	Cancel //

Specifying a Name for Datastore

Figure 198

Γ

**14.** Repeat steps 10 to 13 for all the datastores. Once data stores are added to one host, it will automatically show up for the other hosts too. The end result looks like Figure 199 (on each host):

🚱 VSPEX - vSphere Client							
File Edit View Inventory Administra	tion Plug-ins Help						
🖸 💽 🏡 Home 🕨 🛃 Inv	entory 🕨 🛐 Hosts and Clusters				😴 🔹 Search In	ventory	Q
5 6 8 8 9 4							
VSPEX     VSPEX-DC     VSPEX-Cluster     VSPEX-Cluster     10.65.121.205	10.65.121.209 VMware ESXi, 5.1.0, 79 Getting Started Summary Virtual Ma	achines Performance Config		Events Alarms Permissions M	aps Storage Views	Hardware Status	Update Mar 📢
10.65.121.206 10.65.121.207	Processors	View: Datastores Dev Datastores	nces	Refresh Delete	escan All		
10.65.121.208	Memory	Identification	Status	Device Drive Type	Capacity	Free Type	Last Upr
■ 10.65.121.209 ■ 10.65.121.253	Storage	datastore1 (1)	Normal	DGC Fibre Channel Non-SSD	45.00 GB	44.05 GB VMF55	4/1/201
	Networking	WM-DS1	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFSS	4/1/201
	Storage Adapters	VM-DS10	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Network Adapters	VM-DS11	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMF55	4/1/201
	Advanced Settings	VM-D512	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Power Management	M-DS2	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMF55	4/1/201
		VM-DS3	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Software	VM-D54	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Licensed Features	M-DS5	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Time Configuration	VM-D56	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	DNS and Routing	M-DS7	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Authentication Services	VM-DS8	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Power Management	VM-D59	Normal	DGC Fibre Channel Non-SSD	2.09 TB	2.09 TB VMFS5	4/1/201
	Virtual Machine Startup/Shutdown						
	Virtual Machine Swapfile Location	•					•
	Security Profile	Datastore Details					
	Host Cache Configuration	Datastore Details				P	roperties
	System Resource Allocation						

#### Figure 199 Datastores Added to the Hosts

Configuring VM Datastore for the NFS-Variant of the Solution

To Create Storage Pools for NFS Datastore. Click Storage > Storage Configuration > Storage pools.

1

1

#### Figure 200 Selecting Storage Pools in EMC Unisphere

EMC Unisph	here						Pool L	UN 🗸	Search
< > <b>î</b>	VSPEX5600	🔠 Dashboard	System	Storage	🐌 Hosts	Data Protection	🐝 Settings	👩 Support	
VSPEX5600	> <u>Storage</u> > Storage Confi	guration							
	File Systems Create and manage File S	Systems.			14.14 14.14	Storage Pools Create and manage sto	rage pools and R	AID groups.	
45	Storage Pools for F Create and manage stor					Volumes Create and manage Vol creating File Storage fro			

2. In the EMC Unisphere GUI, choose Storage Pools> Pools. Click Create.
| Fig               | ure 201                    | Creating St     | orage Poo         | ols        |           |             |             |               |
|-------------------|----------------------------|-----------------|-------------------|------------|-----------|-------------|-------------|---------------|
| https://10.29.150 | 0.201/start.html           |                 |                   |            |           |             |             |               |
| MC Unisph         | ere                        |                 |                   |            | Poo       | LUN         | ✓ Sear      | ch            |
| < > 🏠             | VSPEX5500                  | 🖌 🔚 Da:         | shboard           | 📕 System   | n 🍸 St    | orage       | 🐌 Hosts     | 🗊 Data I      |
| VSPEX5500 >       | <u>Storage</u> > <u>St</u> | orage Configura | <u>tion</u> > Sto | rage Pools |           |             |             |               |
| Pools RAID G      | roups                      |                 |                   |            |           |             |             |               |
| Pools             |                            |                 |                   |            |           |             | 3           | 7 🍾 🌛 ?       |
| 🝸 🗸 Filter        | for                        | RAID Type       | u 🔽               |            |           |             |             |               |
| Name              | 🔺 State                    | RAID Type       | Drive Type        | User Capa  | Free Capa | Allocated   | %Consu      | Subscribe %   |
|                   |                            |                 |                   |            |           |             |             |               |
|                   |                            |                 |                   |            |           |             |             |               |
| <                 |                            |                 |                   |            |           |             |             | >             |
|                   | Create Dele                | te Properti     | 11                | ind        |           |             |             | 0 item        |
| E                 |                            |                 |                   |            |           | Last Refres | hed: 2012-0 | 8-06 10:04:06 |
|                   |                            |                 |                   |            |           |             |             |               |

**3.** In the Create Storage Pool window, manually select 45 SAS drives and 2 SATA Flash drives and add to the pool. Under Extreme Performance, choose RAID10 (4 + 4) and under Performance, choose RAID configuration as RAID5 (4+1) from the drop-down list. Number of Flash/ SAS disks will be automatically populated based on the number of disks that is manually added to the pool.

ſ

Storage Pool Parame	eters –					
Storage Pool Type: (	• <u>P</u> ool	O RAID Group	)			
[	Sche	eduled Auto-Tie	ring			
Storage Pool ID:	3					Y
Storage Pool Name:	Pool 3					
Extreme Performan						-1
RAID Configuration	1	Number of Flash	Disks			
RAID1/0 (4+4)	<b>~</b>	2	~			
Performance						
RAID Configuration		Number of SAS	Disks			
			ded)			
RAID5 (4+1) Distribution Extreme Performance Performance	: 183.4	45 (Recommen	)			
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow	: 183.4 : 2415	45 (Recommen 453 GB (0.75%) 6.343 GB (99.2	) 5%) ks			
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow	: 183.4 : 2415	45 (Recommen 453 GB (0.75%) 6.343 GB (99.2	) 5%)	Total Raw Capa	city: 24339.	79
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow Manual	: 183.4 : 2415	45 (Recommen 453 GB (0.75%) 6.343 GB (99.2	) 5%) ks	Total Raw Capa	city: 24339. State	79
RAID5 (4+1)  Distribution Extreme Performance Performance  Disks Automatic Use Pow Manual Disk Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Sav	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB	) 5%) <u>S</u> elect Drive Type SAS	Model STE60005 CL	State Unbound	79
RAID5 (4+1) Distribution Extreme Performance Performance Disks Manual Disk Bus 0 Enclosure 1 Di Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Saw	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB	) 5%) <u>S</u> elect Drive Type SAS SAS	Model STE60005 CL STE60005 CL	State Unbound Unbound	
RAID5 (4+1)  Distribution Extreme Performance Performance  Disks  Manual  Disk Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Saw	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound	^
RAID5 (4+1)  Distribution Extreme Performance Performance  Disks  Manual Disk Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Sav isk 5 isk 6 isk 7 isk 8	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 ving Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound	^
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow Manual Disk Bus 0 Enclosure 1 Di Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Sav isk 5 isk 6 isk 7 isk 8 isk 9	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 7 ing Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound	^
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow Manual Disk Bus 0 Enclosure 1 Di Bus 0 Enclosure 1 Di	: 183.4 : 2415 wer Sav isk 5 isk 6 isk 7 isk 8 isk 9 isk 10	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 7 Ing Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound	^
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow Manual Disk Bus 0 Enclosure 1 Di Bus 0 Enclosure 1 Di	: 183.4 : 2415 isk 5 isk 6 isk 7 isk 8 isk 9 isk 10 isk 11	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 7 Ing Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound	^
RAID5 (4+1) Distribution Extreme Performance Performance Disks Automatic Use Pow Manual Disk Bus 0 Enclosure 1 Di Bus 0 Enclosure 1 Di	: 183.4 : 2415 isk 5 isk 6 isk 7 isk 8 isk 9 isk 10 isk 11 isk 12	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 7 Ing Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SAS	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound Unbound	^
RAID5 (4+1) Distribution Extreme Performance	: 183.4 : 2415 : 2415 : 2415 : 2415 : 345 : 345	45 (Recomment 453 GB (0.75%) 6.343 GB (99.2 7 Ing Eligible Dis Capacity 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB 536.808 GB	) 5%) <u>Select</u> Drive Type SAS SAS SAS SAS SAS SAS SAS SAS SAS SA	Model STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL STE60005 CL	State Unbound Unbound Unbound Unbound Unbound Unbound Unbound Unbound	^

1

Figure 202 Details for Creating Storage Pools

- **4.** Repeat step 3 for required number of pools depending on your architecture. See the Storage Layout diagram for 600 and 1000 VMs, Figure 14 and Figure 15 respectively.
- **5.** To create LUNs from the newly created pools for NFS Datastore; choose **Storage**, right-click on PerformancePool (or "Pool 0", whatever name you have given). Choose **Create LUN**.

	5500 🛩	100						
	and the second se	Das Das	hboard	System	Sto	orage	Hosts	👔 Data Pr
/SPEX5500 > Storage	> <u>Storage</u>	Configurat	tion > Stor	rage Pools				
Pools RAID Groups								
Pools							2 .	9 🔧 🖻 🤉
<b>Filter for</b>	RAI	ID Type A	II 🔽					
Name 🔺 St	ate R/	AID Type	Drive Type	User Capa	Free Capa	Allocated	%Consu	Subscribe %
	ate LUN		SAS	32147.666	32147.666	0.000		0
< Exp			::					>
1 Selected Crea Ana	ice lyzer	> ertie	Expa	nd				1 items
Auto	o-Tiering	>				Last Refresh	ned: 2012-0	8-06 11:08:28
Prop	perties	1	1	*			2.	r 4. 🖻 🤉

### Figure 203 Creating LUNs form Newly Created Pool

I

Γ

6. Make sure, the check box **Thin** is unchecked, User Capacity is 800 G, and number of LUNs to create is 20.

Storage Pool Type:	Pool O RAID Group
RAID Type:	Mixed: Multi-tiered with mixed RAID types
Storage Pool for new LUN:	
Capacity	
Available Capacity: 2993.3	335 GB Consumed Capacity: 16415.750 GB
Oversubscribed By:	
Oversubscribed by:	
LUN Properties	
Thin	
User Capacity: 800	GB
	Number of LUNs to create 20
LUN ID: 49	
LUN Name	
LUN Name	
LUN Name	] (2)
Vame Name Starting ID	] (2)

Figure 204 Details for Creating LUN

7. Select the pool and Select all the newly created LUNs and Click Add to Storage Group as shown Figure 205. Make sure you select all the LUNs from the pools.

Pools				272	- 🝺 (
Y Filter for	RAID Type	All			
Name 🔺 St	ate RAID Type		apa Allocated %Co	onsu Subscribe %Subscri Aut	to-Tieri
PerformancePool Re	eady RAID5	Mixed 95307.785 4871	6.965 46590.820	46,440.527 48.727 Sd	hedule
L Selected Create	Delete Proper	ties Expand			1 ite
				Last Refreshed: 2012-08-06	14:14:
		· · ·			
Pool LUNs Disks				2 P 4	. 🖻
Details Pool LUNs Disks Filter for Name III		ALL User LUNs	Current Owner	Host Information	. 🕑
Pool LUNS Disks		1			~
Pool LUNs Disks	) State	User Capacity (GB)	SP A		
Pool LUNs Disks	D State	User Capacity (GB) 800.000	SP A SP B		~
Pool LUNs Disks	D State 11 Ready 12 Ready	User Capacity (GB) 800.000 800.000	SP A SP B SP A		~
Pool LUNs Disks	State           11         Ready           12         Ready           13         Ready	User Capacity (GB) 800.000 800.000 800.000	SP A SP B SP A SP B		
Pool LUNs Disks	State       11       Ready       12       Ready       13       Ready       14	User Capacity (GB) 800.000 800.000 800.000 800.000 800.000 800.000	SP A SP B SP A SP B SP A		
Pool LUNs Disks	State       11     Ready       12     Ready       13     Ready       14     Ready       15     Ready	User Capacity (GB)	SP A SP B SP A SP B SP A SP B		
Pool LUNS Disks	State       11     Ready       12     Ready       13     Ready       14     Ready       15     Ready       16     Ready	User Capacity (GB)  S00.000 S00.000 S00.000 S00.000 S00.000 S00.000 S00.000 S00.000 S00.000	SP A SP B SP A SP B SP A SP B SP A		~
Pool LUNS Disks	State       11     Ready       12     Ready       13     Ready       14     Ready       15     Ready       16     Ready       17     Ready	User Capacity (GB)  User Capacity (GB)  800.000 800.000 800.000 800.000 800.000 800.000 800.000 800.000 800.000 800.000 800.000 800.000	SP A SP B SP A SP B SP A SP B SP A SP B		~

### Figure 205 Adding Pools and LUNs to Storage Group

I

Γ

8. From the Available Storage Groups, Select "~filestorage" and click the Arrow tab. Once "~filestorage" is selected on right pane, click **OK**.

torage System VSPEX5500	*		
elect Storage Groups			
vailable Storage Groups	Sel	lected Storage Groups	
lame	Nar	me	
<ul> <li>V250-ESXHost7</li> <li>V250-ESXHost2</li> <li>V250-ESXHost5</li> <li>V250-ESXHost1</li> <li>V250-ESXHost4</li> <li>V250-ESXHost8</li> <li>V250-ESXHost3</li> <li>V250-ESXHost3</li> <li>V250-ESXHost9</li> <li>V250-ESXHost10</li> <li>~filestorage</li> </ul>			

Figure 206 Moving Storage Groups to Selected Storage Groups

9. In the EMC Unisphere GUI, choose Storage > Storage Configuration > Storage Pools for Files, and click Rescan storage systems on the right pane. Rescan will take up to 4 minutes of time. Once rescan successfully finishes (track the progress at Background task for files page under System menu), click Refresh and newly created storage pools must be visible in the left pane of the window.

					Search Search
E Dashboard	System Storage	🐌 Hosts 🛛 🔞 Data Protectio	n 🗱 Settings	🗿 Support	
i <u>guration</u> > Storage	Pools for File				
				4, 2 💿 🤈	Wizards
					LUN Provisioning Wizard
	Storage Capacity (GB) Storage Used(	%) Туре	Disk Type	Automatic Extension	RAID Group LUN Expansion Wiza Disk Provisioning Wizard for File
Pool 1 on FNM001	15999.992	Mapped pool	Mixed	Enabled	Storage Assignment Wizard for He
I Pool 3 on FNM001	15999.992	Mapped pool	Mixed	Enabled	SAN Copy Wizard File System Wizard
					CIFS Services Wizard Tiering Manage Auto-Tiering Data Migration Configure SAN Copy Settings Update SAN Copy Connections Block Storage LUN Migration Summary File Storage
					Rescan Storage Systems Dedupfication Settings Configure CIFS Restore LUN Ownership for File
tend Shrink	Delete			2 items	Atmos Management Launch Atmos Configure Atmos
ten	d Shrink	1 Shrink Delete	d Shrink Delete		d Shrink Delete 2 items Last Refreshed: 2013-08-22 15:07:46

I

ſ

### Figure 207 Created Storage Pools are Shown in Storage Pools for File Window of EMC Unisphere

 At this point, the NFS volume is created. Next step is to create highly available network access for the NFS volume. To Create LACP interface, navigate to Settings > Network > Settings for File. and click the Devices tab. Click Create.

Y Filter for		Devices for: All Data Move			
Name	<ul> <li>Data Mover</li> </ul>	Туре	Speed/Duplex	Devices	
€ cge-2-0	B≢ <u>server 2</u>	port	auto		
🗬 cge-2-0	B≠ <u>server 3</u>	port	auto		
€ cge-2-1	B≢ <u>server 2</u>	port	auto		
🗬 cge-2-1	B≢ <u>server 3</u>	port	auto		
🗬 cge-2-2	B≢ server 2	port	auto		
🝘 cge-2-2	B≢ server 3	port	auto		
🗬 cge-2-3	B≢ <u>server 2</u>	port	auto		
🗬 cge-2-3	B# server 3	port	auto		
🗬 fxg-1-0	B# server 2	port	10000FD		
€ fxg-1-0	B≠ <u>server 3</u>	port	10000FD		
🗬 fxg-1-1	B# server 2	port	10000FD		
	B# server 3	port	10000FD		

1

#### Figure 208 Creating LACP Interface

 Choose Date Mover as All Primary Data Movers from the drop-down list, click the Link Aggregation for Type and enter the Device name as lacp-1. Check the two check boxes for 10 Gigabit ports fxg-1-0 and fxg-1-1. Click OK to proceed to the Network Device Creation.

Data Mover:	All Primary Data Movers
Type:	© Ethernet Channel © Link Aggregation
Device Name:	C Fail Safe Network
10/100 ports:	None available
Gigabit ports:	None available
10/100/1000 ports:	□ cge-2-0 □ cge-2-1 □ cge-2-2 □ cge-2-3
10 Gigabit ports:	▼ fxg-1-0 ▼ fxg-1-1
Speed/Duplex:	
	OK Apply Cancel Help

### Figure 209 Creating Network Device

**12.** Figure 210 shows the creation of LACP Network device name as "lacp-1"

### Figure 210 Created LACP Network Device is Shown Under Network Devices

Network Devices				۹. 2 🌛
💎 🗸 Filter for	Show Network D	evices for: All Data Mov	vers 💙	
Name	<ul> <li>Data Mover</li> </ul>	Туре	Speed/Duplex	Devices
🗬 cge-2-0	B# server 2	port	auto	
🗬 cge-2-0	D# server 3	port	auto	
€ cge-2-1	B# server 2	port	auto	
🗬 cge-2-1	B# server 3	port	auto	
€ cge-2-2	B# server 2	port	auto	
🗬 cge-2-2	B# server 3	port	auto	
€ cge-2-3	B≇ server 2	port	auto	
🗬 cge-2-3	B# server 3	port	auto	
	B# server 2	port	10000FD	
🗬 fxg-1-0	D# server 3	port	10000FD	
	B≉ server 2	port	10000FD	
	D# server 3	port	10000FD	
	B# server 2	lacp	10000FD	f×g-1-0,f×g-1-1

Γ

13. From the Settings for File tab. Click Interfaces and then click Create.

1

Interfaces					2.
8.	🖾 Show	Network Interfaces for: All Da	ata Movers 💌		
Address	<ul> <li>Name</li> </ul>	Netmask	Data Mover	Device	State
128.221.252.	2 el30	255.255.255.0	server 2	mge0	Up
128.221.252.	3 el30	255.255.255.0	server 3	mge0	Up
128.221.253.	2 el31	255.255.255.0	server 2	mge1	Up
128.221.253.	3 el31	255.255.255.0	server 3	mge1	Up

### Figure 211 Creating Network Interface

14. Choose the Data Mover as server\_2 and Choose Device name as lacp-1 from the drop-down list. Specify the valid IP address, Netmask and Interface name as "fs01" & MTU value as "9000" to allow jumbo frames for the lacp interface.

Data Mover:	server_2	-
Device Name:	lacp-1	
Address:	10.10.40.11	
Name:	fs01	
Netmask:	255.255.255.0	
Broadcast Address:	10.10.40.255	
MTU:	9000	
VLAN ID:		
	OK Apply Cancel Help	

### Figure 212 Details for Creating Network Interface

To Create File system for NFS data store, navigate to Storage > Storage Configuration. Click File Systems and then click Create.

From the Create File System window, click the **Storage Pool** radio button and Specify File System Name as **NFS-DS-1** for Virtual machine datastore. Then, Select Storage Pool from the drop-down list. Specify Storage Capacity as **5 TB**, check the check box **Thin Enabled**, **7340032** MB (7TB) as Max Capacity, and choose Data Mover as **Server\_2**. Click **OK** to create NFS-DS-1 File system.

I

🕹 ¥SPEX5	600 - Create Storage Poo	ol - Mozilla Firefox 📃 🗆 🗙
https:/	/10.6.117.30/action/storageP	oolDisplay
		©Storage Pool ©Meta Volume
File Syste	m Name:	NFS-DS-1
Storage P	ool:	Pool 3 15.6 TB (16383980 MB)
Storage C	apacity:	7 ТВ 💌
Auto Exte	nd Enabled:	
Thin Enab	led:	
Water Mark: Capacity (MB):	% (Ranges from 50-99 90 if left blank defaults to 90) Required 7340032 is enabled.	; 
Slice Volu	mes:	
Deduplica	tion Enabled:	
VMware VAAI nested clone support: Data Mover (R/W): Mount Point:		(Must be selected at file system creation time) server_2 © Default
0		Ccustom
		OK Apply Cancel Help

Figure 213 Details for Creating Storage Pool

16. Wait until the NFS-DS-1 File system creation process to complete. Verify the process using Background Tasks for File under System menu. Once the NFS-DS-1 is successfully created, repeat steps 15 and 16 for one more NFS file system NFS-DS-2 for the given pool. You will need to create total 10 File systems for 600 VM setup and 16 File Systems for 1000 VM setup.

1

 To enable Direct Writes for all the NFS File system. Select Storage > Storage Configuration > File Systems. Click the Mounts tab, select the path /NFS-OS for the file system NFS-OS and click Properties.

🝸 🗸 Filter for	Show	Mounts for: All Data Mo	vers 🔽 File Syst	em Name: All	~	
Path	🔺 Data Mover	File System	Read Only	Access-Chec	Virus Checki	CIFS Oplocks.
📮 /NFS-Data01	B≉ <u>server_2</u>	MFS-Data01	No	NATIVE	Yes	Yes
🗘 /NFS-Data02	B≉ <u>server_2</u>	T NFS-Data02	No	NATIVE	Yes	Yes
📮 /NFS-Data03	B≄ <u>server_2</u>	MFS-Data03	No	NATIVE	Yes	Yes
📮 /NFS-Data04	B≉ <u>server_2</u>	MFS-Data04	No	NATIVE	Yes	Yes
🗘 /NFS-Data05	B≉ <u>server_2</u>	MFS-Data05	No	NATIVE	Yes	Yes
📮 /NFs-Data06	B≉ <u>server_2</u>	T NFs-Data06	No	NATIVE	Yes	Yes
/NFS-Data07	B≉ <u>server_2</u>	T NFS-Data07	No	NATIVE	Yes	Yes
📮 /NFS-Data08	B≉ <u>server_2</u>	T NFS-Data08	No	NATIVE	Yes	Yes
/NFS-Data09	B≉ <u>server_2</u>	T NFS-Data09	No	NATIVE	Yes	Yes
🗘 /NFS-Data10	B≉ <u>server_2</u>	MFS-Data10	No	NATIVE	Yes	Yes
INFS-OS	Br server 2	MFS-OS	No	NATIVE	Yes	Yes

Figure 214 Select /NFS-OS to Enable Direct Writes

- From the /NFS-OS mount properties. Make sure the radio buttons Read/Write and Native for Access policy are selected. Then, check the Set Advanced Options check box.
- Figure 215 /NFS-OS Mount Properties Part 1

ſ

VSPEX5500 - /NFS-05	- Mount Properties - Windows Internet Explorer	_	
https://10.29.150.201/	action/mountDisplay	Sertificate Error	18
Path:	/NFS-OS		2
DataMover:	server 2		
File System Name:	NFS-OS		
Read Only: C	© Read/Write C Read Only		
Access-Checking Policy:	C NT - CIFS client rights checked against ACLs; NFS client rights checked against ACLs and permissio C UNIX - NFS client rights checked against permission bits; CIFS client rights checked against permiss C SECURE - Both NFS and CIFS client rights checked against both permission bits AND ACLs NATIVE - NFS client rights checked against permission bits; CIFS client rights checked against ACLs MIXED - Both NFS and CIFS client rights checked against ACL; Only a single set of security attribut MIXED_COMPAT - Both NFS and CIFS client rights checked against either permission bits or ACL de protocol was last used to set permission	sion bits AND ACLs : es maintained	
Virus Checking Enabled:	R		
Cifs Oplocks Enabled:	<b>u</b>		
Set Advanced Options:			
	OK Apply	Cancel Help	p

19. Check the Set Advanced Options and the Direct Writes Enabled check box and click OK.

CV5PEX5500 - /NFS-OS - Mo	unt Properties - Windows Internet Explorer
bttps://10.29.150.201/action	/mountProperties Certificate Error
Path:	/NFS-OS
DataMover:	server 2
File System Name:	NFS-OS
Read Only:	© Read/Write
Access-Checking Policy:	C Read Only C NT - CIFS client rights checked against ACLs; NFS client rights checked against ACLs and permission bits C UNIX - NFS client rights checked against permission bits; CIFS client rights checked against permission bits AND ACLs C SECURE - Both NFS and CIFS client rights checked against both permission bits AND ACLs (* NATIVE - NFS client rights checked against permission bits; CIFS client rights checked against ACLs (* NATIVE - NFS client rights checked against permission bits; CIFS client rights checked against ACLs (* MIXED - Both NFS and CIFS client rights checked against ACL; Only a single set of security attributes maintained
	MIXED_COMPAT - Both NFS and CIFS client rights checked against either permission bits or ACL depending on which protocol was last used to set permissions
Virus Checking Enabled:	
Cifs Oplocks Enabled:	
Set Advanced Options:	
Use NT Credential:	
Direct Writes Enabled:	
Prefetch Enabled:	
Multi-Protocol Locking Policy:	© nolock O writelock O rwlock
CIFS Sync Writes Enabled:	
CIFS Notify Enabled:	CIFS Notify Trigger Level: 512
	CIFS Notify On Access Enabled:
	CIFS Notify On Write Enabled:
	OK Apply Cancel Help
Done	S Internet   Protected Mode: Off

Figure 216 /NFS-OS Mount Properties - Part 2

- 20. Follow the Steps to enable Direct Writes for all the remaining NFS Data file systems.
- **21.** To Create NFS-Exports for all the NFS File systems. Click **Storage > Shared Folders > NFS** and click **Create**.

1

1

EMC Unisphere			Pool	LUN	Search	
< > 🁔 🗊 VSPEX5500 💌	🔠 Dashboard	System	🕤 Storage	Hosts	🐻 Data Protection	-
<u>VSPEX5500</u> > <u>Storage</u> > <u>Shared</u>	Folders > NFS					
NFS Exports					۹., 2 🗈	?
Y Filter for Sho	w NFS Exports for: se	rver_2 💌	Select a File Sys	tem: NFS-Data0	1	
Path	▲ File System	m		Data Mover		
						- 1
0 Selected Create Properties	Delete				Filtered: 0	of 1
				Last Refre	eshed: 2012-08-31 17:52	:54

### Figure 217 Creating NFS Exports

22. Select Data mover as server-2 and Choose File system as NFS-OS and specify Path as /NFS-OS. In the Root Hosts and Access Hosts fields, enter the IP address of all the ESXi hosts VMKernel Storage NIC. Separate multiple host vmkernel IP's by : (colon) and click OK. Repeat this step for all the NFS File Systems created on the storage array.

ſ

S Exports	VSPEX5500 - Create	NFS Export - Windows Internet Explorer		×
	https://10.29.150.201/	action/exportDisplay	😵 Certificate Error	
🌱 📮 Filter for	Choose Data Mover:	server_2		4
th				
	File System:	NFS-OS (/NFS-OS)		
	Path:	/NFS-OS		
	Host Access Read-only Export:			
	Read-only Hosts:	×		
	Read/Write Hosts:			
	Root Hosts:	10.10.40.21		
	Access Hosts:	10.10.40.21		
		OK Apply Cancel	Help	
elected Create	Pro			

Figure 218 Details for Creating NFS Export

### **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 that the VMs are spread across different VM datastores to properly load-balance the storage usage. The final snapshot of VMs in a cluster looks like Figure 220.

Figure 220 Summary Window Showing VMs in the Cluster in vCenter



## Validating Cisco Solution for EMC VSPEX VMware Architectures

This section provides a list of items that should be reviewed when 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 before deploying for 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, make sure to have a continuous ping to default gateway and to check if the 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, during FI reboot). Also, all the datastores must be visible and accessible from all the hosts at all the time.

- 1. Administratively shutdown one of the two server ports connected to the Fabric Extender A. Make sure that the connectivity is not affected. Upon administratively enabling the shutdown port, the traffic should be rebalanced. This can be validated by clearing interface counters and showing the counters after forwarding some data from virtual machines on the Nexus switches.
- 2. Administratively shutdown both server ports connected to Fabric Extender A. ESXi hosts should be able to use fabric B in this case.
- **3.** Administratively shutdown one of the two data links connected to the storage array from FI. Make sure that the storage is still available from all the ESXi hosts. Upon administratively enabling the shutdown of 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 Cisco UCS Fabric Interconnects while storage and network access from the servers are up. 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. Reboot the active storage processor of the VNX storage array and make sure that all the datastores are still accessible during and after the reboot of the storage processor.
- 6. 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.

I

**7.** Reboot the host in maintenance mode, and remove it from the maintenance mode; this should re-balance the VM distribution across the cluster.

### **Cisco Validation Test Profile**

"vdbench" testing tool was used with Windows Server 2012 to test scaling of the solution in Cisco labs. Table 11 details on the test profile used.

Table 11Test Profile Details

Profile characteristic	Value
Number of virtual machines	300. 600, or 1000
Virtual machine OS	Windows Server 2012
Processors per virtual machine	1
Number of virtual processors per physical CPU core	4
RAM per virtual machine	2 GB
Average storage available for each virtual machine	100 GB
Average IOPS per virtual machine	25 IOPS

## **Bill of Material**

Γ

Table 12 gives the list of the components used in this CVD. The number of actual Cisco UCS servers will vary depending on the size of the architecture. For actual number of servers and chassis, see Table 3.

Table 12 List of Hardware Components Used in the CVD

Description	Part #
Cisco UCS C220M3 Rack Servers	UCSC-C220-M3S
Cisco UCS B200M3 Blade Server	UCSB-B200-M3
CPU for Cisco UCS Servers (2 per server)	UCS-CPU-E52650B
Memory for Cisco UCS Servers (8 per server)	UCS-MR-1X162RY-A
Cisco UCS 1225 VIC Adapter (1 per rack server)	UCSC-PCIE-CSC-02
Cisco UCS 1240 VIC Adapter (1 per blade server)	UCSB-MLOM-40G-01
Cisco UCS 2232PP Fabric Extenders (2)	N2K-C2232PP-10GE
Cisco UCS 2208XP Fabric Extenders (2)	UCS-IOM-2208XP
Cisco UCS 6248UP Fabric Interconnects (2)	UCS-FI-6248UP
Cisco UCS Nexus 5548UP Switches (2)	N5K-C5548UP-FA
10 Gbps SFP+ multifiber mode	SFP-10G-SR

# **Customer Configuration Data Sheet**

Before you start the configuration, gather the customer-specific network and host configuration information. Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, Table 19 provide information on assembling the required network, host address, numbering, and naming information. This worksheet can also be used as a "leave behind" document for future reference.

1

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

### Table 13 Common Server Information

### Table 14ESXi Server Information

Server Name	Purpose	Management	Private Net (storage) addresses	vMotion IP
	ESXi			
	Host 1			
	ESXi			
	Host 2			

Table 15	Array Information
----------	-------------------

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

Description	IP	Subnet Mask	Default Gateway
UCS Manager Virtual IP address			
UCS Fabric Intercon- nect A address			
UCS Fabric Intercon- nect B address			
N5k A management IP address			
N5k B management IP address			
N1kv management IP address			

### Table 16 Network Infrastructure Information

I

Γ

### Table 17VLAN Information

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

### Table 18 VSAN Information

Name	Network Purpose	VSAN ID	Allowed Subnets
Storage	Storage access		

### Table 19Service Accounts

Account	Purpose	Password (optional, secure appropriately)	
	UCS Manager administrator		
	N5k switches administrator		
	N1kv switch administrator		
	Windows Server administrator		
Root	ESXi root		
	Array administrator		
	vCenter administrator		
	SQL Server administrator		

# References

Cisco UCS:

http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified\_computing.html

VMware vSphere:

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

Cisco Nexus 5000 Series NX-OS Software Configuration Guide:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConf igurationGuide.html

EMC VNX 5xxx series resources:

http://www.emc.com/storage/vnx/vnx-series.htm#!resources

Microsoft SQL Server installation guide:

http://msdn.microsoft.com/en-us/library/ms143219.aspx