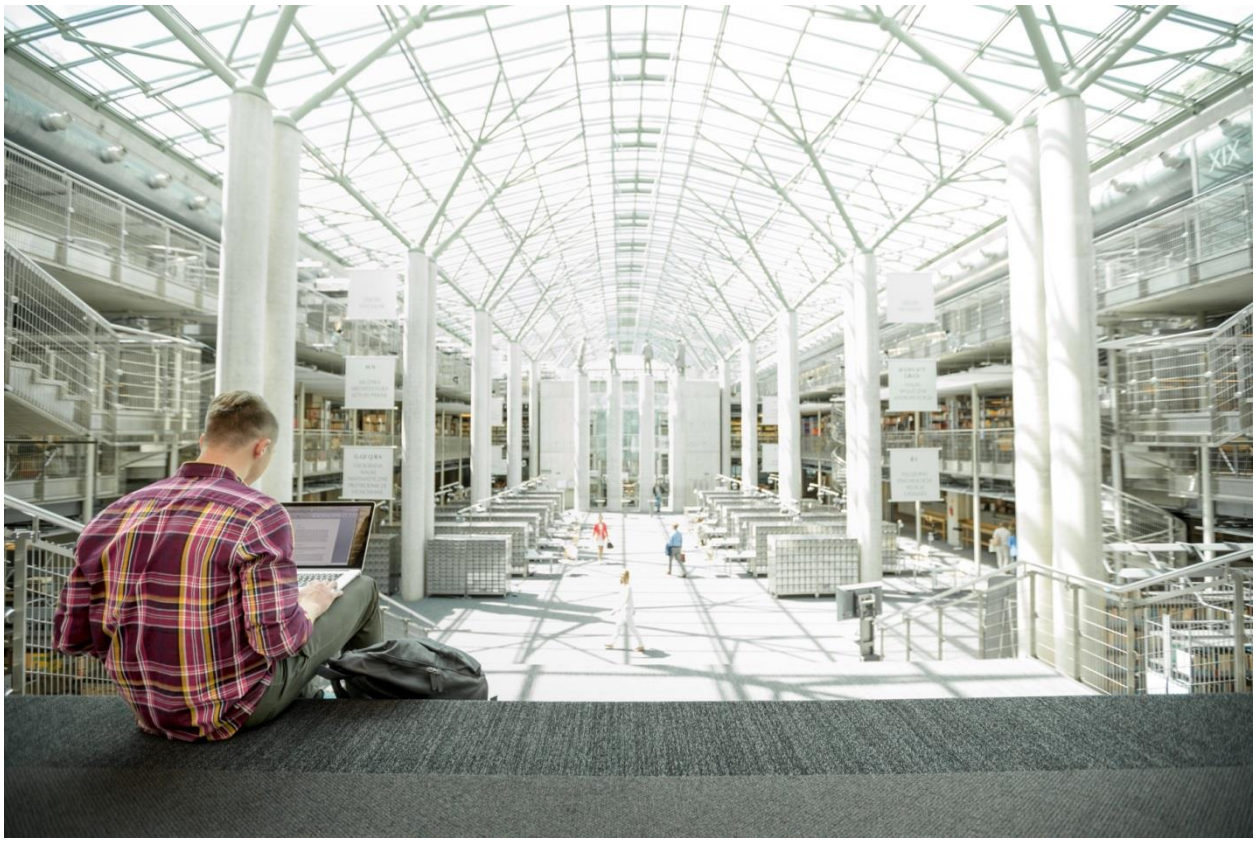


# Cisco UCS Integrated Infrastructure Solutions for SAP Applications

## Design and Deployment of Cisco UCS, Cisco Nexus 9000 Series Switches and EMC VNX Storage

**Last Updated:** July 17, 2017

CISCO VALIDATED DESIGN

# About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit

http://www.cisco.com/go/designzone.

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2016 Cisco Systems, Inc. All rights reserved.

# Table of Contents

About Cisco Validated Designs ..... 2
Table of Contents ..... 3
Executive Summary ..... 11
Solution Overview ..... 12
Introduction ..... 12
Audience ..... 12
Purpose of this Document ..... 12
Business Requirements ..... 12
Solution Summary ..... 13
Technology Overview ..... 15
Cisco Unified Computing System ..... 15
Cisco UCS Manager ..... 15
Fabric Interconnect ..... 16
Cisco UCS 6248UP Fabric Interconnect ..... 16
Cisco UCS 2204XP Fabric Extender ..... 16
Cisco UCS 2208XP Fabric Extender ..... 16
Cisco UCS Blade Server Chassis ..... 17
Cisco UCS B200 M4 Blade Server ..... 17
Cisco C220 M4 Rack-Mount Servers ..... 18
Cisco UCS B260 M4 Blade Server ..... 19
Cisco UCS B460 M4 Blade Server ..... 19
Cisco UCS C460 M4 Rack-Mount Server ..... 20
Cisco C880 M4 Rack-Mount Server ..... 21
Cisco I/O Adapters for Blade and Rack Servers ..... 23
Cisco VIC 1240 Virtual Interface Card ..... 23
Cisco VIC 1280 Virtual Interface Card ..... 24
Cisco VIC 1227 Virtual Interface Card ..... 25
Cisco VIC 1225 Virtual Interface Card ..... 26
Cisco Nexus 9396PX Switch ..... 26
Cisco Nexus 3548 Switches ..... 27
Cisco MDS 9148S 16G Multilayer Fabric Switch ..... 28
Specifications-at-a-Glance ..... 28
Cisco Nexus 1000v Virtual Switch ..... 29

Cisco UCS Differentiators ..... 30
VMware vSphere 5.5 ..... 32
EMC Storage Technologies and Benefits ..... 32
Deployment Hardware and Software ..... 34
Global Hardware Requirements for SAP HANA ..... 34
Network ..... 34
Storage ..... 36
Filesystem Sizes ..... 37
Scale-Up Solution ..... 37
Scale-Out Solutions ..... 37
Log Volume with Intel E7-x890v2 CPU ..... 38
Operating System ..... 38
High Availability ..... 38
Solution Design ..... 39
SAP HANA System on a Single Server–Scale-Up (Bare Metal or Virtualized) ..... 39
SAP HANA System on Multiple Servers–Scale-Out ..... 39
SAP HANA Cloud ..... 40
Private Cloud ..... 40
Public Cloud ..... 41
SAP HANA Hosting ..... 41
Architectural Overview ..... 41
Hardware and Software Components ..... 42
Scaling Options ..... 43
Guidelines for VMware ESXi ..... 47
Memory Configuration Guidelines for Virtual Machines ..... 47
VMware ESX/ESXi Memory Management Concepts ..... 47
Virtual Machine Memory Concepts ..... 47
Allocating Memory to Virtual Machines ..... 48
Storage Guidelines ..... 50
Storage Protocol Capabilities ..... 50
Virtual Networking ..... 50
Storage Best Practices ..... 51
VMware Storage Virtualization ..... 52
Storage Layout ..... 52
Storage Virtualization ..... 52
Cisco UCS Service Profile Design ..... 52

Network High Availability Design....53
Jumbo MTU....54
About Network Path Separation with Cisco UCS....55
Pre-deployment Tasks....58
Customer Configuration Data....59
Solution Configuration Guidelines....60
Install and Configure the Management Pod....61
Device Cabling....61
Cisco Nexus 3548 M1....62
Cisco Nexus 3548 M2....63
Cisco 2911 ISR....64
Configure Domain Name Service (DNS)....65
Network Configuration for Management Pod....65
Cisco Nexus 3500 Configuration....65
Initial Configuration Setup....66
Enable Appropriate Cisco Nexus 3500 Features and Settings....70
Create VLANs for Management Traffic....71
Create VLANs for Nexus 1000v Traffic....72
Create VLANs for ESXi Traffic....72
Configure Virtual Port Channel Domain....73
Configure Network Interfaces for the VPC Peer Links....74
Validate VLAN and VPC Configuration....75
Configure Network Interfaces to Connect the Cisco UCS C220 Management Server with LOM....76
Configure Network Interfaces to Connect the Cisco UCS C220 Management Server with VIC1225....78
Configure Network Interfaces to Connect the Cisco 2911 ISR....79
Configure Network Interfaces to Connect the EMC VNX5400 Storage....80
Configure Network Interfaces for Out of Band Management Access....81
Configure the Port as an Access VLAN Carrying the Out of Band Management VLAN Traffic....82
Configure the Port as an Access VLAN Carrying the Out of Band Management VLAN Traffic....82
Configure Network Interfaces for Access to the Managed Landscape....83
Configure VLAN Interfaces and HSRP....85
Uplink into Existing Network Infrastructure....85
Configure Cisco2911 ISR....85
Management Server Installation....88
Management Server Configuration....89
CIMC Configuration....89

VIC1225 Configuration ..... 91
Local Storage Configuration ..... 95
EMC VNX Storage Configuration ..... 99
Initial Storage Setup ..... 100
Configure Storage Pool ..... 106
Configure Network on the Datamover ..... 112
Create a File System for the NFS Datastore ..... 115
Create NFS-Export for the File Systems ..... 118
VMware ESXi Installation ..... 120
Set Up Management Networking for ESXi Hosts ..... 123
VMware ESXi Configuration with VMware vCenter Client ..... 125
Mount the Datastore ..... 130
VMware Management Tool deployment ..... 131
Deploy the VMware vCenter Server Appliance ..... 132
Install and Configure the Cisco Nexus1000V Virtual Switch Update Manager and Virtual Supervisor Module ..... 144
Install Cisco Nexus 1000v VSM ..... 151
Install and Configure EMC Secure Remote Services ..... 154
Install and Configure the Cisco UCS Integrated Infrastructure ..... 182
Device Cabling ..... 183
Cisco Nexus 9000 A ..... 184
Cisco Nexus 9000 B ..... 185
Cisco MDS 9148 A ..... 187
Cisco MDS 9148 B ..... 188
Cisco UCS 6248 A ..... 190
Cisco UCS 6248 B ..... 192
Cisco Nexus 9000 Configuration ..... 194
Initial Cisco Nexus 9000 Configuration ..... 195
Enable the Appropriate Cisco Nexus 9000 Features and Settings ..... 202
Configure the Spanning Tree Defaults ..... 202
Create VLANs for Management and ESX Traffic ..... 203
Configure Virtual Port Channel Domain ..... 204
Configure Network Interfaces for the VPC Peer Links ..... 206
Configure Network Interfaces to Connect the EMC VNX Storage ..... 209
Configure Network Interfaces for Access to the Management Landscape ..... 214
Configure Administration Port Channels to Cisco UCS Fabric Interconnect ..... 218
Configure Port Channels Connected to Cisco UCS Fabric Interconnects ..... 223

Configure Network Interfaces to the Backup Destination ..... 228
Configure Ports connected to Cisco C880 M4 for VMware ESX ..... 230
Cisco MDS Configuration ..... 232
Cisco MDS Initial Configuration ..... 234
Configure the Management Port ..... 242
Configure Fibre Channel Ports and Port Channels ..... 243
Configure VSANs ..... 247
Configure the Fibre Channel Zoning ..... 255
Cisco UCS Configuration ..... 257
Configure the Cisco UCS Fabric Interconnects ..... 257
Configure LAN Settings ..... 272
Configure SAN Settings ..... 323
Configure Server (Service Profile) Policies and Pools ..... 350
Server Pool for SAP HANA ..... 365
Configure the Service Profile Templates to Run VMware ESXi ..... 372
Instantiate Service Profiles for VMware ESX ..... 380
Create SAN Zones on the MDS Switches ..... 382
Cisco MDS 9148 A ..... 383
Cisco MDS 9148 B ..... 387
EMC VNX Storage Configuration ..... 390
Initial Storage Setup ..... 390
Configure Storage Pool for Operating Systems and Non-SAP HANA Applications ..... 396
Configure LUNs for VMware ESX Hosts ..... 401
Register Hosts and Configure Storage Groups ..... 404
Configure Storage Pools for File ..... 411
Configure Network and File Service ..... 416
Create Additional Network Settings ..... 431
Create NFS Share ..... 432
Software Repository ..... 433
VMware ESXi Host Installation ..... 433
Set Up Management Networking for ESXi Hosts ..... 436
Register and Configure ESX Hosts with VMware vCenter ..... 439
Add Hosts to Cisco Nexus1000V ..... 447
Connect VLAN-Groups to Cisco Nexus1000V ..... 456
Configure Cisco Nexus 1000V ..... 461
Configure Storage Groups for Virtual Machine Templates ..... 464

Mount Datastores ..... 466
Configure ESX-Hosts for SAP HANA ..... 472
Virtual Machine Templates ..... 474
Virtual Machine Template with SUSE Linux Enterprise for SAP Applications ..... 475
Virtual Machine Template with Red Hat Enterprise Linux for SAP HANA ..... 490
Virtual Machine Template with Microsoft Windows ..... 512
Install and Configure Management Tools ..... 532
Install and Configure EMC Solution Enabler SMI Module ..... 532
Install and Configure Cisco UCS Performance Manager ..... 539
Reference Workloads and Use Cases ..... 555
Operating System Installation and Configuration ..... 555
RedHat Enterprise Linux 6 ..... 555
SUSE Linux Enterprise 11 ..... 572
Virtualized SAP HANA Scale-Up System (vHANA) ..... 586
Workload Definition ..... 587
Requirements ..... 587
Create VLANs ..... 587
Check Available VMware Datastore and Available Capacity ..... 597
Create a New Datastore ..... 598
Create Virtual Machine from VM-Template ..... 607
Configure IP Addresses ..... 618
Configure Storage for SAP HANA ..... 618
Install SAP HANA ..... 620
Test the connection to SAP HANA ..... 622
SAP HANA Scale-Up System on a Bare Metal Server (Single SID) ..... 623
Workload Definition ..... 623
Requirements ..... 624
Switch Configuration ..... 624
Cisco UCS Configuration ..... 626
Configure Cisco MDS Switches ..... 636
Configure EMC VNX ..... 640
Install the Operating System ..... 648
Enabling data traffic on vHBA3 and vHBA4 ..... 656
Configure EMC VNX ..... 660
Configure SUSE Linux for SAP HANA ..... 666
Install SAP HANA ..... 669

Test the Connection to SAP HANA ..... 672
SAP HANA Scale-Up System with Multi Database Container ..... 672
Workload Definition ..... 673
Requirements ..... 673
Switch Configuration ..... 674
Cisco UCS Configuration ..... 676
Configure Cisco MDS Switches ..... 680
Configure EMC VNX ..... 684
Install the Operating System ..... 692
Enabling Data Traffic on vHBA3 and vHBA4 ..... 699
Configure EMC VNX ..... 703
Configure SUSE Linux for SAP HANA ..... 709
Install SAP HANA ..... 712
Test the Connection to SAP HANA ..... 713
Install SAP HANA Database Container ..... 714
Configure the Linux Firewall ..... 720
SAP HANA Scale-Up System with SAP HANA Dynamic Tiering ..... 721
Workload Definition ..... 722
Requirements ..... 722
Switch Configuration ..... 723
Cisco UCS Configuration ..... 726
Configure Cisco MDS Switches ..... 738
Configure EMC VNX ..... 743
Install the Operating System ..... 763
Enabling data traffic on vHBA3 and vHBA4 (SAP HANA Node) ..... 773
Configure EMC VNX ..... 777
Install SAP HANA ..... 782
SAP HANA Scale Out System ..... 793
Workload Definition ..... 793
Requirements ..... 793
Switch Configuration ..... 794
Cisco UCS Configuration ..... 796
Configure Cisco MDS Switches ..... 812
Configure EMC VNX ..... 817
Install the Operating System ..... 848
Enabling Data Traffic on vHBA3 and vHBA4 (SAP HANA Node) ..... 856

Configure EMC VNX....863
Install SAP HANA....874
Validating Cisco UCS Integrated Infrastructure with SAP HANA....883
Post Install Checklist....883
Verify the Redundancy of the Solution Components....883
Optional Components....885
Cisco UCS Central....885
Register Cisco UCS Manager with Cisco UCS Central....894
Cisco UCS Platform Emulator....896
Appendix–Solution Variables Data Sheet....905
References....922
About the Authors....923
Acknowledgements....923

# Executive Summary

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

This document describes the architecture and deployment procedures for a Cisco UCS Integrated Infrastructure composed of Cisco compute and network switching products, VMware virtualization and EMC VNX storage components to run Enterprise Applications. Our initial focus is the configuration for SAP HANA Tailored Data Center integration option, as this impacts the solution design most. The solution design is not limited to run SAP HANA; it will also take care that other applications required for an SAP Application landscape can run on the same infrastructure. The intent of this document is to show the configuration principles with the detailed configuration steps based on the individual situation.

# Solution Overview

## Introduction

A cloud deployment model provides a better utilization of the underlying system resources leading to a reduced Total Cost of Ownership (TCO). However, choosing an appropriate platform for Databases and Enterprise Applications like SAP HANA can be a complex task. Platforms should be flexible, reliable and cost effective to facilitate various deployment options of the applications while being easily scalable and manageable. In addition, it is desirable to have an architecture that allows resource sharing across points of delivery (PoD) to address the stranded capacity issues, both within and outside the integrated stack. In this regard, this Cisco Integrated Infrastructure solution for Enterprise Applications provides a comprehensive validated infrastructure platform to suit customers' needs. This document describing the infrastructure installation and configuration to run multiple enterprise applications, like SAP BusinessSuite or SAP HANA, on a shared infrastructure. The use cases to validate the design in this document are all SAP HANA based.

## Audience

The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers deploy the SAP HANA. The reader of this document is expected to have the necessary training and background to install and configure EMC VNX series storage arrays, Cisco Unified Computing System (UCS) and Unified Computing Systems Manager (UCSM), Cisco Nexus 3000 series, Nexus 9000 series and Nexus1000v network switches, or have access to resources with the required knowledge. External references are provided where applicable and it is recommended that the reader be familiar with these documents. Readers are also expected to be familiar with the infrastructure and database security policies of the planned installation.

## Purpose of this Document

This document describes the steps required to deploy and configure a Cisco UCS Integrated Infrastructure for Enterprise Applications with the focus on SAP HANA using VMware 5.5 as hypervisor. Cisco's validation is further confirmation of component compatibility, connectivity and correct operation of the entire integrated stack. This document show cases one variant of cloud architecture for SAP HANA. While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to the deployment of this solution are specifically mentioned.

## Business Requirements

A Cisco CVD provides guidance to create complete solutions that enable you to make informed decisions towards an application ready platform.

Enterprise applications like SAP Business Suite are moving into the consolidated compute, network, and storage environment. Cisco UCS Integrated Infrastructure solution with EMC VNX helps to reduce complexity of configuring every component of a traditional deployment. The complexity of integration management is reduced while maintaining application design and implementation options. Administration is unified, while

process separation can be adequately controlled and monitored. The following are the business requirements for this Cisco UCS Integrated Infrastructure:

- Provide an end-to-end solution to take full advantage of unified infrastructure components.
- Provide a Cisco ITaaS solution for an efficient environment catering to various SAP HANA use cases.
- Show implementation progression of a Reference Architecture design for SAP HANA with results.
- Provide a reliable, flexible and scalable reference design.

## Solution Summary

This Cisco UCS Integrated Infrastructure with EMC VNX storage provides an end-to-end architecture with Cisco, EMC and VMware technologies that demonstrate support for multiple SAP HANA workloads with high availability and server redundancy.

The following are the components used in the design and deployment of this solution:

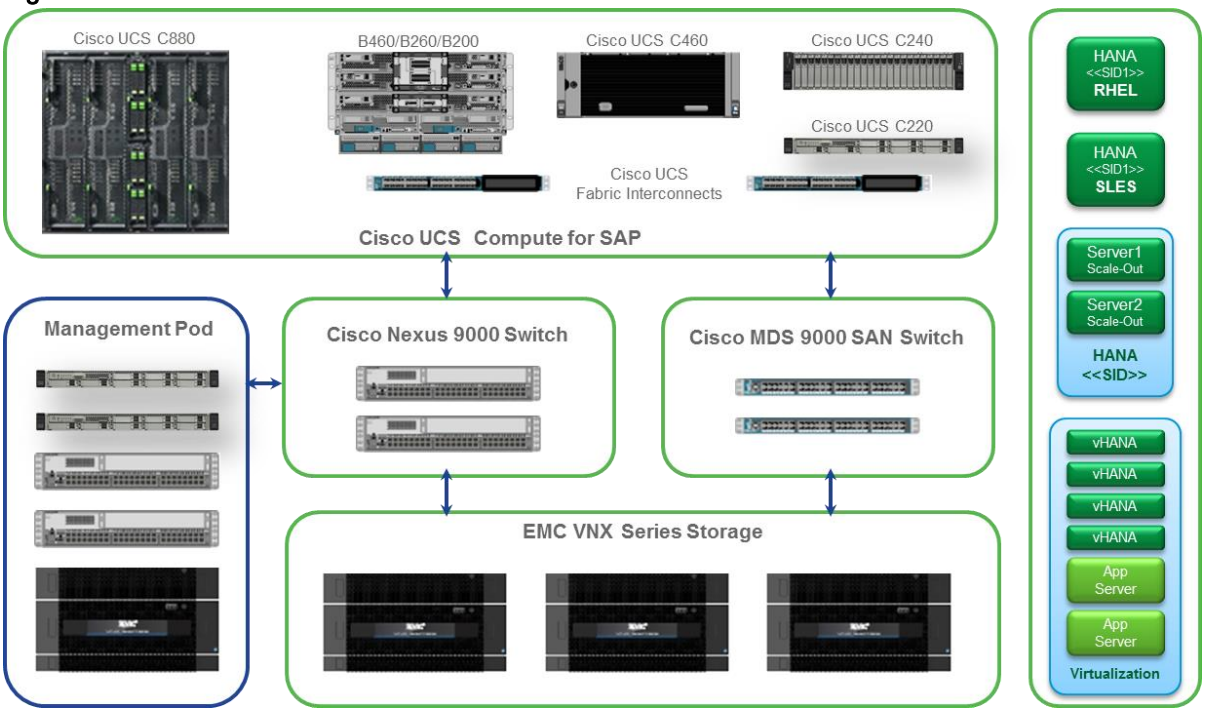
- Cisco Unified Compute System (UCS)
- Cisco UCS B-series or C-series servers, as per customer choice
- Cisco UCS VIC adapters
- Cisco Nexus 9396PX switches
- Cisco MDS 9148S Switches
- Cisco Nexus 1000V virtual switch
- EMC VNX5400 or VNX8000 storage array based on customer needs
- VMware vCenter 5.5
- SUSE Enterprise Linux Server 11 / SUSE Linux Enterprise Server for SAP
- Red Hat Enterprise Linux for SAP HANA

The solution is designed to host scalable, mixed workloads of SAP HANA and other SAP Applications.



The Management Point of Delivery (POD) (Blue border line) in the Solution Design is not part of the Cisco UCS Integrated Infrastructure. To build a manageable solution it is required to specify the management components and the communication paths between all components. In case you have the required management tools already in place, you can go to the section “Install and Configure the Management Pod” to identify the required changes.

Figure 1 Solution Overview



# Technology Overview

## Cisco Unified Computing System

The Cisco Unified Computing System (Cisco UCS) is a state-of-the-art data center platform that unites computing, network, storage access, and virtualization into a single cohesive system.

The main components of Cisco Unified Computing System are:

- Computing - The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers based on Intel Xeon Processor E5 and E7. The Cisco UCS servers offer the patented Cisco Extended Memory Technology to support applications with large datasets and allow more virtual machines (VM) per server.
- Network - The system is integrated onto a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- Virtualization - The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- Storage access - The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying the storage access the Cisco Unified Computing System can access storage over Ethernet (NFS or iSCSI), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This provides customers with 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 Unified Computing System Manager (UCSM) provides unified, embedded management of all software and hardware components of the Cisco UCS 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.

## Fabric Interconnect

These devices provide a single point for connectivity and management for the entire system. Typically deployed as an active-active pair, the system's fabric interconnects integrate all components into a single, highly-available management domain controlled by Cisco UCS Manager. The fabric interconnects manage all I/O efficiently and securely at a single point, resulting in deterministic I/O latency regardless of a server or virtual machine's topological location in the system.

## Cisco UCS 6248UP Fabric Interconnect

Cisco UCS 6200 Series Fabric Interconnects support the system's 10-Gbps unified fabric with low-latency, lossless, cut-through switching that supports IP, storage, and management traffic using a single set of cables. The fabric interconnects feature virtual interfaces that terminate both physical and virtual connections equivalently, establishing a virtualization-aware environment in which blade, rack servers, and virtual machines are interconnected using the same mechanisms. The Cisco UCS 6248UP is a 1-RU Fabric Interconnect that features up to 48 universal ports that can support 10 Gigabit Ethernet, Fibre Channel over Ethernet, or native Fibre Channel connectivity. The Cisco UCS 6296UP packs 96 universal ports into only two rack units.

**Figure 2 Cisco UCS 6248UP Fabric Interconnect**



## Cisco UCS 2204XP Fabric Extender

The Cisco UCS 2204XP Fabric Extender (Figure 3) has four 10 Gigabit Ethernet, FCoE-capable, and Enhanced Small Form-Factor Pluggable (SFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2204XP has thirty-two 10 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gbps of I/O to the chassis.

**Figure 3 Cisco UCS 2204 XP**



## Cisco UCS 2208XP Fabric Extender

The Cisco UCS 2208XP Fabric Extender (0) has eight 10 Gigabit Ethernet, FCoE-capable, and Enhanced Small Form-Factor Pluggable (SFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2208XP has thirty-two 10 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 160 Gbps of I/O to the chassis.

**Figure 4 Cisco UCS 2208 XP**



## Cisco UCS Blade Server 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 2200XP Fabric Extenders.

A passive mid-plane supports up to 2x 40 Gbit Ethernet links to each half-width blade slot or up to 4x 40 Gbit links to each full-width slot. It provides 8 blades with 1.2 terabits (Tb) of available Ethernet throughput for future I/O requirements. Note that the UCS 6324 FI supports only 512 Gbps.

The chassis is capable of supporting future 80 Gigabit Ethernet standards. The Cisco UCS Blade Server Chassis is shown in Figure 5.

**Figure 5 Cisco Blade Server Chassis (front and back view)**



## Cisco UCS B200 M4 Blade Server

Optimized for data center or cloud, the Cisco UCS B200 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the UCS Manager and simplified server access of SingleConnect technology. The Cisco UCS B200 M4 is built with the Intel® Xeon® E5-2600 v3 processor family, up to 768 GB of memory (with 32 GB DIMMs), up to two drives, and up to 80 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco UCS has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B200 M4 Blade Server delivers:

- Suitability for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Half-width form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

**Figure 6 Cisco UCS B200 M4 Blade Server**



## Cisco C220 M4 Rack-Mount Servers

The Cisco UCS C220 M4 Rack-Mount Server is the most versatile, high-density, general-purpose enterprise infrastructure and application server in the industry today. It delivers world-record performance for a wide range of enterprise workloads, including virtualization, collaboration, and bare-metal applications.

The enterprise-class Cisco UCS C220 M4 Rack-Mount Server extends the capabilities of the Cisco Unified Computing System portfolio in a one rack-unit (1RU) form-factor. The Cisco UCS C220 M4 Rack-Mount Server provides the following:

- Dual Intel® Xeon® E5-2600 v3 processors for improved performance suitable for nearly all 2-socket applications
- Next-generation double-data-rate 4 (DDR4) memory and 12 Gbps SAS throughput
- Innovative Cisco UCS virtual interface card (VIC) support in PCIe or modular LAN on motherboard (MLOM) form factor

The Cisco UCS C220 M4 server also offers maximum reliability, availability, and serviceability (RAS) features, including:

- Tool-free CPU insertion
- Easy-to-use latching lid
- Hot-swappable and hot-pluggable components
- Redundant Cisco Flexible Flash SD cards

In Cisco UCS-managed operations, Cisco UCS C220 M4 takes advantage of our standards-based unified computing innovations to significantly reduce customers' TCO and increase business agility.

**Figure 7 Cisco C220 M4 Rack Server**



## Cisco UCS B260 M4 Blade Server

Optimized for data center or cloud, the Cisco UCS B260 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the Cisco UCS Manager and simplified server access of SingleConnect technology. The Cisco UCS B260 M4 is built with the Intel® Xeon® E7-4800 v2 processor family, up to 1.5 Terabyte of memory (with 32 GB DIMMs), up to two drives, and up to 160 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco UCS has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B260 M4 Blade Server delivers the following:

- Suitable for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Full-width form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

**Figure 8 Cisco UCS B260 M4 Blade Server**



## Cisco UCS B460 M4 Blade Server

Optimized for data center or cloud, the Cisco UCS B460 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the Cisco UCS Manager and simplified server access of SingleConnect technology. The UCS B460 M4 is built with the Intel® Xeon® E7-4800 v2 processor family, up to 3 Terabyte of memory (with 32 GB DIMMs), up to two drives, and up to 320 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco UCS has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B460 M4 Blade Server delivers the following:

- Suitable for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Full-width double high form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

**Figure 9 Cisco UCS B460 M4 Blade Server**



## Cisco UCS C460 M4 Rack-Mount Server

The Cisco UCS C460 M4 Rack Server offers industry-leading performance and advanced reliability well suited for the most demanding enterprise and mission-critical workloads, large-scale virtualization, and database applications.

Either as standalone or in Cisco UCS-managed operations, customers gain the benefits of the Cisco UCS C460 M4 server's high-capacity memory when very large memory footprints are required, as follows:

- SAP workloads
- Database applications and data warehousing
- Large virtualized environments
- Real-time financial applications
- Java-based workloads
- Server consolidation

The enterprise-class Cisco UCS C460 M4 server extends the capabilities of the Cisco Unified Computing System portfolio in a four rack-unit (4RU) form-factor. It provides the following:

- Either Two or Four Intel® Xeon® processor E7-4800 v2 or E7-8800 v2 product family CPU
- Up to 6 terabytes (TB)* of Double-data-rate 3 (DDR3) memory in 96 dual in-line memory (DIMM) slots
- Up to 12 Small Form Factor (SFF) hot-pluggable SAS/SATA/SSD disk drives
- 10 PCI Express (PCIe) Gen 3 slots supporting the Cisco UCS Virtual Interface Cards and third-party adapters and GPUs
- Two Gigabit Ethernet LAN-on-motherboard (LOM) ports
- Two 10-Gigabit Ethernet ports
- A dedicated out-of-band (OOB) management port

*With 64GB DIMMs.

The Cisco UCS C460 M4 server also offers maximum reliability, availability, and serviceability (RAS) features, including:

- Tool-free CPU insertion
- Easy-to-use latching lid
- Hot-swappable and hot-pluggable components
- Redundant Cisco Flexible Flash SD cards

In Cisco UCS-managed operations, Cisco UCS C460 M4 takes advantage of our standards-based unified computing innovations to significantly reduce customers' TCO and increase business agility.

**Figure 10 Cisco UCS C460 M4 Rack-Mount Server**



## Cisco C880 M4 Rack-Mount Server

The Cisco C880 M4 Rack-Mount Server offers industry-leading performance and advanced reliability well suited for the most demanding enterprise and mission-critical workloads, large-scale virtualization, and database applications.

As standalone operations, customers gain the benefits of the Cisco C880 M4 server's high-capacity memory when very large memory footprints such as the following are required:

- SAP workloads
- Database applications and data warehousing

The enterprise-class Cisco C880 M4 server extends the capabilities of the Cisco Unified Computing System portfolio in a ten rack-unit (10RU) form-factor. It provides the following:

- Eight Intel® Xeon® processor E7-8800 v2 product family CPU
- Up to 12 terabytes (TB)* of Double-data-rate 3 (DDR3) memory in 192 dual in-line memory (DIMM) slots
- Up to 4 internal Small Form Factor (SFF) hot-pluggable SAS/SATA/SSD disk drives
- Up to 12 PCI Express (PCIe) Gen 3 slots supporting the IO adapters and GPUs
- Four Gigabit Ethernet LAN-on-motherboard (LOM) ports
- Two 10 Gigabit Ethernet LA LAN-on-motherboard (LOM) ports
- A dedicated out-of-band (OOB) management port

*With 64GB DIMMs.

The Cisco C880 M4 server also offers maximum reliability, availability, and serviceability (RAS) features, including:

- Tool-free CPU insertion
- Easy-to-use latching lid
- Hot-swappable and hot-pluggable components

**Figure 11 Cisco C880 M4 Rack-Mount Server**



## Cisco I/O Adapters for Blade and Rack Servers

Cisco Virtual Interface Card (VIC) was developed to provide acceleration for the various new operational modes introduced by server virtualization. The VIC is a highly configurable and self-virtualized adaptor that can create up 256 PCIe endpoints per adapter. These PCIe endpoints are created in the adapter firmware and present fully compliant standard PCIe topology to the host OS or hypervisor.

Each of the PCIe endpoints that the VIC creates can be configured individually with the following attributes:

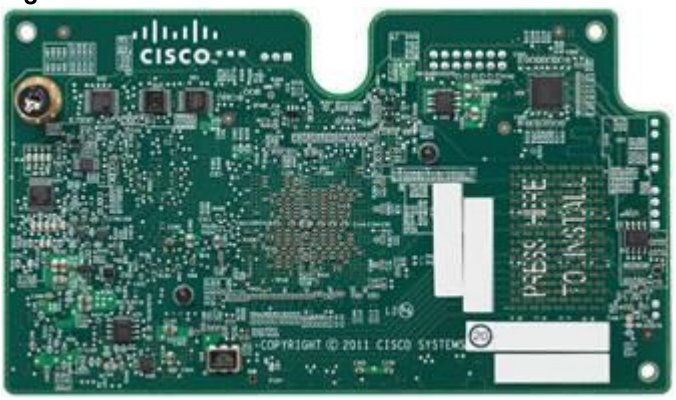
- Interface type: Fibre Channel over Ethernet (FCoE), Ethernet, or Dynamic Ethernet interface device
- Resource maps that are presented to the host: PCIe base address registers (BARs), and interrupt arrays
- Network presence and attributes: Maximum transmission unit (MTU) and VLAN membership
- QoS parameters: IEEE 802.1p class, ETS attributes, rate limiting, and shaping

## Cisco VIC 1240 Virtual Interface Card

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

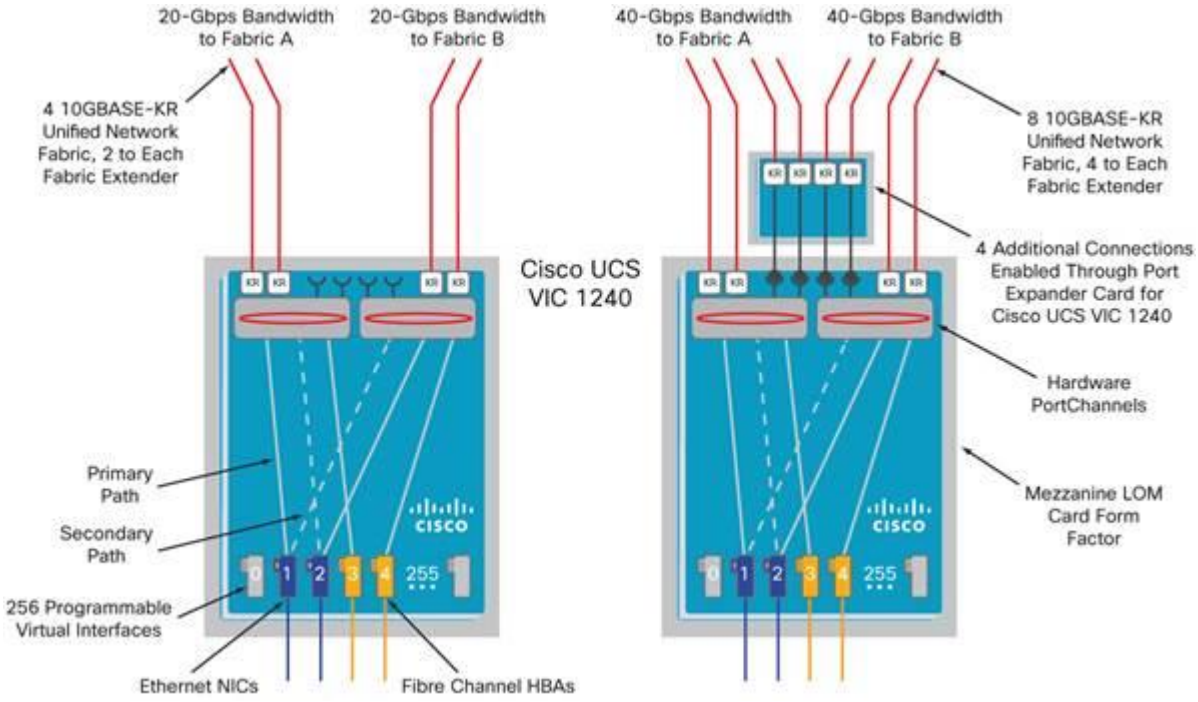
The Cisco UCS Virtual Interface Card (VIC) 1240 (Figure 12) is a 4 x 10-Gbps Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed for the M3 and M4 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1240 capabilities is enabled for eight ports of 10-Gbps Ethernet.

**Figure 12 Cisco UCS 1240 VIC Card**




The Cisco UCS VIC 1240 enables a policy-based, stateless, agile server infrastructure that can present over 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 and management.

**Figure 13 Cisco UCS VIC 1240 Architecture**




## Cisco VIC 1280 Virtual Interface Card

The Cisco UCS blade server has various Converged Network Adapters (CNA) options. The Cisco UCS VIC 1280 Virtual Interface Card (VIC) option is used in this Cisco Validated Design.

The Cisco UCS Virtual Interface Card (VIC) 1280 (Figure 14) is a 8 x 10-Gbps Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed for the M3 and M4 generation of Cisco UCS B-Series Blade Servers.

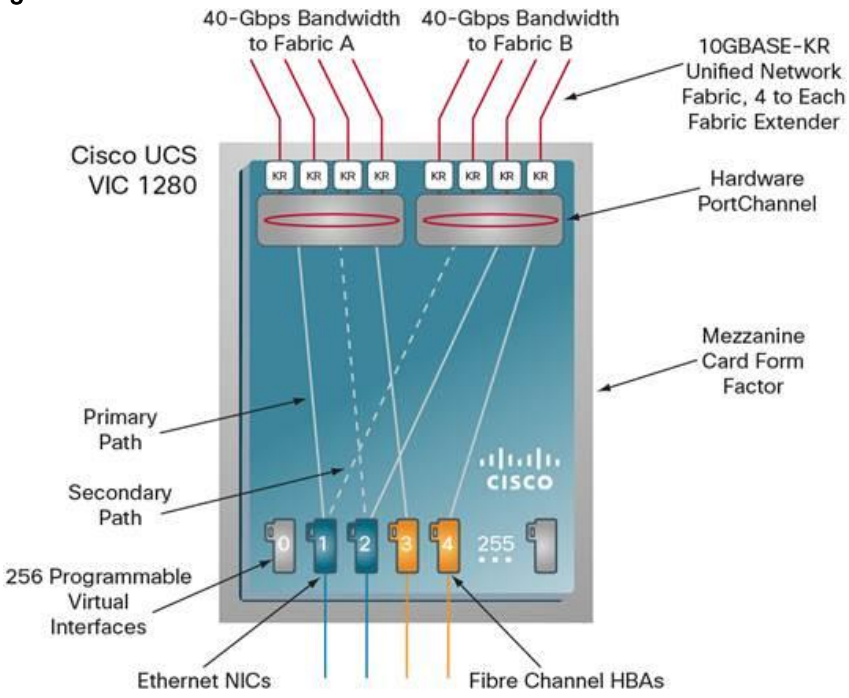
**Figure 14 Cisco UCS 1280 VIC Card**



The Cisco UCS VIC 1280 enables a policy-based, stateless, agile server infrastructure that can present over 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 1280 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 and management.

**Figure 15 Cisco UCS VIC 1280 Architecture**




## Cisco VIC 1227 Virtual Interface Card

The Cisco UCS rack mount server has various Converged Network Adapters (CNA) options. The Cisco UCS 1227 Virtual Interface Card (VIC) is option is used in this Cisco Validated Design.

The Cisco UCS Virtual Interface Card (VIC) 1227 is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter designed exclusively for Cisco UCS C-Series Rack Servers (Figure 11). New to Cisco rack servers, the mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1227 supports Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

Figure 16 Cisco UCS VIC 1227 Card




## Cisco VIC 1225 Virtual Interface Card

The Cisco UCS 1225 Virtual Interface Card (VIC) option is used in this Cisco Validated Design to connect the Cisco UCS C460 M4 Rack server.

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. Cisco 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 17 Cisco UCS VIC 1225 Card



## Cisco Nexus 9396PX Switch

The Cisco Nexus 9000 family of switches supports two modes of operation: NXOS standalone mode and Application Centric Infrastructure (ACI) fabric mode. In standalone mode, the switch performs as a typical Cisco Nexus switch with increased port density, low latency and 40G connectivity. In fabric mode, the administrator can take advantage of Cisco ACI.

The Cisco Nexus 9396PX is a 2RU switch which delivers comprehensive line-rate layer 2 and layer 3 features in a two-rack-unit form factor. It supports line rate 1/10/40 GE with 960 Gbps of switching capacity. It is ideal for top-of-rack and middle-of-row deployments in both traditional and Cisco Application Centric Infrastructure (ACI)–enabled enterprise, service provider, and cloud environments.

### Specifications-at-a-Glance

- Forty-eight 1/10 Gigabit Ethernet Small Form-Factor Pluggable (SFP+) non-blocking ports
- Twelve 40 Gigabit Ethernet Quad SFP+ (QSFP+) non-blocking ports
- Low latency (approximately 2 microseconds)
- 50 MB of shared buffer
- Line rate VXLAN bridging, routing, and gateway support
- Fibre Channel over Ethernet (FCoE) capability
- Front-to-back or back-to-front airflow

**Figure 18 Cisco Nexus 9396PX Switch**



## Cisco Nexus 3548 Switches

The Cisco Nexus 3548 and 3524 Switches are based on identical hardware, differentiated only by their software licenses, which allow the Cisco Nexus 3524 to operate 24 ports, and enable the use of all 48 ports on the Cisco Nexus 3548. These fixed switches are compact one-rack-unit (1RU) form-factor 10 Gigabit Ethernet switches that provide line-rate Layer 2 and 3 switching with ultra-low latency. Both software licenses run the industry-leading Cisco NX-OS Software operating system, providing customers with comprehensive features and functions that are deployed globally. The Cisco Nexus 3548 and 3524 contain no physical layer (PHY) chips, allowing low latency and low power consumption.

The Cisco Nexus 3548 and 3524 have the following hardware configuration:

- 48 fixed Enhanced Small Form-Factor Pluggable (SFP+) ports (1 or 10 Gbps); the Cisco Nexus 3524 enables only 24 ports
- Dual redundant hot-swappable power supplies
- Four individual redundant hot-swappable fans
- One 1-PPS timing port, with the RF1.0/2.3 QuickConnect connector type*
- Two 10/100/1000 management ports

- One RS-232 serial console port
- One USB port
- Locator LED
- Locator LED button
- Front-to-back or back-to-front airflow

**Figure 19 Cisco Nexus 3548 switch**



## Cisco MDS 9148S 16G Multilayer Fabric Switch

The Cisco MDS 9148S 16G Multilayer Fabric Switch is the next generation of the highly reliable Cisco MDS 9100 Series Switches. It includes up to 48 auto-sensing line-rate 16-Gbps Fibre Channel ports in a compact easy to deploy and manage 1-rack-unit (1RU) form factor. In all, the Cisco MDS 9148S is a powerful and flexible switch that delivers high performance and comprehensive Enterprise-class features at an affordable price.

### Features and Capabilities

- Flexibility for growth and virtualization
- Optimized bandwidth utilization and reduced downtime
- Enterprise-class features and reliability at low cost
- PowerOn Auto Provisioning and intelligent diagnostics
- In-Service Software Upgrade and dual redundant hot-swappable power supplies for high availability
- High-performance inter-switch links with multipath load balancing

## Specifications-at-a-Glance

### Performance and Port Configuration

- 2/4/8/16-Gbps auto-sensing with 16 Gbps of dedicated bandwidth per port
- Up to 256 buffer credits per group of 4 ports (64 per port default, 253 maximum for a single port in the group)
- Supports configurations of 12, 24, 36, or 48 active ports, with pay-as-you-grow, on-demand licensing

Figure 20 Cisco MDS9148S 16G Fabric Switch



## Cisco Nexus 1000v Virtual Switch

The Cisco Nexus 1000V Series Switches are virtual machine access switches for the VMware vSphere environments running the Cisco NX-OS operating system. Operating inside the VMware ESX or ESXi hypervisors, the Cisco Nexus 1000V Series provides:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Non-disruptive operational model for your server virtualization and networking teams

When server virtualization is deployed in the data center, virtual servers typically are not managed the same way as physical servers. Server virtualization is treated as a special deployment, leading to longer deployment time, with a greater degree of coordination among server, network, storage, and security administrators. With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the virtual machine access layer to the core of the data center network infrastructure. Virtual servers can now use the same network configuration, security policy, diagnostic tools, and operational models as their physical server counterparts attached to dedicated physical network ports.

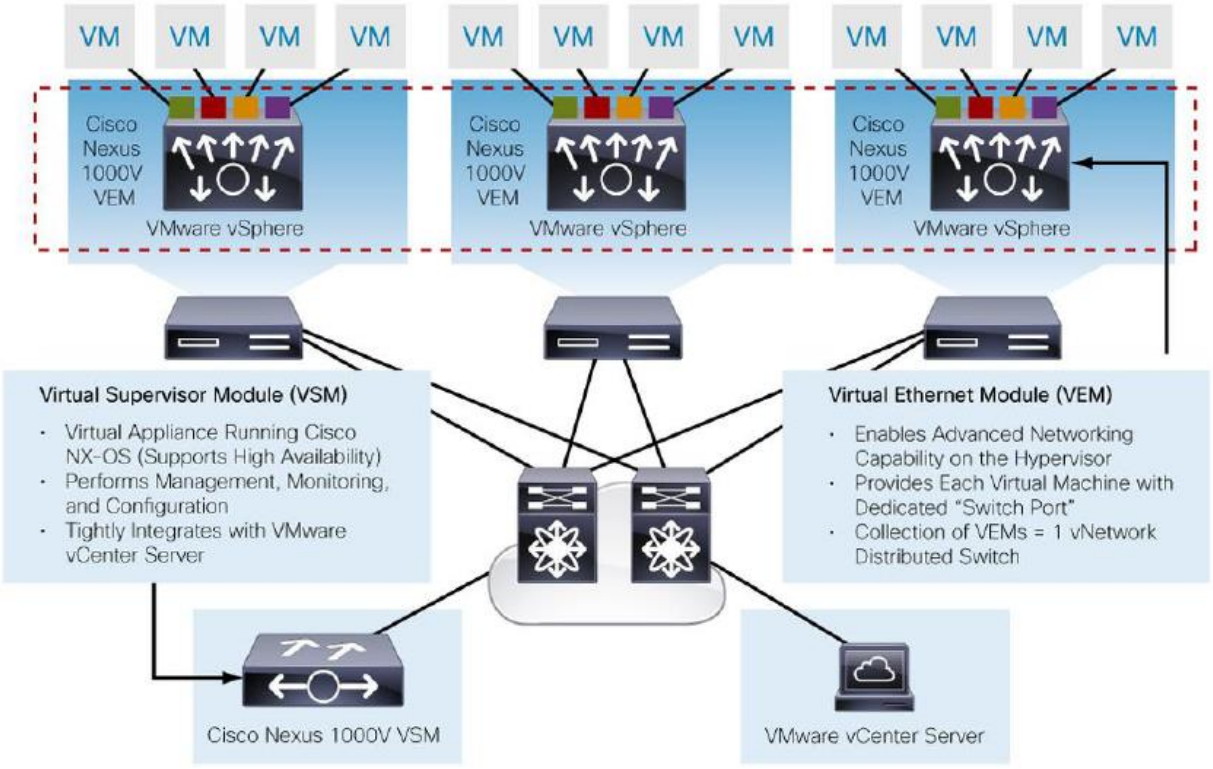
Virtualization administrators can access predefined network policies that follow mobile virtual machines to ensure proper connectivity saving valuable time to focus on virtual machine administration. This comprehensive set of capabilities helps you to deploy server virtualization faster and realize its benefits sooner.

Cisco 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 21 Cisco Nexus 1000v virtual Distributed Switch Architecture




## Cisco UCS Differentiators

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

- Embedded management: In Cisco UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating 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 provides enormous scaling on management plane.
- Unified fabric: In Cisco 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.
- 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. Combination of unified fabric and auto-discovery enables wire-once architecture of Cisco UCS, where compute capability of Cisco UCS can extending easily while keeping the existing external connectivity to LAN, SAN and management networks.
- Policy based resource classification: When a compute resource is discovered by Cisco 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 show cases the policy based resource classification of Cisco UCS Manager.

- Combined Rack and Blade server management: Cisco UCS Manager can manage B-series blade servers and C-series rack server under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic. In this CVD, we are show-casing combination of B and C series servers to demonstrate stateless and form factor independent computing work load.
- Model based management architecture: Cisco UCS Manager architecture and management database is model based and data driven. Open, standard based XML API is provided to operate on the management model. This enables easy and scalable integration of Cisco UCS Manager with other management system, such as VMware vCloud director, Microsoft system center, and Citrix CloudPlatform.
- Policies, Pools, Templates: Management approach in Cisco UCS Manager is based on defining policies, pools and templates, instead of cluttered configuration, which enables simple, loosely coupled, data driven approach in managing compute, network and storage resources.
- Loose referential integrity: In Cisco UCS Manager, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each-other. This provides great flexibilities where different experts from different domains, such as network, storage, security, server and virtualization work together to accomplish a complex task.
- Policy resolution: In Cisco 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 other policy by name is resolved in the org hierarchy with closest policy match. If a policy with a specific name is not found in the hierarchy until root org, then special policy named “default” is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibilities to owners of different orgs.
- Service profiles and stateless computing: Service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.
- Built-in multi-tenancy support: Combination of policies, pools and templates, loose referential integrity, policy resolution in org hierarchy and service profile based approach to compute resources makes Cisco UCS Manager inherently friendly to multi-tenant environment typically observed in private and public clouds.
- Virtualization aware network: VM-FEX technology makes access layer of network aware about host virtualization. This prevents domain pollution of compute and network domains with virtualization when virtual network is managed by port-profiles defined by the network administrators team. VM-FEX also offloads hypervisor CPU by performing switching in the hardware, thus allowing hypervisor CPU to do more virtualization related tasks. VM-FEX technology is well integrated with VMware vCenter, Linux KVM and Hyper-V SR-IOV to simplify cloud management.

- Simplified QoS: Even though the fibre-channel and Ethernet are converged in Cisco UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in Cisco UCS Manager by representing all system classes in one GUI panel.

## VMware vSphere 5.5

VMware vSphere 5.5 is a next-generation virtualization solution from VMware which builds upon ESXi 5.1 and provides greater levels of scalability, security, and availability to virtualized environments. vSphere 5.5 offers improvements in performance and utilization of CPU, memory, and I/O. It also offers users the option to assign up to thirty two virtual CPU to a virtual machine–giving system administrators more flexibility in their virtual server farms as processor-intensive workloads continue to increase.

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

## EMC Storage Technologies and Benefits

The EMC VNX™ 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 Fibre Channel protocol based on the best practices and use case requirements. EMC VNX series storage arrays have 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™ for a single management interface for all network-attached storage (NAS), storage area network (SAN), and replication needs

- Software suites available:
  - 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 available:
  - Total Value Pack – Includes all protection software suites and the Security and Compliance Suite

# Deployment Hardware and Software

## Global Hardware Requirements for SAP HANA

There are hardware and software requirements defined by SAP Societas Europaea (SE) to run SAP HANA systems. Follow the guidelines provided by SAP documentation at http://saphana.com for SAP HANA appliances and the Tailored Datacenter Integration (TDI) option. Please check the documents regularly as SAP SE can change requirements on demand.

A list of certified server for SAP HANA is published at http://global.sap.com/community/ebook/2014-09-02-hana-hardware/enEN/index.html. All Cisco UCS server listed there can be used in this Reference Architecture as the solution design is not based on the server type – this includes server models introduced after the publication of this document. The servers listed in the "Supported Entry Level Systems" are for SAP HANA Scale-Up configurations with the SAP HANA Tailored Datacenter Integration (TDI) option only.

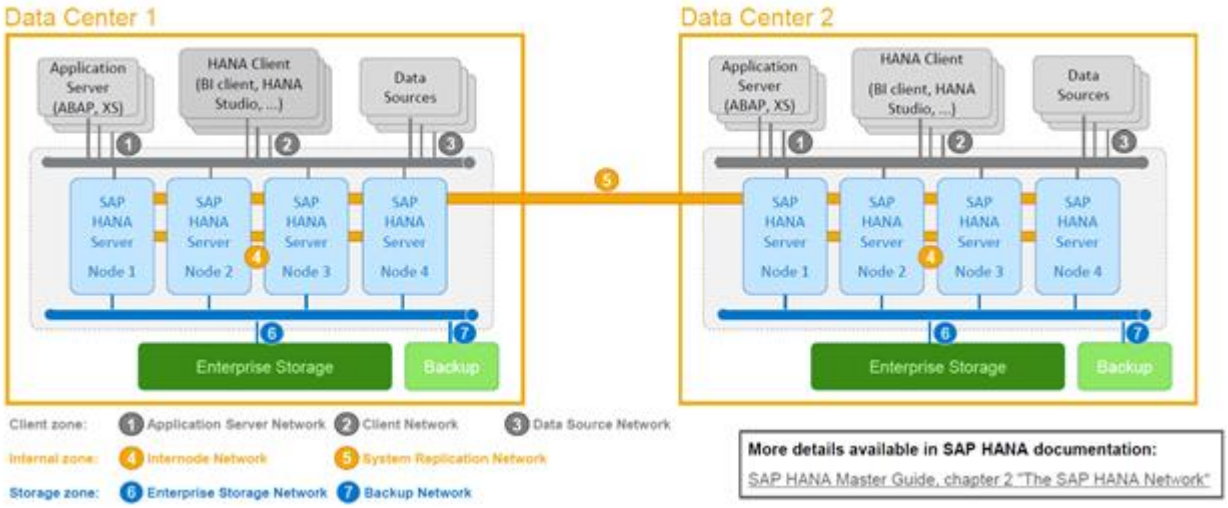
### Network

A SAP HANA data center deployment can range from a database running on a single host to a complex distributed system with multiple hosts located at a primary site and one or more secondary sites and supporting a distributed multi-terabyte database with full fault and disaster recovery.

SAP HANA has different types of network communication channels to support the different SAP HANA scenasrios and setups, as follows:

- Client zone: Channels used for external access to SAP HANA functions by end-user clients, administration clients, and application servers, and for data provisioning through SQL or HTTP
- Internal zone: Channels used for SAP HANA internal communication within the database or, in a distributed scenario, for communication between hosts
- Storage zone: Channels used for storage access (data persistence) and for backup and restore procedures

Figure 22 High-Level SAP HANA Network Overview




Details about the network requirements for SAP HANA are available from the white paper from SAP at: http://www.saphana.com/docs/DOC-4805.

Table 1 lists networks defined by SAP, Cisco, or requested by customers.

Table 1 List of Known Networks

| Name | Use Case | Solutions | Bandwidth requirements |
|---|---|---|---|
| Client Zone Networks | | | |
| Application Server Network | SAP Application Server to DB communication | All | 1 or 10 GbE |
| Client Network | User / Client Application to DB communication | All | 1 or 10 GbE |
| Data Source Network | Data import and external data integration | Optional for all SAP HANA systems | 1 or 10 GbE |
| Internal Zone Networks | | | |
| Inter-Node Network | Node to node communication within a scale-out configuration | Scale-Out | 10 GbE |
| System Replication Network | SAP HANA System Replication | For SAP HANA Disaster Tolerance | TBD with Customer |
| Storage Zone Networks | | | |

| Name | Use Case | Solutions | Bandwidth requirements |
|---|---|---|---|
| Backup Network | Data Backup | Optional for all SAP HANA systems | 10 GbE or 8 GBit FC |
| Storage Network | Node to Storage communication | Scale-Out<br>Storage TDI | 10 GbE or 8 GBit FC network |
| Infrastructure Related Networks | | | |
| Administration Network | Infrastructure and SAP HANA administration | Optional for all SAP HANA systems | 1 GbE |
| Boot Network | Boot the Operating Systems via PXE/NFS or FCoE | Optional for all SAP HANA systems | 1 GbE |

All networks need to be properly segmented and may be connected to the same core/ backbone switch. It depends on the customer's high-availability requirements if and how to apply redundancy for the different SAP HANA network segments.



Network security and segmentation is a function of the network switch and must be configured according to the specifications of the switch vendor.

Based on the listed network requirements every server must be equipped with 2x 1/10 Gigabit Ethernet (10 GbE is recommended) for Scale-Up systems to establish the communication with the application or user (Client Zone). If the storage for HANA is external and accessed via the Network two additional 10 GbE Interfaces are required for the Storage Zone.

For Scale-Out solutions an additional redundant network for the HANA node to HANA node communication with ≥10 GbE is required (Internal Zone).

## Storage

The storage used must be listed as part of a "Certified Appliance" in the Certified SAP HANA Hardware Directory at http://global.sap.com/community/ebook/2014-09-02-hana-hardware/enEN/index.html. The storage is only listed in the detail description of a certified solution. Click the entry in the Model Column to see the details. The storage can also be listed as Certified Enterprise Storage based on SAP HANA TDI option at the same URL in the "Certified Enterprise Storage" tab.

All relevant information about storage requirements is documented in the white paper "SAP HANA Storage Requirements" and is available at: http://www.saphana.com/docs/DOC-4071.



It is important to know that SAP makes no difference between a virtualized SAP HANA system with 64GB memory and a physical installed SAP HANA system with 2TB memory in regards to storage requirements.

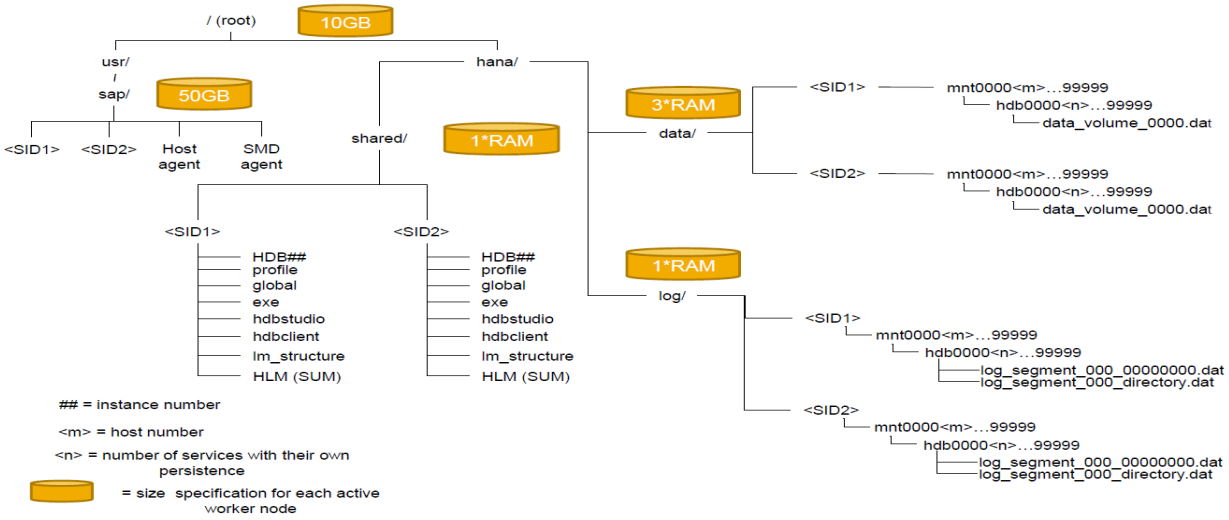
If the storage is certified i.e. 4 nodes, you can run 4 VMs, or 4 bare metal systems, or a mixture of them on this storage.

Using the same storage for multiple applications can cause a significant performance degradation of the SAP HANA systems and the other applications. It is recommended to separate the storage for SAP HANA systems from the storage for other applications. It is required to specify the storage options together with your storage vendor based on your requirements.

## Filesystem Sizes

To install and operate SAP HANA the following file system layout and sizes must be provided.

**Figure 23 File System Layout for SAP HANA**




The recommendation from SAP about the file system layout for a SAP HANA TDI option differs from the one shown in Figure 23. For /hana/data the minimum size is 1* RAM instead of 3* RAM; the recommended size is 1.5* RAM.

## Scale-Up Solution

The following is a sample of a system with 512GB memory:

| | |
|---|---|
| Root-FS: | 50 GB |
| /usr/sap: | 50 GB |
| /hana/log: | 1x Memory (512 GB) |
| /hana/data: | 1x memory (512 GB) |

## Scale-Out Solutions

The following is a sample of a solution with 512GB memory per server:

For each server:

Root-FS: 50 GB

/usr/sap: 50 GB

/hana/shared: # of Nodes * 512 GB (2+0 configuration sample: 2x 512 GB = 1024 GB)

For every active HANA node:

/hana/log/<SID>/mntXXXXX: 1x Memory (512 GB)

/hana/data/<SID>/mntXXXXX: 1x Memory (512 GB)

## Log Volume with Intel E7-x890v2 CPU

For solutions based on Intel E7-x890v2 CPU the size of the Log volume has changed:

- ½ or the server memory for systems ≤ 256 GB memory
- Min 512 GB for systems with ≥ 512 GB memory

## Operating System

The supported operating systems for SAP HANA are as follows:

- SUSE Linux Enterprise 11
- SUSE Linux Enterprise for SAP Applications
- Red Hat Enterprise Linux for SAP HANA

## High Availability

SAP HANA scale-out comes with in integrated high-availability function. If the SAP HANA system is configured with a stand-by node, a failed part of SAP HANA will start on the stand-by node automatically. The infrastructure for a SAP HANA scale-out solution must have no single point of failure. After a failure in the components, the SAP HANA database must still be operational and running. For automatic host failover, the proper implementation and operation of the SAP HANA storage connector application programming interface (API) must be used.

Hardware and software components should include the following:

- Internal storage: A RAID-based configuration is preferred.
- External storage: Redundant data paths, dual controllers, and a RAID-based configuration are preferred.
- Ethernet switches: Two or more independent switches should be used.

For the latest information from SAP go to: http://saphana.com or http://service.sap.com/notes.

# Solution Design

Since there are multiple implementation options, it is important to define the requirements before starting to bring the solution components together. This section sets the basic definition, and later in the document, we will refer to these definitions.

## SAP HANA System on a Single Server–Scale-Up (Bare Metal or Virtualized)

A single-host system is the simplest system installation type. It is possible to run an SAP HANA system entirely on one host and then scale the system up as needed. A scale-up solution is, for some SAP HANA use cases the only supported option. All data and processes are located on the same server and can be accessed locally, and no network communication to other SAP HANA nodes is required. In general it provides the best SAP HANA performance

The network requirements for this option depend on the client and application access and storage. If you do not require system replication or a backup network, one 1 Gigabit Ethernet (access) and one 10 Gigabit Ethernet storage networks are sufficient to run SAP HANA Scale-Up.

For virtualized SAP HANA installation, please remember that hardware components are shared like network interfaces. It is recommended to use dedicated network adapters per virtualized SAP HANA system.

Based on the SAP HANA TDI option for shared storage and a shared network, you can build a solution to run multiple SAP HANA Scale-Up systems on a shared infrastructure.

## SAP HANA System on Multiple Servers–Scale-Out

You should use a scale-out solution if the SAP HANA system does not fit into the main memory of a single server based on the rules defined by SAP. You can scale SAP HANA either by increasing RAM for a single server, or by adding hosts to the system to deal with larger workloads. This allows you to go beyond the limits of a single physical server. This means combining multiple independent servers into one system. The main reason for distributing a system across multiple hosts that is, scaling out is to overcome the hardware limitations of a single physical server. This means that an SAP HANA system can distribute the load between multiple servers. In a distributed system, each index server is usually assigned to its own host to achieve maximum performance. It is possible to assign different tables to different hosts (partitioning the database), as well as to split a single table between hosts (partitioning of tables). Distributed systems can be used for failover scenarios and to implement high availability. Individual hosts in a distributed system have different roles master, worker, slave, standby depending on the task.



Some use cases are either not supported or not fully supported on scale-out solutions. Please check with SAP if your use case can be deployed on a scale-out solution.

The network requirements for this option are higher than for scale-up systems. In addition to the client and application access and storage access network, you also must have a node-to-node network. If you do not need system replication or a backup network, one 10 Gigabit Ethernet (access) and one 10 Gigabit Ethernet

(node-to-node) and one 10 Gigabit Ethernet storage networks are required to run SAP HANA in a scale-out configuration.

Based on the SAP HANA TDI option for shared storage and shared network, you can build a solution to run multiple SAP HANA scale-out systems on a shared infrastructure.



Virtualized SAP HANA Scale-Out is not supported by SAP as of December 2014.

## SAP HANA Cloud

One reason for the popularity of SAP HANA is the option to deploy it in a cloud model. There are hundreds of interpretations of cloud. To set the scope for this document, three very high-level areas that are relevant for SAP HANA have been designed:

- Private Cloud, offered from the IT department to multiple customers within the same company
- Public Cloud, where SAP HANA is offered through a website, based on a global service description, by which you can get it just by a few mouse clicks and your credit card information
- SAP HANA Hosting, where a service provider runs the SAP HANA system based on an individual contract that includes a service-level agreement (SLA) about availability, performance, and security
- The cloud model affects the infrastructure setup and configuration in a variety of ways. The following are some examples: The performance requirements will define how many SAP HANA systems can run on the same hypervisor, storage, or network.
- The security requirements will influence whether or not you must run on dedicated hardware; that is, whether or not you must dedicate the physical host, the storage system, or the network equipment.

The availability requirements will influence how SAP HANA is deployed in the data center(s), the requirements for infrastructure or application clustering, and the data-replication technology and backup and restore procedures.

The network requirements for SAP HANA in a cloud environment are a combination of the requirements for SAP HANA scale-up and scale-out systems. You also can consider a very basic implementation of security and network traffic separation.

The storage requirements are not easy to define. On one side are the performance requirements for SAP HANA and the other applications. On the other side are requirements such as backup location, data mobility, and multi–data center concepts, and so on. These requirements must follow the data center best practices that are already in place.

### Private Cloud

Private cloud for or with SAP HANA represents a very broad area of options. You can have a Solution for Multiple SAP HANA Systems – Scale-Up (bare metal or virtualized) with additional automation tools to provide a flexible and easy way to provision and de-provision SAP HANA systems. You can also use an already existing infrastructure for virtual desktop infrastructure (VDI) or other traditional applications and add

SAP HANA to it. In most private-cloud deployments SAP HANA is not the only application that will run on the shared infrastructure.

### Public Cloud

A public-cloud solution is used to run many small to medium-size SAP HANA systems; most of those systems are virtualized and the solution is 100-percent automated. A self-service portal for the end customer is used to request, deploy, and operate the SAP HANA system. There are no individual SLAs; you have to accept the predefined agreement to close the contract.

### SAP HANA Hosting

A solution for SAP HANA hosting is used to run small to large-size SAP HANA systems; some are virtualized, some are bare metal scale-up, and some are scale-out. The solution is automated to a level that makes sense for the owner. A self-service portal for the end customer is not mandatory, but can be in place. Individual contracts are created, with a dedicated SLA per end customer. The infrastructure must be able to provide the best flexibility based on the individual performance, security, and availability requirements of the end customers.

## Architectural Overview

This Cisco UCS Integrated Infrastructure is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized SAP HANA solutions. The architecture includes EMC VNX storage, Cisco Nexus® networking, the Cisco Unified Computing System™ (Cisco UCS®), and VMware vSphere software. The design is flexible enough that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.

One benefit of this architecture is the ability to customize or scale the environment to suit a customer's requirements. This design can easily scale as requirements and demand change. The unit can scale both up and out. The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an integrated solution. A storage system capable of serving multiple protocols allows for customer choice and investment protection because it truly is a wire-once architecture.

This CVD focuses on the architecture to run SAP HANA as the main workload, targeted for Enterprise and Service Provider segment, using EMC VNX storage arrays.  The architecture uses Cisco UCS with B-series and C-series servers with EMC VNX5400 or VNX8000 storage attached to the Nexus 9396PX switches for NFS access and to the Cisco MDS 9148S switches for Fibre Channel access. The C-Series rack servers are connected directly to Cisco UCS Fabric Interconnect with single-wire management feature. VMware vSphere 5.5 is used as server virtualization architecture. This infrastructure is deployed to provide SAN-booted hosts with file-level and block-level access to shared storage. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

## Hardware and Software Components

Table 2 lists the various hardware and software components, which occupies different tiers of the Cisco UCS Integrated Infrastructure under test.

**Table 2 List of Hardware and Software Components**

| Vendor | Product | Version | Description |
|---|---|---|---|
| Cisco | UCSM | 2.2(3f) | UCS Manager |
| Cisco | UCS 6248UP FI | 5.2(3)N2(2.23c) | UCS Fabric Interconnects |
| Cisco | UCS 5108 Chassis | NA | UCS Blade server chassis |
| Cisco | UCS 2200XP FEX | 2.2(3f) | UCS Fabric Extenders for Blade Server chassis |
| Cisco | UCS B-Series M4 servers | 2.2(3f) | Cisco B-Series M4 blade servers |
| Cisco | UCS VIC 1240/1280 | 4.0(1b) | Cisco UCS VIC 1240/1280 adapters |
| Cisco | UCS C220 M4 servers | 2.0.3i – CIMC<br>C220M4.2.0.3d – BIOS | Cisco C220 M4 rack servers |
| Cisco | UCS C240 M4 servers | 2.0.3i – CIMC<br>C240M4.2.0.3d – BIOS | Cisco C240 M4 rack servers |
| Cisco | UCS VIC 1227 | 4.0(1b) | Cisco UCS VIC adapter |
| Cisco | UCS C460 M4 servers | 2.0.3i – CIMC<br>C460M4.2.0.3c - BIOS | Cisco C460 M4 rack servers |
| Cisco | UCS VIC 1225 | 4.0(1b) | Cisco UCS VIC adapter |
| Cisco | MDS 9148 | 6.2(9) | Cisco MDS 9148 8G Multi Fabric switches |
| Cisco | Nexus 9396PX | 6.1(2)I2(2a) | Cisco Nexus 9396x switches |
| Cisco | Nexus 1000v | 5.2.1.SV3.1.2 | Cisco Nexus 1000v virtual switch. |

| Vendor | Product | Version | Description |
|---|---|---|---|
| EMC | VNX5400 | - | VNX storage array |
| EMC | VNX8000 | - | VNX storage array |
| VMware | ESXi 5.5 | 5.5 Update 2 | Hypervisor |
| VMware | vCenter Server | 5.5 | VMware Management |
| SUSE | SUSE Linux Enterprise Server (SLES) | 11 SP3 | Operating System to host SAP HANA |
| Red Hat | Red Hat Enterprise Linux (RHEL) for SAP HANA | 6.6 | Operating System to host SAP HANA |

**Table 3 Cisco UCS B220M4 or C220M4 Server Configuration (per server basis)**

| Component | Capacity |
|---|---|
| Memory (RAM) | 256 GB (16 x 16GB DDR4 DIMMs) |
| Processor | 2 x Intel® Xeon ® E5-2660 v3 CPUs, 2.6 GHz, 10 cores, 20 threads |

**Table 4 Cisco UCS B460M4 or C460M4 server configuration (per server basis)**

| Component | Capacity |
|---|---|
| Memory (RAM) | 1024 GB (64x 16GB DDR4 DIMMs) |
| Processor | 4 x Intel® Xeon ® E7-4880 v2 CPUs, 2.4 GHz, 15 cores, 30 threads |

## Scaling Options

This is one of the most difficult topics to define for a solution based on multiple components hosting multiple use-cases. The CPU and memory requirements per server to run the application gives you the information what must run on bare-metal and what can be virtualized. For virtualized workloads, the number of parallel running virtual machines per server is limited by the available CPU and memory resources. The IO requirements from the server to the Cisco UCS Fabric Interconnects for network and storage access and from the Cisco UCS Fabric Interconnects to the upstream LAN and SAN switches will define the required number of cables. The number of ports on the Cisco UCS Fabric Interconnect is limiting the number of servers managed by a single domain. The number of possible Cisco UCS Domains and EMC Storages

attached to the SAN switches are limited by the model and the number of Cisco MDS switches. And the same logic applies also to the LAN switches, limited by the number and model of Nexus 9000 series switches used for this deployment.

In the “Reference Workloads and Use Cases” section later in this document, the base line requirements are defined case by case. With this information together with the basic requirements documented by SAP and the planned use of the infrastructure a basic sizing can be done.

Example 1: If you plan to install two very large SAP HANA systems with 80TB main memory each you need 2x 40 B460 M4 with 2TB each. Based on the IO requirements for SAP HANA Scale-Out it is necessary to use server from two or more Cisco UCS for a single SAP HANA system. A single Cisco UCS is limited to 30 servers to provide the required performance on all layers.

Example 2: If you plan to install many of SAP HANA systems with 64GB or 128GB main memory, mostly non-productive, the IO requirements are different. For this deployment it is possible to run 400 or more SAP HANA systems on a single Cisco UCS with 100 or more server.

One of the most important tasks of the daily operation is the check if there are bottlenecks in the solution. To support this it is recommended to use Cisco UCS Performance Manager to visualize the utilization of all LAN, SAN and server connections on the Cisco UCS level together with the storage utilization. With this information it is possible to identify possible bottlenecks ahead of time and add the required components or rebalance the workloads.

Based on the experience defining, certifying and deploying SAP HANA solutions from the past years the following three Scale Options are defined as a base line. Following table highlights the change in hardware components, as required by different scale. It is important to know that SAP has specified the storage performance for SAP HANA based on a per server rule, independent from the server size. In other words the maximum number of servers per storage is the same if you use virtual machine with 64GB main memory or Cisco UCS B460 M4 with 2 TB main memory for SAP HANA.

**Table 5 Sample Scale Options for SAP HANA**

| Component | Scale Option 1 | Scale Option 2 | Scale Option 3 |
|---|---|---|---|
| Servers | 10 x Cisco C-Series or B-Series M4 servers | 20 x Cisco C-Series or B-Series M4 servers | 30 x Cisco C-Series or B-Series M4 servers |
| Blade servers chassis | 5 x Cisco 5108 Blade server chassis | 10 x Cisco 5108 Blade server chassis | 15 x Cisco 5108 Blade server chassis |
| Storage | 1x EMC VNX5400<br>or<br>1x EMC VNX8000 | 2x EMC VNX5400<br>2x EMC VNX8000 | 3x EMC VNX5400<br>2x EMC VNX8000 |

Although this is the base design, each of the components can be scaled easily to support specific business requirements. For example, more (or different) servers or even blade chassis can be deployed to increase compute capacity, additional EMC VNX series storage can be added to increase storage capacity, improve I/O capability and throughput, and special hardware or software features can be added to introduce new features.

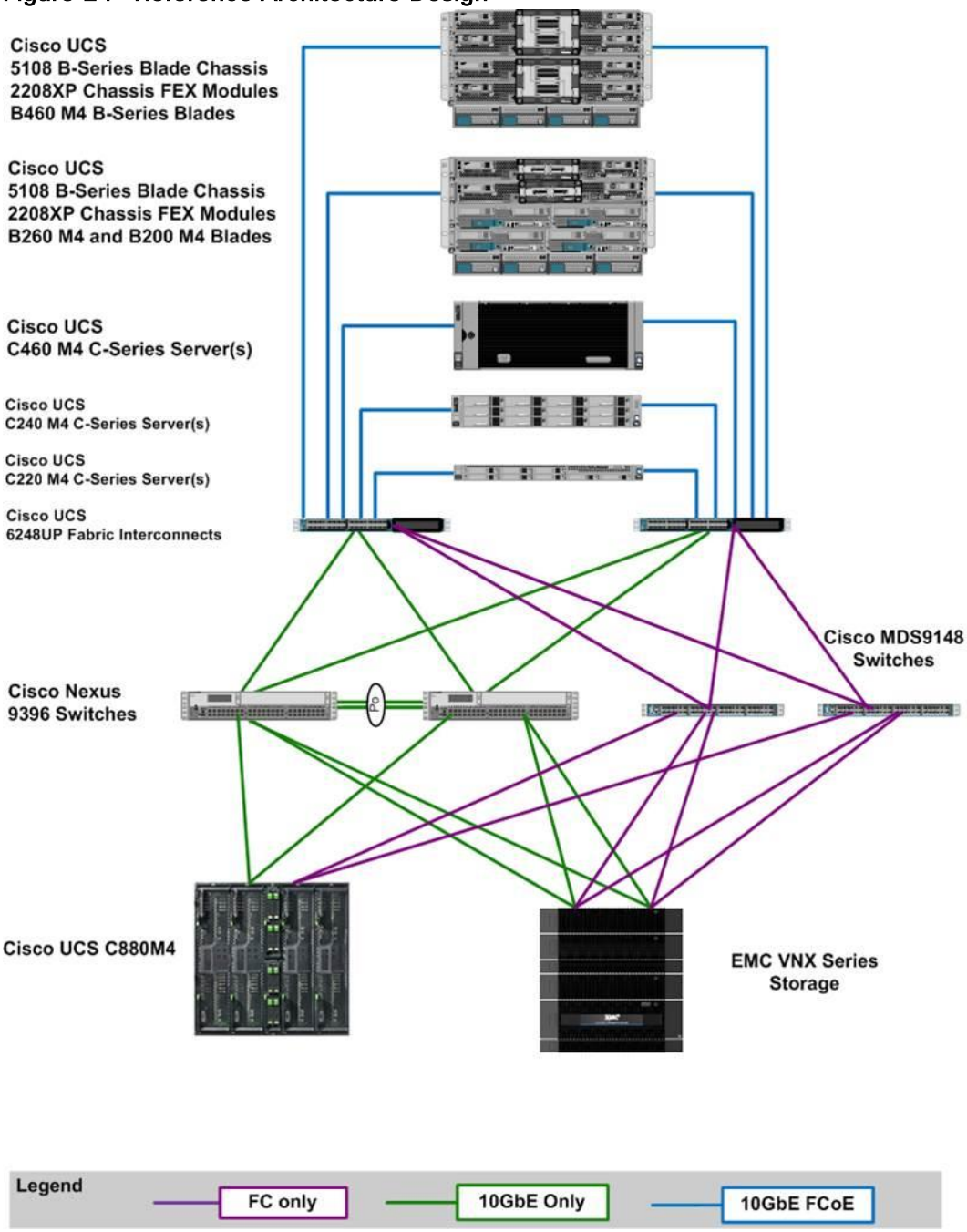
In addition to the SAP HANA scale shown in table 5 the solution allows adding non SAP HANA workload. The scaling options in addition to the information in Table 5 are shown in Table 6 .

**Table 6 Additional HW for Non-HANA Workloads**

| Component | Scale Option 1 | Scale Option 2 | Scale Option 3 |
|---|---|---|---|
| Non-SAP HANA Servers | 80 x Cisco B200 M4 servers | 40 x Cisco B200 M4 servers | 0 x Cisco B200 M4 servers |
| Blade servers chassis | 10 x Cisco 5108 Blade server chassis | 5 x Cisco 5108 Blade server chassis | 0 x Cisco 5108 Blade server chassis |
| Additional Storage for Non-SAP HANA | 2x EMC VNX5400 or<br>1x EMC VNX8000 | 1x EMC VNX5400<br>1x EMC VNX8000 | 0x EMC VNX5400<br>0x EMC VNX8000 |

This CVD guides you through the steps for deploying the base architecture, as shown in Figure 24. These procedures cover everything from physical cabling to network, compute and storage device configurations.

Figure 24 Reference Architecture Design



# Guidelines for VMware ESXi

## Memory Configuration Guidelines for Virtual Machines

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

## VMware ESX/ESXi Memory Management Concepts

VMware 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:

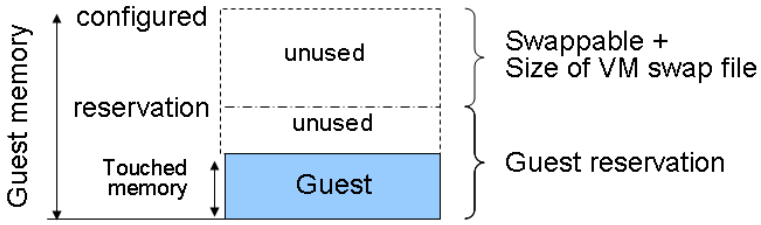
- Memory sharing across virtual machines that have similar data (that is, same guest operating systems).
- Memory over-commitment, which means allocating more memory to virtual machines than is physically available on the VMware ESX/ESXi host. For SAP HANA it is not supported to use Memory over-commitment, this can only be used for non-SAP HANA workload on the shared infrastructure.
- 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 25 illustrates the use of memory settings parameters in the virtual machine.

**Figure 25 Virtual Machine Memory Settings**




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

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

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

## Allocating Memory to Virtual Machines

The proper sizing of memory for a virtual machine 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. Following table outlines the CPU and memory resources used by a single virtual machine for SAP HANA

This document is not a sizing instrument but delivers a guideline of technically possible configurations. For proper sizing, refer to SAP Business Warehouse on SAP HANA (BWoH) and SAP Business Suite on SAP HANA (SoH) sizing documentation available from SAP. The ratio between CPU and memory can be defined as 6.4 GB per vCPU for Intel Xeon E7 v2 CPUs (Westmere EX) and 8.53 GB per vCPU for Intel Xeon E7 v3 CPUs (Ivy Bridge EX). The numbers for Suite on SAP HANA can be doubled.

See that the VMware ESXi host and every virtual machine produce some memory overhead. For example, a VMware ESXi server with 512 GB physical RAM cannot host a virtual machine with 512 GB vRAM because the server would need some static memory space for its kernel and some dynamic memory space for each virtual machine. For example, a virtual machine with 500 GB vRAM would most likely fit into a 512 GB ESXi host.

**Table 7 vCPU to Memory mapping by a Single Virtual Machine for SAP HANA.**

| vCPU (Westmere EX) | | vCPU (Ivy Bridge EX) | | vCPU (Haswell EX) | | vRAM | Dynamic memory overhead (est.) |
|---|---|---|---|---|---|---|---|
| Analytics | SoH | Analytics | SoH | Analytics | SoH | | |
| 10 | 10 | 15 | 15 | 18 | 18 | 64 GB | 0.2 GB |
| 20 | 10 | 15 | 15 | 18 | 18 | 128 GB | 0.5 GB |
| 40 | 20 | 30 | 15 | 36 | 18 | 256 GB | 1 GB |
| 60 | 30 | 45 | 30 | 36 | 18 | 384 GB | 2 GB |
| - | 40 | 60 | 30 | 54 | 36 | 512 GB | 2 GB |
| - | 60 | - | 45 | 72* | 36 | 768 GB | 4 GB |

| vCPU (Westmere EX) | | vCPU (Ivy Bridge EX) | | vCPU (Haswell EX) | | vRAM | Dynamic memory overhead |
|---|---|---|---|---|---|---|---|
| - | - | - | 60 | 108* | 54 | 1 TB | 8 GB |
| - | - | - | - | - | 72* | 1.5 TB | 8 GB |
| - | - | - | - | - | 108* | 2 TB | 12 GB |

More details and background information about SAP HANA on VMware ESX can be found at: http://scn.sap.com/docs/DOC-55263 and http://www.vmware.com/files/pdf/SAP_HANA_on_vmware_vSphere_best_practices_guide.pdf

The following are descriptions of recommended best practices for Non SAP HANA workloads:

- Account for memory overhead – Virtual machines require memory beyond the amount allocated, and this memory overhead is per-virtual machine. Memory overhead includes space reserved for virtual machine devices, depending on applications and internal data structures. The amount of overhead required depends on the number of vCPUs, configured memory, and whether the guest operating system is 32-bit or 64-bit. As an example, a running virtual machine with one virtual CPU and two gigabytes of memory may consume about 100 megabytes of memory overhead, where a virtual machine with two virtual CPUs and 32 gigabytes of memory may consume approximately 500 megabytes of memory overhead. This memory overhead is in addition to the memory allocated to the virtual machine and must be available on the ESXi host.

- ”Right-size” memory allocations – Over-allocating memory to virtual machines can waste memory unnecessarily, but it can also increase the amount of memory overhead required to run the virtual machine, thus reducing the overall memory available for other virtual machines. Fine-tuning the memory for a virtual machine is done easily and quickly by adjusting the virtual machine properties. In most cases, hot-adding of memory is supported and can provide instant access to the additional memory if needed.

- Intelligently overcommit – Memory management features in vSphere allow for over commitment of physical resources without severely affecting performance. Many workloads can participate in this type of resource sharing while continuing to provide the responsiveness users require of the application. It is important to know that memory overcommit is NOT allowed for SAP HANA workload. It is still best practice to configure memory over commitment for other workloads in the same vCenter environment. When looking to scale beyond the underlying physical resources, consider the following:

- Establish a baseline before overcommitting. Note the performance characteristics of the application before and after. Some applications are consistent in how they utilize resources and may not perform as expected when vSphere memory management techniques take control. Others, such as Web servers, have periods where resources can be reclaimed and are perfect candidates for higher levels of consolidation.

- Use the default balloon driver settings. The balloon driver is installed as part of the VMware Tools suite and is used by ESXi if physical memory comes under contention. Performance tests show that the balloon driver allows ESXi to reclaim memory, if required, with little to no impact to performance. Disabling the balloon driver forces ESXi to use host-swapping to make up for the lack of available physical memory which adversely affects performance.



SAP HANA does not support memory ballooning. Please take care that this function is note used on all hosts where SAP HANA can run.

- Set a memory reservation for virtual machines that require dedicated resources. Virtual machines running SQL or SAP HANA services consume more memory resources than other application and Web front-end virtual machines. In these cases, memory reservations can guarantee that those services have the resources they require while still allowing high consolidation of other virtual machines.

Based on this best practices it can happen that in larger installations the SAP HANA workload and Non SAP HANA will run on different VMware ESXi cluster within the same virtual data center as the memory consumption options are different.

## Storage Guidelines

This Cisco UCS Integrated Infrastructure uses Fibre Channel as the main path to access storage arrays, NFS is only used in case the same file system must be mounted on multiple servers (not ESXi hosts). VMware 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 Fibre Channel (FC), or multiple protocols for tiered scenarios such as using FC for high-throughput storage pools and NFS for high-capacity storage pools. For more information, see the VMware whitepaper Comparison of Storage Protocol Performance in VMware vSphere 5 at: http://www.vmware.com/files/pdf/perf_vsphere_storage_protocols.pdf.

## Virtual Networking

This Cisco UCS Integrated Infrastructure demonstrates use and benefits of Cisco Nexus1000V virtual switching technology. Each server has one ore multiple physical adapters with a minimum of two 10 GE links going to fabric A and fabric B of Cisco UCS for high availability. Cisco UCS VIC presents two or more virtual Network Interface Cards (vNICs) to the hypervisor and also two virtual Host Bus Adapters (vHBAs) to the hypervisor. The MAC addresses to these vNICs are assigned using MAC address pool defined on Cisco UCS. The vNICs are configured always as a set of two per use-case. One vNIC is assigned for fabric A and the other vNIC is assigned to fabric B without the Cisco UCS Failover capability. The load-balancing and high-availability function is provided by the vSwitch on VMware ESXi level and a second layer of failover

technology will increase the effort for trouble shooting in case of a failure. 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 Cisco UCS, upstream switch failure (due to "End Host Mode" architecture).
- Enable PortFast on ESXi host uplinks – Failover events can cause spanning tree protocol recalculations that can set switch ports into forwarding or blocked state to prevent a network loop. This process can cause temporary network disconnect. 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 the Nexus switches or infrastructure switches that connect to the Cisco UCS Fabric Interconnect uplinks for faster convergence of STP in the events of FI reboots or FI uplink flaps.
- Jumbo MTU for vMotion and Storage traffic – This best practice is implemented in the architecture by configuring jumbo MTU end-to-end.

## Storage Best Practices

The following are vSphere storage best practices:

- Host multi-pathing – Having a redundant set of paths to the storage area network is critical to protecting the availability of your environment. This redundancy is in the form of dual adapters connected to separate fabric switches.
- Partition alignment – Partition misalignment can lead to severe performance degradation due to I/O operations having to cross track boundaries. Partition alignment is important both at the VMFS level as well as within the guest operating system. Use the vSphere Client when creating VMFS datastores to be sure they are created aligned. When formatting volumes within the guest, Windows 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 required downtime.
- Calculate your total virtual machine size requirements – The swap file size is calculated by "Virtual Machine configured memory" – "memory reservation", for SAP HANA systems, where the memory is 100% reserved the swap file size is 0. For all other workloads please use the following guidance. 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, up to 16GB for the virtual machine swap file (size of allocated memory), and 100MB for log files (total virtual disk size + configured memory + 100MB) or 36.1GB total.

- Understand I/O Requirements – Under-provisioned storage can significantly slow responsiveness and performance for applications. In a multitier application, you can expect each tier of application to have different I/O requirements. As a general recommendation, pay close attention to the amount of virtual machine disk files hosted on a single VMFS volume. Over-subscription of the I/O resources can go unnoticed at first and slowly begin to degrade performance if not monitored proactively.

# VMware Storage Virtualization

## Storage Layout

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

## Storage Virtualization

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

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

# Cisco UCS 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 host uses following identities in this architecture:
  - Host UUID
  - Mac Addresses: one per each vNIC on the server
  - One WWNN and one WWPN per each vHBA on the server
- All of these identifiers are defined in their respective identifier pools and the pool names are referred in the service profile template.

- 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 Cisco 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 Cisco UCS and Cisco 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. If a server has physical fault (faulty memory, or PSU or fan, for example), by following the steps below, a new server can be procured within minutes:

- For ESX hosts: Put the faulty server in maintenance mode using vCenter. This would move VMs running on fault server to other healthy servers on the cluster.
- For Bare Metal host: Shutdown the application and Operating System
  - Step 1: 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).
  - Step 2: Physically install the new server and connect it to the Fabric Extenders. The new server will be discovered by Cisco UCS Manager.
  - Step 3: Associate the service profile to the newly deployed rack server. This would boot the same ESXi or OS server image from the storage array as what the faulty server was running.
- For ESX hosts: 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.
- For Bare Metal hosts: Start all applications on this server

This approach is only valid if no intern disks are used to store the Operating System, applications, or data.

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 Cisco 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 High Availability Design

Figure 24 illustrates the logical layout of the architecture. The following are the key aspects of this solution:

- Mix of Cisco UCS B-Series and C-Series servers are used, managed by Cisco UCS Manager (UCSM)
- 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 Cisco Nexus 9396PX and Cisco UCS Fabric Interconnects for high availability
- vPC and port-aggregation is used between Cisco Nexus 9396PX and EMC VNX storage for high availability
- Four 10GE links between Cisco UCS FI and IO-Module provides enough bandwidth for SAP HANA and other applications. The oversubscription can be reduced by adding more 10GE links between FI and IO-Module if needed by the applications running on the hosts.
- vHBAs on Fabric A and Fabric B used to provide FC based storage access high availability.
- Storage is made highly available by deploying following practices:
- FC SAN access for booting the hypervisor and OS images. The Cisco UCS Fabric Interconnects (A and B) are connected upstream Fabric Switch MDS9148 (A & B) for Fabric zoning.
- EMC 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.
- Cisco MDS 9148 switches (A and B) are connected to both Storage Processors SPA and SPB (over FC) and Cisco Nexus 9396PX switches (A and B) are connected to both Data Movers (over Ethernet), however, a given FI connected to one Cisco MDS 9148 and both Cisco Nexus 9396PX switches for FC and NFS storage access respectively.
- vPC on Cisco Nexus 9396PX switches and port-aggregation on EMC 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 the entire load. If the whole Data Mover fails, then the standby DM takes over the role of active DM.
- The EMC VNX Storage Processors are always in the active/active mode; if the target cannot be reached on SAN-A, server can access the LUNs thru SAN-B and storage-processor inter-link.
- On hosts, boot order lists vHBA on both fabrics for high-availability.

## Jumbo MTU

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

- NFS Storage access
- SAP HANA Internal traffic
- vMotion traffic
- Backup traffic

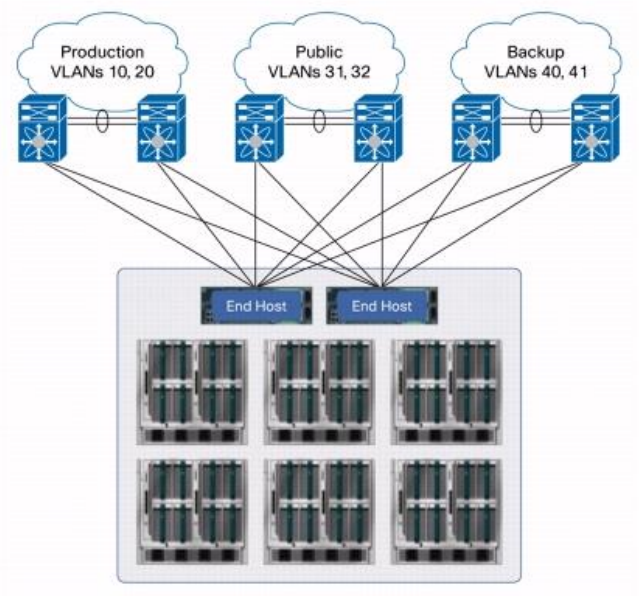
These traffic types are “bulk transfer” traffic, and larger MTU significantly improves the performance. Jumbo MTU must be configured end-to-end to ensure that IP packets are not fragmented by intermediate network nodes. Following is the checklist of end-points where jumbo MTU needs to be configured:

- Ethernet ports on EMC VNX Storage Processors
- System QoS classes in Cisco Nexus 9396PX switches
- System QoS classes in Cisco UCS
- vNICs in service profiles
- Cisco Nexus 1000v switch or VMware vSwitches on the VMware ESXi hosts
- VM-Kernel ports used for vMotion and storage access on the VMware ESXi hosts

## About Network Path Separation with Cisco UCS

With Cisco UCS™ Manager 2.0, disjoint Layer 2 networks upstream of Cisco UCS was introduced. Figure 21 shows a common topology. The production, public, and backup networks are separate Layer 2 domains and do not have adjacencies with each other; however, Cisco UCS blades may need to access all three networks. Furthermore, in the case of a virtualized host, the host may include virtual machines that need access to all three networks.

Figure 26 Disjoint Layer 2 Networks Upstream




The number of Layer 2 networks for which a blade can send and receive traffic depends on the number of vNICs supported by the mezzanine card because a vNIC can be pinned to only one uplink port (or PortChannel). On a system level, a maximum of 31 disjoint networks are supported.

The Cisco UCS Virtual Interface Card (VIC) is required if a virtualized environment requires individual virtual machines to talk to different upstream Layer 2 domains. Multiple vNICs would need to be created on the service profile in Cisco UCS, and the vNICs need to be assigned to different VMware virtual switches (vSwitches) or have a different uplink port profile assigned to them (Cisco Nexus ® 1000V Switch).

For example, in 0, if the vNIC definition for vmnic0 has VLANs 10 to 20 trunked to it, pinning will fail because no uplink port matches the VLAN membership. Instead, vmnic0 should have VLANs 10 to 15 (or a subset such as VLANs 10 to 12) trunked to it.

Figure 27 vNIC Pinning using End-Host Mode with Disjoint Layer 2 Networks Upstream

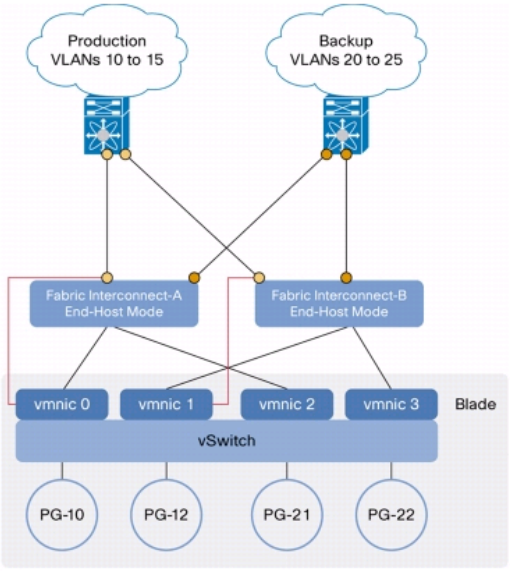



Figure 28 Log Entry with Misconfigured VLAN(s) per vNIC

| Severity | Code | ID | Affected object | Cause | Last Tran... | Description |
|---|---|---|---|---|---|---|
| | F0207 | 2739535 | sys/chassis-1/... | link-down | 2011-09-13T... | Adapter host interface 1/1/1/1 link state: down |
| | F0479 | 2739458 | sys/chassis-1/... | vif-down | 2011-09-13T... | Virtual interface 924 link state is down |
| | F0479 | 2739456 | sys/chassis-1/... | vif-down | 2011-09-13T... | Virtual interface 923 link state is down |
| | F0283 | 2739455 | sys/chassis-1/... | link-down | 2011-09-13T... | ether VIF 1 / 1 A-923 down, reason: ENM source pinning failed |
| | F0283 | 2739454 | sys/chassis-1/... | link-down | 2011-09-13T... | ether VIF 1 / 1 B-924 down, reason: ENM source pinning failed |

For detailed information, refer to the white paper “Deploy Layer 2 Disjoint Networks Upstream in End Host Mode” on the cisco.com web site.

In this Cisco UCS Integrated Infrastructure we show the use of Disjoint Layer 2 networks by separating the Administrative network traffic from the Client / Application network traffic. This is not mandatory and you can use a single Layer 2 network design. You can use this example also to separate the network traffic from Tenant A and from Tenant B if this is required.

In this CVD the following mappings are used:

- VLANs 1,76,2034,2031
  - Nexus 9000 Port Channel pc11 -> Cisco UCS vPC-11 -> Admin-Zone -> vNIC-Temp ESX-A/B -> Nexus1000V Uplink
  - Nexus 9000 Port Channel pc12 -> Cisco UCS vPC-12 -> Admin-Zone -> vNIC-Temp ESX-A/B ->Nexus1000V Uplink
- VLANs 199
  - Nexus 9000 Port Channel pc11 -> Cisco UCS vPC-11 -> Backup-Zone -> Nexus1000V Backup-Zone

  - Nexus 9000 Port Channel pc12 -> Cisco UCS vPC-12 -> Backup-Zone -> Nexus1000V Backup-Zone

- VLANs 2,3001-3010
  - Nexus 9000 Port Channel pc13 -> Cisco UCS vPC-13 -> Client-Zone -> vNIC-Temp ESX-A/B-Appl ->Nexus1000V Client-Zone
  - Nexus 9000 Port Channel pc14 -> Cisco UCS vPC-14 -> Client-Zone -> vNIC-Temp ESX-A/B-Appl ->Nexus1000V Client-Zone



In case you deploy your landscape with a different setup, build your mapping first and use this documentation as an example of how to setup the different components.

## 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, etc. These tasks should be performed before the installation starts to reduce the required time.

- 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 following table to confirm that all equipment, software, and appropriate licenses are available before the deployment process.
- Gather data: Collect the specific configuration data for networking, naming, and required accounts. Enter this information into the Configuration Variables worksheet for reference during the deployment process.

**Table 8 Customer Specific Configuration Data**

| Requirement | Description | Reference |
|---|---|---|
| Hardware | Cisco UCS Fabric Interconnects, Fabric Extenders and UCS chassis for network and compute infrastructure | See corresponding product documentation |
| | Cisco Nexus 9396PX, Nexus 3548 switches and Cisco MDS 9148 Fabric Switches for NFS and FC access respectively. | |
| | Cisco UCS B-Series and/or C-Series servers to host SAP HANA or virtual machines | |

| Requirement | Description | Reference |
|---|---|---|
| | VMware vSphere™ 5.5 server to host virtual infrastructure servers<br><br>Note: This requirement may be covered in the existing infrastructure | |
| | EMC VNX storage: Multiprotocol storage array with the required disk layout as per architecture requirements | |
| Software | Cisco Nexus 1000v VMS and VEM installation media | See corresponding product documentation |
| | VMware ESXi™ 5.5 installation media | |
| | VMware vCenter Server 5.5 installation media | |
| | EMC VSI for VMware vSphere: Unified Storage Management – Product Guide | |
| | EMC VSI for VMware vSphere: Storage Viewer–Product Guide | |
| | SUSE Linux Enterprise Server for SAP | |
| | Red Hat Enterprise Linux for SAP HANA | |
| | SAP HANA 1.0 | |
| Licenses | SAP HANA license keys | Consult your corresponding vendor to obtain license keys |
| | Cisco Nexus 1000v license key | |
| | VMware vCenter 5.5 license key | |
| | VMware ESXi 5.5 license keys | |
| | SLES and RHEL license keys | |

## Customer Configuration Data

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

The Appendix Configuration Variables provides a table to maintain a record of relevant information. This form can be expanded or contracted as required, and information may be added, modified, and recorded as deployment progresses.

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

## Solution Configuration Guidelines

The configuration for Cisco UCS Integrated Infrastructure is divided in to following steps:

1. Install and configure the Management POD (if required)
2. Connect network cables for LAN and SAN components
3. Configure Cisco Nexus 9396PX switches
4. Configure Cisco MDS 9148 switches
5. Prepare Cisco UCS Fabric Interconnects and configure Cisco UCS Manager
6. Configure EMC VNX Storage
7. Install VMware ESXi servers
8. Configure storage for virtual machine datastores and SAP HANA
9. Install and instantiate virtual machines thru VMware vCenter
10. Install different SAP HANA use cases on Bare Metal Cisco UCS Server or virtual machines
11. Test the installation

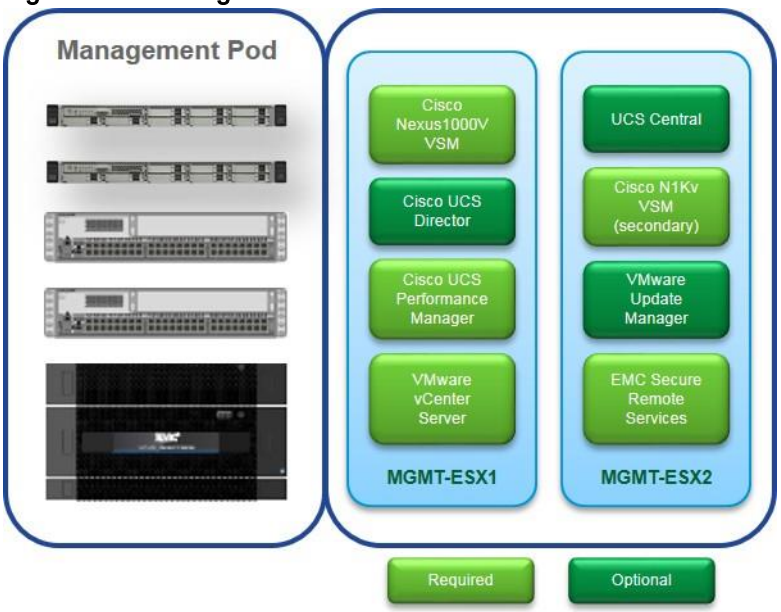
# Install and Configure the Management Pod

In order to manage a multiple Pod environment for SAP HANA, build a Management Pod which is used to manage the environment. The management pod includes but not limited to a pair of Cisco Nexus 3500switches for out-of-band Management network and a pair of Cisco UCS C220 rack mount servers. The Cisco UCS rack mount servers will run VMware ESXi with VMware vCenter with additional management and monitoring servers.

The device list for the management POD is as follows:

| | |
|---|---|
| 2* Nexus 3548 | Names: Nexus3500-M1 and Nexus3500-M2 |
| 2* Cisco UCS C220 M4 | Names: C220M4-M1 and C220M4-M2 |
| 1* Cisco 2911 ISR | Names: C2911-M1 |
| 1* EMC VNX5400 Storage | Names: EMC-VNX5400-M1 |

**Figure 29 Management Pod Overview**




## Device Cabling

See the Cisco Nexus 3548, Cisco UCS C220 M4 server and EMC VNX storage array configuration guide for detailed information about how to mount the hardware on the rack. Figure 30 shows the connectivity details for the Cisco UCS Integrated Infrastructure covered in this document.

Ethernet cable connectivity can be divided in to the following five categories in this architecture:

- Cisco Nexus 3500 switches to EMC VNX Data Mover 10G Ethernet links (Red)
- Cisco Nexus 3500 switches vPC peer links (Green)

- Cisco Nexus 3500 switches to Cisco UCS C220 M4 Server links (Blue)
- Cisco Nexus 3500 switches to Cisco 2911 ISR (Purple)
- Cisco Nexus 3500 switches to the SAP HANA Pod (direct or through Customer LAN) (Gray)

**Figure 30 Connectivity of the Management Components**

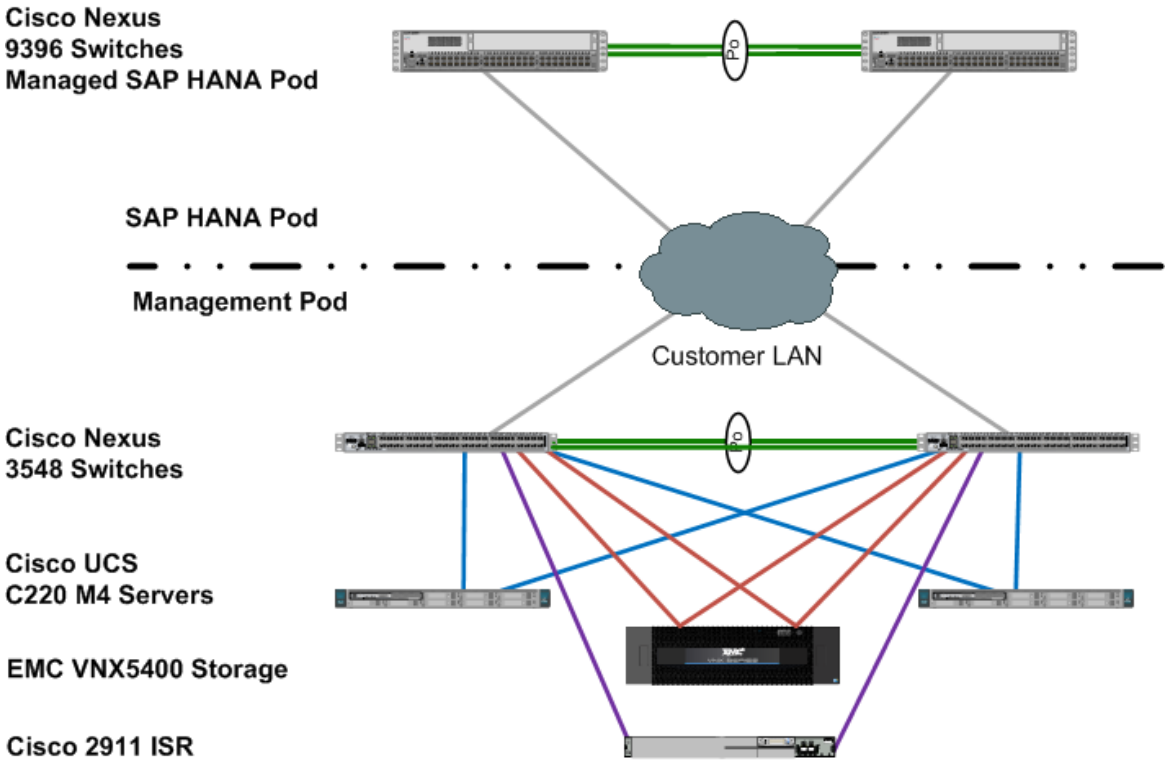



Table 9 lists the detailed Ethernet cable connectivity for this architecture.

## Cisco Nexus 3548 M1

**Table 9 Ethernet Cable Connectivity for Cisco Nexus 3500 M1**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco Nexus 3500 M1 | Eth1/5 | 10GbE | Cisco Nexus 9000 A | Eth1/11 |
| | Eth1/6 | 10GbE | Cisco Nexus 9000 B | Eth1/11 |
| | Eth1/2 | 10GbE | Cisco Nexus 3500 M2 | Eth1/2 |
| | Eth1/4 | 10GbE | Cisco Nexus 3500 M2 | Eth1/4 |
| | MGMT0 | GbE | Cisco Nexus 3500 M2 | MGMT0 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/7 | 1GbE | EMC VNX5400-M1 CS1 | MGMT0 |
| | Eth1/8 | 10GbE | EMC VNX5400-M1 DM2 | 0/0 |
| | Eth1/9 | 10GbE | EMC VNX5400-M1 DM3 | 0/0 |
| | Eth1/10 | 1GbE | Cisco UCS C220M4 M1 | MGMT |
| | Eth1/11 | 1/10GbE | Cisco UCS C220M4 M1 | PCI1/1 |
| | Eth1/12 | 1/10GbE | Cisco UCS C220M4 M2 | PCI1/1 |
| | Eth1/3 | 1GbE | Cisco 2911 ISR | GE0/0 |
| | Eth1/20 | 1GbE | Cisco UCS fabric interconnect A | MGMT0 |
| | Eth1/21 | 1GbE | Cisco Nexus 9000 A | MGMT0 |
| | Eth1/22 | 1GbE | Cisco MDS 9148S A | MGMT0 |
| | Eth1/23 | 10GbE | EMC VNX5400-1 CS1 | MGMT0 |

## Cisco Nexus 3548 M2

**Table 10 Ethernet Cable Connectivity for Cisco Nexus 3500 M2**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco Nexus 3500 M2 | Eth1/5 | 10GbE | Cisco Nexus 9000 A | Eth1/12 |
| | Eth1/6 | 10GbE | Cisco Nexus 9000 B | Eth1/12 |
| | Eth1/2 | 10GbE | Cisco Nexus 3500 M1 | Eth1/2 |
| | Eth1/4 | 10GbE | Cisco Nexus 3500 M1 | Eth1/4 |
| | MGMT0 | GbE | Cisco Nexus 3500 M1 | MGMT0 |
| | Eth1/7 | 1GbE | EMC VNX5400-M1 CS2 | MGMT0 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/8 | 10GbE | EMC VNX5400-M1 DM2 | 0/1 |
| | Eth1/9 | 10GbE | EMC VNX5400-M1 DM3 | 0/1 |
| | Eth1/10 | 1GbE | Cisco UCS C220M4 M2 | MGMT |
| | Eth1/11 | 1/10GbE | Cisco UCS C220M4 M1 | PCI1/2 |
| | Eth1/12 | 1/10GbE | Cisco UCS C220M4 M2 | PCI1/2 |
| | Eth1/3 | 1GbE | Cisco 2911 ISR | GE0/1 |
| | Eth1/20 | 1GbE | Cisco UCS fabric interconnect B | MGMT0 |
| | Eth1/21 | 1GbE | Cisco Nexus 9000 B | MGMT0 |
| | Eth1/22 | 1GbE | Cisco MDS 9148S B | MGMT0 |
| | Eth1/23 | 10GbE | EMC VNX5400-1 CS2 | MGMT0 |

## Cisco 2911 ISR

**Table 11 Cable Connectivity for Cisco 291 ISR**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco 2911 ISR | GE0/0 | 10GbE | Cisco Nexus 3500 M1 | Eth1/3 |
| | GE0/1 | 10GbE | Cisco Nexus 3500 M2 | Eth1/3 |
| | Async0/0/0 | Serial | Cisco Nexus 9000 A | Console |
| | Async0/0/1 | Serial | Cisco Nexus 9000 B | Console |
| | Async0/0/2 | Serial | Cisco UCS fabric interconnect A | Console |
| | Async0/0 | Serial | Cisco UCS fabric interconnect B | Console |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | /3 | | | |
| | Async0/0/4 | Serial | Cisco MDS 9148S A | Console |
| | Async0/0/5 | Serial | Cisco MDS 9148S B | Console |
| | Async0/0/6 | Serial | Cisco Nexus 3500 M1 | Console |
| | Async0/0/7 | Serial | Cisco Nexus 3500 M2 | Console |
| | Async0/0/8 | Serial | | Console |
| | Async0/0/9 | Serial | | Console |
| | Async0/0/10 | Serial | | Console |
| | Console | Serial | Customer Console Server | Any |

## Configure Domain Name Service (DNS)

Components in this Cisco Integrated Infrastructure require a Domain Name Service (DNS) to work properly. You can use the default DNS installed in your datacenter if possible. For this solution, Microsoft Windows Server DNS was used in the Lab setup. Configure all A and PTR records for the managed components.

## Network Configuration for Management Pod

The following sections provide a detailed procedure for configuring the Cisco Nexus 3500 Switches for the management environment.

### Cisco Nexus 3500 Configuration

This section describes configuring the Cisco Nexus 3500 switches as follows:

- Initial Configuration

- VLAN configuration
- Virtual Port Channel Domain configuration
- Port Configuration to all connected devices

Table 12 lists the information required to setup the Cisco Nexus 3500 switches in this Cisco UCS Integrated Infrastructure.

**Table 12 Information to Setup Cisco Nexus Switches in the Management POD**

| Name | Variable |
|---|---|
| Hostname Nexus M1 | <<var_nexus_m1_hostname>> |
| IP address Nexus M1 | <<var_nexus_m1_mgmt0_ip>> |
| Netmask of the management network | <<var_mgmt_netmask>> |
| Gateway in the management network | <<var_mgmt_gw>> |
| IP Address of the global NTP server | <<var_global_ntp_server_ip>> |
| Hostname Nexus M2 | <<var_nexus_m2_hostname>> |
| IP address Nexus M2 | <<var_nexus_m2_mgmt0_ip>> |
| VLAN ID of the management network | <<var_management_vlan_id>> |
| VLAN ID of the global administration network | <<var_admin_vlan_id>> |
| VLAN ID of the global backup network | <<var_backup_vlan_id>> |
| VLAN ID of the Nexus1000V control network | <<var_n1k_control_vlan_id>> |
| VLAN ID of the vMotion network | <<var_mgmt_vmotion_vlan_id>> |
| VLAN ID of the NFS traffic network for ESX | <<var_mgmt_esx_nfs_vlan_id>> |
| VPC Domain ID for the two Nexus3000 switches | <<var_mgmt_nexus_vpc_domain_id>> |

## Initial Configuration Setup

The following steps provide the details for the initial Cisco Nexus 9000 Switch setup.

### Cisco Nexus 3500 M1

To set up the initial configuration for the first Cisco Nexus switch complete the following steps:



On the initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]:
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : <<var_nexus_m1_hostname>>
  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
    Mgmt0 IPv4 address : <<var_nexus_m1_mgmt0_ip>>
    Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var_mgmt_gw>>
  Configure advanced IP options? (yes/no) [n]:
```

```
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
    Type of ssh key you would like to generate (dsa/rsa) [rsa]:
    Number of rsa key bits <1024-2048> [2048]:
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_global_ntp_server_ip>>
  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
  password strength-check
  switchname <<var_nexus_m1_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_mgmt_gw>>
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server <<var_global_ntp_server_ip>>
  copp profile strict
interface mgmt0
ip address <<var_nexus_m1_mgmt0_ip>> <<var_mgmt_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]:   Enter
Use this configuration and save it? (yes/no) [y]:   Enter
[########################################] 100%
Copy complete.
```

### Cisco Nexus 3500 M2

To set up the initial configuration for the second Cisco Nexus switch, complete the following steps:



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : <<var_nexus_m2_hostname>>
  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
    Mgmt0 IPv4 address : <<var_nexus_m2_mgmt0_ip>>
    Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var_mgmt_gw>>
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
```

```
    Type of ssh key you would like to generate (dsa/rsa) [rsa]:
    Number of rsa key bits <1024-2048> [2048]:
  Configure the ntp server? (yes/no) [n]:   y
    NTP server IPv4 address : <<var_global_ntp_server_ip>>
  Configure default interface layer (L3/L2) [L3]: L2
  Configure default switchport interface state (shut/noshut) [shut]:   Enter
  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
  password strength-check
  switchname <<var_nexus_m2_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_mgmt_gw>>
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server <<var_global_ntp_server_ip>>
  copp profile strict
interface mgmt0
ip address <<var_nexus_m2_mgmt0_ip>> <<var_mgmt_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]:   Enter
Use this configuration and save it? (yes/no) [y]:   Enter
[########################################] 100%
Copy complete.
```

## Enable Appropriate Cisco Nexus 3500 Features and Settings

### Cisco Nexus 3500 M1 and Cisco Nexus 3500 M2

The following commands enable IP switching feature and set default spanning tree behaviors.

On each Nexus 3500, enter configuration mode:

```
config terminal
```

Use the following commands to enable the necessary features:

```
feature udld

feature lacp

feature vpc
feature interface-vlan
feature lldp

feature hsrp
```

### Configure the Spanning Tree Defaults

To enable the bridge protocol data unit (BPDU) guard and BPDU Filtering by default on all spanning tree edge ports, use these commands:

```
spanning-tree port type edge bpduguard default

spanning-tree port type edge bpdufilter default
```

### Configure Jumbo Frame Support

If a Jumbo packet has to traverse a Nexus 3500 switch, you need to configure the Policy-map:

```
policy-map type network-qos jumbo

  class type network-qos class-default

    mtu 9216

system qos

  service-policy type network-qos jumbo
```

### Configure Port Speed Defaults

To attach devices with 100, 1000, or 10000 Mbps capabilities, set the default speed on all ports to auto:

```
int eth1/1-48

speed auto
```

Save the running configuration to start-up:

```
copy run start
```

## Create VLANs for Management Traffic

### Cisco Nexus 3500 M1 and Cisco Nexus 3500 M2

To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

From the configuration mode, run the following commands:

```
vlan <<var_management_vlan_id>>
name Infrastructure-Management

vlan <<var_admin_vlan_id>>
name Global-Admin-Network

vlan <<var_backup_vlan_id>>
name Global-Backup-Network
```

Save the running configuration to start-up on both Nexus 3500:

```
copy run start
```

## Create VLANs for Nexus 1000v Traffic

### Cisco Nexus 3500 M1 and Cisco Nexus 3500 M2

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

From the configuration mode, run the following commands:

```
vlan <<var_n1k_control_vlan_id>>
name Nexus-1000v-Control-Network
```

Save the running configuration to start-up on both Nexus 3500:

```
copy run start
```

## Create VLANs for ESXi Traffic

### Cisco Nexus 3500 M1 and Cisco Nexus 3500 M2

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

From the configuration mode, run the following commands:

```
vlan <<var_mgmt_vmotion_vlan_id>>
name Mgmt-ESX-vMotion-Network

vlan <<var_mgmt_esx_nfs_vlan_id>>
name Mgmt-ESX-NFS-Network
```

Save the running configuration to start-up on both Nexus 3500:

```
copy run start
```

## Configure Virtual Port Channel Domain

### Cisco Nexus 3500 M1

To configure virtual port channels (vPCs) for switch A, complete the following steps:

From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_mgmt_nexus_vpc_domain_id>>
```

Make Nexus 3500 M1 the primary vPC peer by defining a low priority value:

```
role priority 10
```

Use the management interfaces on the supervisors of the Nexus 3500 to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_m2_mgmt0_ip>>  source
<<var_nexus_m1_mgmt0_ip>>
```

Enable following features for this vPC domain:

```
peer-switch

delay restore 150

peer-gateway

auto-recovery
```

Save the running configuration to start-up.

```
copy run start
```

### Cisco Nexus 3500 M2

To configure vPCs for switch M2, complete the following steps:

From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_mgmt_nexus_vpc_domain_id>>
```

Make Cisco Nexus 3500 M2 the secondary vPC peer by defining a higher priority value than that of the Nexus 3500 M1:

```
role priority 20
```

Use the management interfaces on the supervisors of the Cisco Nexus 3500 to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_m1_mgmt0_ip>>  source
<<var_nexus_m2_mgmt0_ip>>
```

Enable following features for this vPC domain:

```
peer-switch

delay restore 150

peer-gateway
```

```
auto-recovery
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces for the VPC Peer Links

### Cisco Nexus 3500 M1

Define a port description for the interfaces connecting to VPC Peer <<var_nexus_m2_hostname>>:

```
interface Eth1/2

description VPC Peer <<var_nexus_m2_hostname>>:1/2


interface Eth1/4

description VPC Peer <<var_nexus_m2_hostname>>:1/4
```

Apply a port channel to both VPC Peer links and bring up the interfaces:

```
interface Eth1/2,eth1/4

channel-group 1 mode active

no shutdown
```

Define a description for the port channel connecting to <<var_nexus_m2_hostname>>:

```
interface Po1

description vPC peer-link
```

Make the port channel a switchport, and configure a trunk to allow required VLANs:

```
switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Make this port channel the VPC peer link and bring it up:

```
spanning-tree port type network

vpc peer-link

no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500 M2

Define a port description for the interfaces connecting to VPC peer <<var_nexus_m1_hostname>>:

```
interface Eth1/2
description VPC Peer <<var_nexus_m1_hostname>>:1/2

interface Eth1/4
description VPC Peer <<var_nexus_m1_hostname>>:1/4
```

Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface Eth1/2,eth1/4
channel-group 1 mode active
no shutdown
```

Define a description for the port channel connecting to <<var_nexus_m1_hostname>>:

```
interface Po1
description vPC peer-link
```

Make the port channel a switchport, and configure a trunk to allow HANA VLANs:

```
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Make this port channel the VPC peer link and bring it up:

```
spanning-tree port type network
vpc peer-link
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

## Validate VLAN and VPC Configuration

To validate the VPC status, runs the following commands:

```
cra-n3-m1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id                     : 139
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         : failed
Type-2 inconsistency reason       : SVI type-2 configuration incompatible
vPC role                          : primary
Number of vPCs configured         : 0
Peer Gateway                      : Enabled
Peer gateway excluded VLANs     : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,1031,1034,2121
cra-n3-m1#
```

## Configure Network Interfaces to Connect the Cisco UCS C220 Management Server with LOM

If using the LOM ports with 1GbE, follow the steps below. If not, skip this and go to the next section.

Define a port description for the interface connecting to Cisco UCS C220M4-M1 and Cisco UCS C220M4-M2.

### Cisco Nexus 3500 M1

```
interface Eth1/10

description C220-M1:CIMC
switchport
switchport mode access
```

```
switchport access vlan <<var_management_vlan_id>>


interface Eth1/11

description C220-M1:LOM1

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>


interface Eth1/12

description C220-M2:LOM1

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500 M2

```
interface Eth1/10

description C220-M2:CIMC

switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>


interface Eth1/11

description C220-M1:LOM2

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>


interface Eth1/12
```

```
description C220-M2:LOM2

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces to Connect the Cisco UCS C220 Management Server with VIC1225

If using the VIC1225 ports with 10GbE, complete the following steps:

Define a port description for the interface connecting to Cisco UCS C220M4-M1 and Cisco UCS C220M4-M2.

### Cisco Nexus 3500 M1

```
interface Eth1/10

description C220-M1:CIMC
switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>


interface Eth1/11

description C220-M1:PCI1/1

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>


interface Eth1/12

description C220-M2:PCI1/1

switchport
switchport mode trunk
```

```
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500 M2

```
interface Eth1/10

description C220-M2:CIMC

switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>


interface Eth1/11

description C220-M1:PCI1/2

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>


interface Eth1/12

description C220-M2:PCI1/2

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_mgmt_vmotion_vlan_id>>,<<v
ar_mgmt_esx_nfs_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k_control_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces to Connect the Cisco 2911 ISR

Define a port description for the interface connecting to Cisco 2911 ISR for serial console access to all devices.

### Cisco Nexus 3500 M1

```
interface Eth1/3
```

```
description Cisco2911-ISR:GE00
switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500 M2

```
interface Eth1/3

description Cisco2911-ISR:GE01

switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces to Connect the EMC VNX5400 Storage

### Cisco Nexus 3500 M1

Define a port description for the interface connecting to EMC-VNX5400-M1:

```
interface Eth1/7

description EMC-VNX5400-M1:CS1
switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>


interface Eth1/8

description EMC-VNX5400-M1-DM2:0/0

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_mgmt_esx_nfs_vlan_id>>


interface Eth1/9

description EMC-VNX5400-M1-DM3:0/0

switchport
switchport mode trunk
```

```
switchport trunk allowed vlan <<var_mgmt_esx_nfs_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500 M2

Define a port description for the interface connecting to EMC-VNX5400-M1:

```
interface Eth1/7

description EMC-VNX5400-M1:CS2
switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>


interface Eth1/8

description EMC-VNX5400-M1-DM2:0/1

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_mgmt_esx_nfs_vlan_id>>


interface Eth1/9

description EMC-VNX5400-M1-DM3:0/1

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_mgmt_esx_nfs_vlan_id>>
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces for Out of Band Management Access

The following is an example of the configuration for the Management Ports. Cable and configure based on the datacenter requirement.

### Cisco Nexus 3500 M1

To enable management access to the managed infrastructure, complete the following steps:

Define a port description for the interface connecting to the management switch:

```
interface eth1/20
```

```
description OOB-Mgmt-UCS-FI-A

interface eth1/21
description OOB-Mgmt-NX9000-A
interface eth1/22
description OOB-Mgmt-MDS-A
interface eth1/23
description OOB-Mgmt-EMC-VNX-CS1
```

### Configure the Port as an Access VLAN Carrying the Out of Band Management VLAN Traffic

```
interface eth1/20-23
switchport
switchport mode access
switchport access vlan <<var_management_vlan_id>>
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

#### Cisco Nexus 3500 M2

To enable management access to the managed infrastructure, complete the following steps:

Define a port description for the interface connecting to the management switch:

```
interface eth1/20
description OOB-Mgmt-UCS-FI-B

interface eth1/21
description OOB-Mgmt-NX9000-B
interface eth1/22
description OOB-Mgmt-MDS-B
interface eth1/23
description OOB-Mgmt-EMC-VNX-CS2
```

### Configure the Port as an Access VLAN Carrying the Out of Band Management VLAN Traffic

```
interface eth1/20-23
```

```
switchport
switchport mode access

switchport access vlan <<var_management_vlan_id>>
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces for Access to the Managed Landscape

The following is an example of the configuration for the Network Ports connected to the Cisco Nexus 9000 switches of the managed infrastructure.

### Cisco Nexus 3500 M1

To enable access to the managed infrastructure, complete the following steps:

Define a port description for the interface connecting to the management switch:

```
interface eth1/5

description Aceess-POD1-N9000-A:Eth1/11


interface eth1/6

description Aceess-POD1-N9000-B:Eth1/11
```

Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/5-6

channel-group 33 mode active

no shutdown
```

Define a description for the port channel:

```
interface Po33

description Aceess-POD1-vPC
```

Make the port channel a switchport, and configure a trunk to allow Management VLANs:

```
switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k
_control_vlan_id>>
```

Make this port channel a VPC and bring it up:

```
spanning-tree port type network

vpc 33
```

```
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 3500M2

To enable access to the managed infrastructure, complete the following steps:

Define a port description for the interface connecting to the management switch:

```
interface eth1/5
description Aceess-POD1-N9000-A:Eth1/12

interface eth1/6
description Aceess-POD1-N9000-B:Eth1/12
```

Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/5-6
channel-group 33 mode active
no shutdown
```

Define a description for the port channel:

```
interface Po33
description Aceess-POD1-vPC
```

Make the port channel a switchport, and configure a trunk to allow Management VLANs:

```
switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_backup_vlan_id>>,<<var_n1k
_control_vlan_id>>
```

Make this port channel a VPC and bring it up:

```
spanning-tree port type network
vpc 33
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Configure VLAN Interfaces and HSRP

To simulate network routing within this lab setup, use the Nexus 3500 devices with VLAN interfaces and the Hot Standby Router Protocol (HSRP):

```
feature hsrp


int vlan 76
ip address <<var_nexus_m1_mgmt_ip>>
hsrp 23
ip 192.168.76.5
feature hsrp
int vlan 76
ip address <<var_nexus_m2_mgmt_ip>>
hsrp <<var_nexus_hsrp_id>>
ip <<var_nexus_hsrp_mgmt_ip>>
```

### Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink from the Management environment to connect to the SAP HANA environments. If an existing Cisco Nexus environment is present, Cisco recommends using vPCs to uplink the Cisco Nexus 9000 switches in the Management environment. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run copy run start to save the configuration on each switch after configuration is completed.

## Configure Cisco2911 ISR

This device is used to access the serial console port of all devices with a console port.

Connect to the system with a serial cable from your computer connected to CON port.

Table 13 lists the information used for the setup of the Cisco 2911 ISR in this Cisco UCS Integrated Infrastructure.

**Table 13 Information Required to Setup Cisco 2911 ISR in the Management POD**

| Name | Variable |
|---|---|
| Hostname Cisco 2911 M1 | <<var_mgmt_isr_hostname>> |
| IP address Cisco 2911 M1 | <<var_mgmt_isr_ip>> |
| Netmask of the management network | <<var_mgmt_netmask>> |

| Name | Variable |
|---|---|
| Gateway in the management network | <<var_mgmt_gw>> |
| Default management password | <<var_mgmt_passwd>> |

Set the hostname and default settings:

```
conf t


hostname <<var_mgmt_isr_hostname>>
no ip http server
no ip http authentication local
no ip http timeout-policy idle 60 life 86400 requests 10000
control-plane
line con 0
 password <<var_mgmt_passwd>>
 login
 autohangup
line aux 0
line 0/0/0 0/0/15
 transport input all
 autohangup
 no exec
line vty 0 15
password <<var_mgmt_passwd>>
 login
 transport input telnet
scheduler allocate 20000 1000
```

Configure the ports where the Nexus 3000 switches connected:

```
interface GigabitEthernet0/0
description Nexus3000-M1:eth1/3
switchport
```

```
interface GigabitEthernet0/1
description Nexus3000-M2:eth1/3
switchport

interface vlan1
ip address <<var_mgmt_isr_ip>> <<var_mgmt_netmask>>
```

Configure the serial ports where the managed devices are connected:

```
interface Async0/0/0
 description NX9000-A
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/1
 description NX9000-B
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/2
 description UCS6200-A
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/3
 description UCS6200-B
 no ip address
 encapsulation slip
 no ip route-cache
```

```
interface Async0/0/4
 description MDS9148-A
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/5
 description MDS9148-B
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/6
 description NX3548-A
 no ip address
 encapsulation slip
 no ip route-cache

interface Async0/0/7
 description NX3548-B
 no ip address
 encapsulation slip
 no ip route-cache

exit
```

Save the running configuration for start-up:

```
copy run start
```

## Management Server Installation

The Cisco UCS C220 M4 server acts as a management server for the solution. VMware ESXi 5.5 must be installed on both Cisco UCS C220 systems. Since separate Cisco MDS switches in the Management Pod for Fibre Channel access are not used, use local disks to install the VMware ESX server.

This section describes the configuration of the Cisco UCS C220 server with the following steps:

1. CIMC configuration
2. VIC1225 configuration
3. Local Storage configuration

Table 14 lists the information used for setting up the Cisco UCS C200 Server in this Cisco UCS Integrated Infrastructure.

**Table 14 Information to Setup Cisco UCS C220 in the Management POD**

| Name | Variable |
|---|---|
| IP address Cisco UCS C220 M1 CIMC Interface | <<var_mgmt_c220-m1_cimc_ip>> |
| IP address Cisco UCS C220 M1 CIMC Interface | <<var_mgmt_c220-m2_cimc_ip>> |
| Netmask | <<var_mgmt_netmask>> |
| Gateway | <<var_mgmt_gw>> |
| Default Password | <<var_mgmt_passwd>> |

## Management Server Configuration



The CIMC, LOM ports, and VIC ports are to connect to the Cisco Nexus 3500 as documented earlier in this document.

## CIMC Configuration

To configure the IP-Address on the CIMC, use one of the default methodologies.

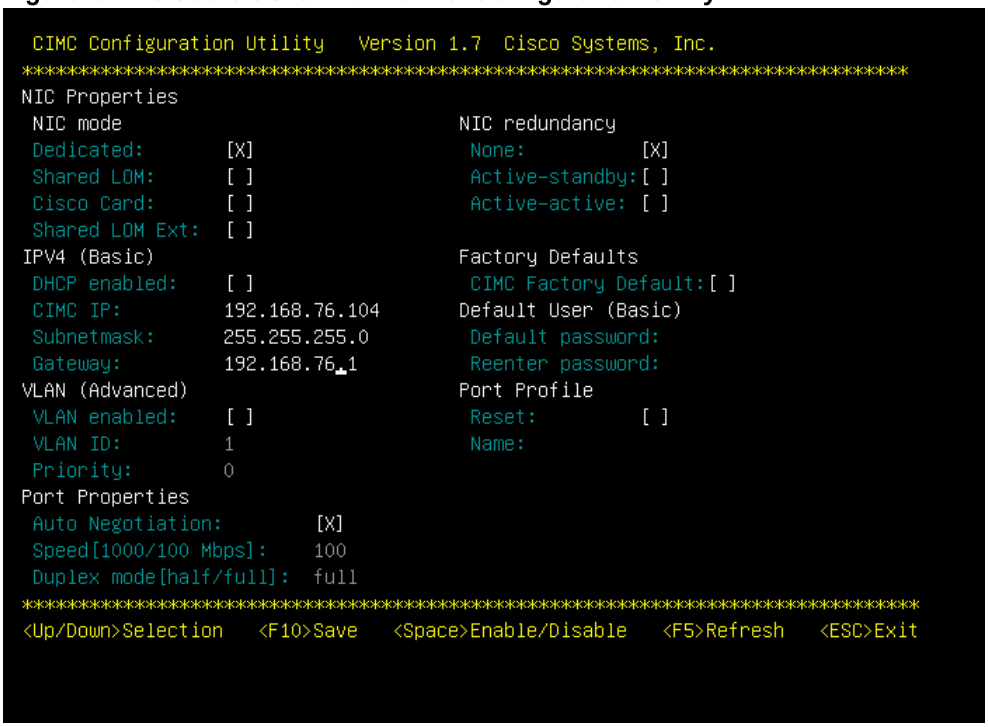
Example: With a direct attached monitor and keyboard, press F8 as soon you see the screen below.

Figure 31 Cisco UCS C220 – POST Screen




Configure the CIMC as required to be accessible from the customer Console LAN.

Figure 32 Cisco UCS C220 – CIMC Configuration Utility




To connect to CIMC to the Management Switch, complete the following steps:

1. Choose Dedicated under NIC mode

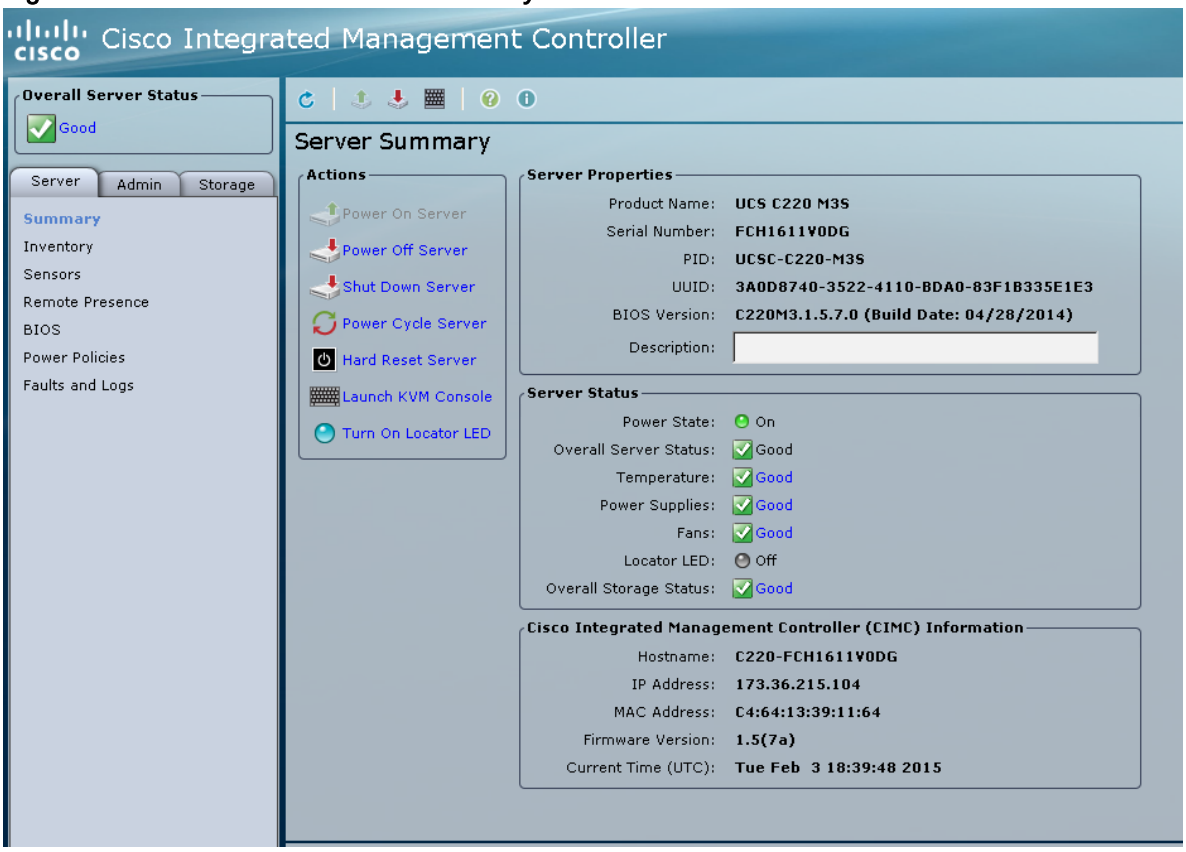
2. Enter the IP address for CIMC <<var_mgmt_c220-m1_cimc_ip>> or <<var_mgmt_c220-m2_cimc_ip>>
3. Enter the Subnet mask for CIMC network <<var_mgmt_netmask>>
4. Enter the Default Gateway for CIMC network <<var_mgmt_gw>>
5. Choose NIC redundancy as None
6. Enter <<var_mgmt_passwd>> as the Default password for admin user under Default User (Basic) and Reenter password

## VIC1225 Configuration

If you are using a Cisco VIC1225, complete the following steps. If you are using the LOM ports, skip this section.

1. Open a web browser and navigate to the Cisco C220 CIMC IP address, <<var_mgmt_c220-m1_cimc_ip>> or <<var_mgmt_c220-m2_cimc_ip>>
2. Enter admin as the user name and enter <<var_mgmt_passwd>> the administrative password.
3. Click Login to log in to CIMC

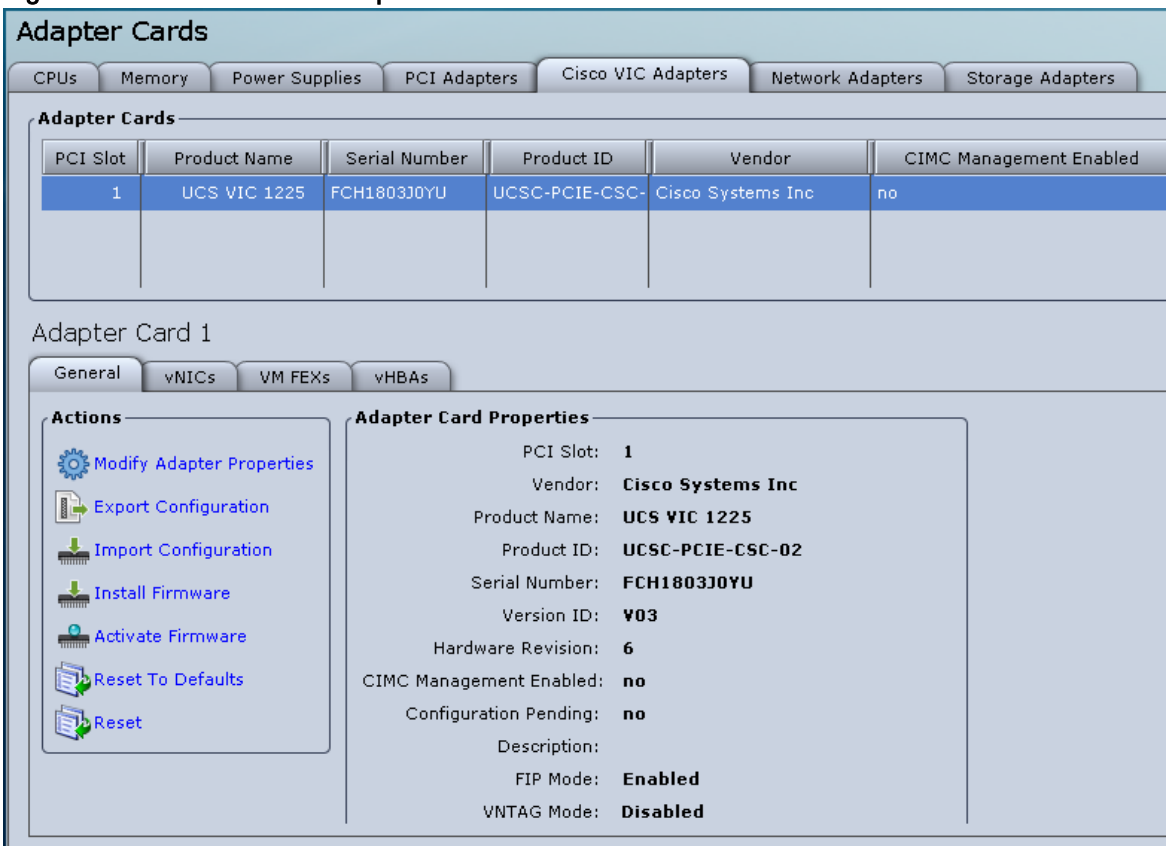
Figure 33 Cisco CIMC – Server Summary




4. Click Inventory under the Server tab

5. On the Control Pane Click Cisco VIC Adapters

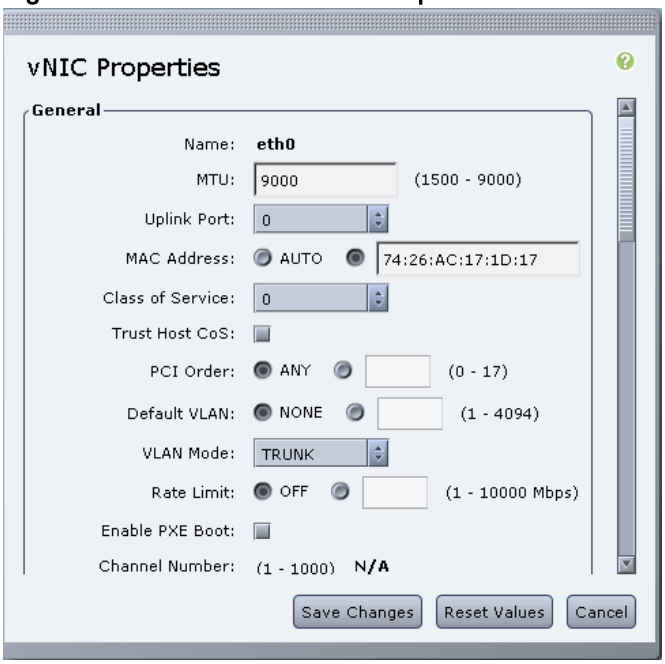
Figure 34 Cisco CIMC – Adapter Cards




6. Click vNICs tab

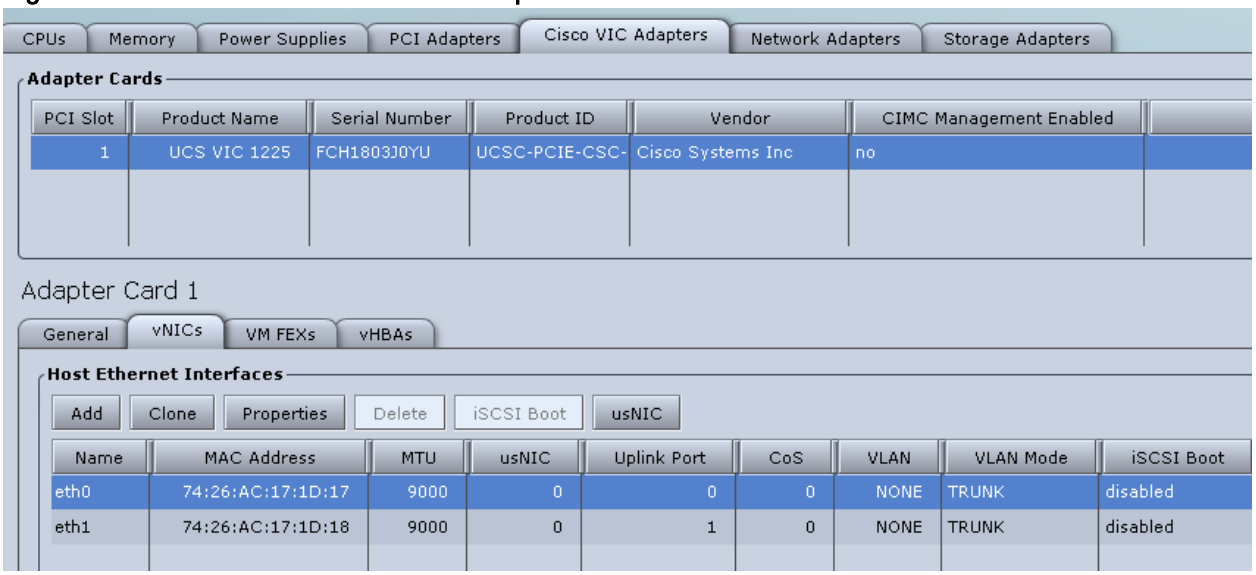
7. Under eth0 Click Properties Change the MTU to 9000 and the VLAN Mode: to TRUNK

Figure 35 Cisco CIMC vNIC Properties




8. In eth1 click Properties and change the MTU to 9000 and the VLAN Mode to TRUNK

Figure 36 Cisco CIMC – List of VIC Adapters and vNICs




9. Reboot the server From Server > Summary > Hard Reset Server

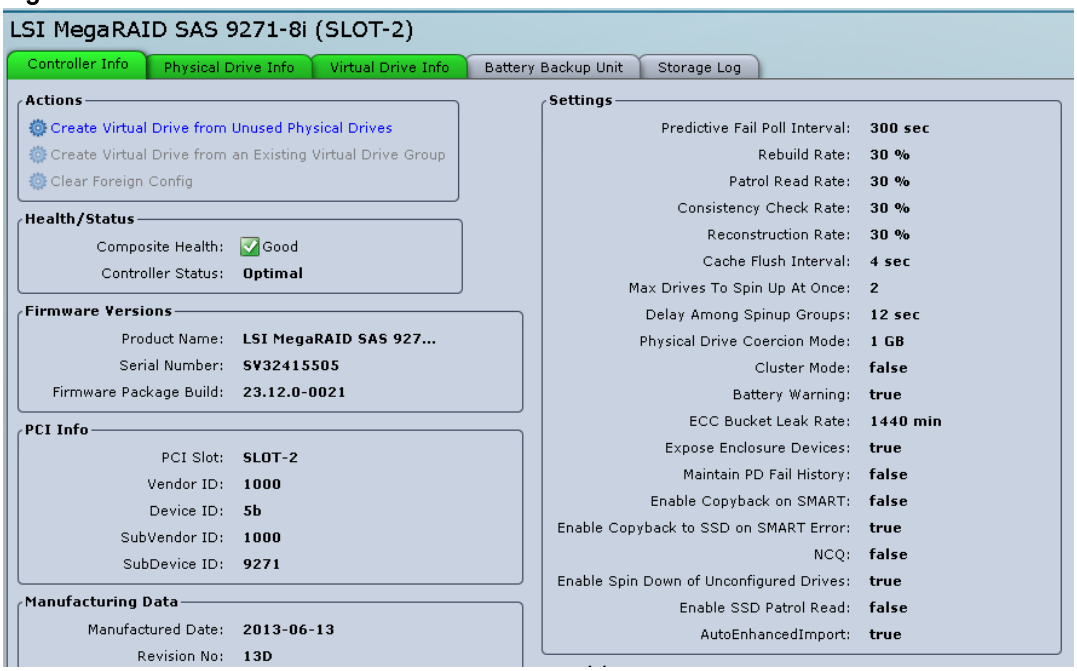
## Local Storage Configuration

It is mandatory to create a redundant virtual drive (RAID 1) on the internal disks to host VMware ESXi. Optionally, the EMC VNX storage can be used to create a redundant virtual drive if FC switches are available to connect Server and Storage.

You can set up the RAID1 with two internal disks from CIMC web Browser to install ESXi.

1. On the Control Pane click the Storage tab

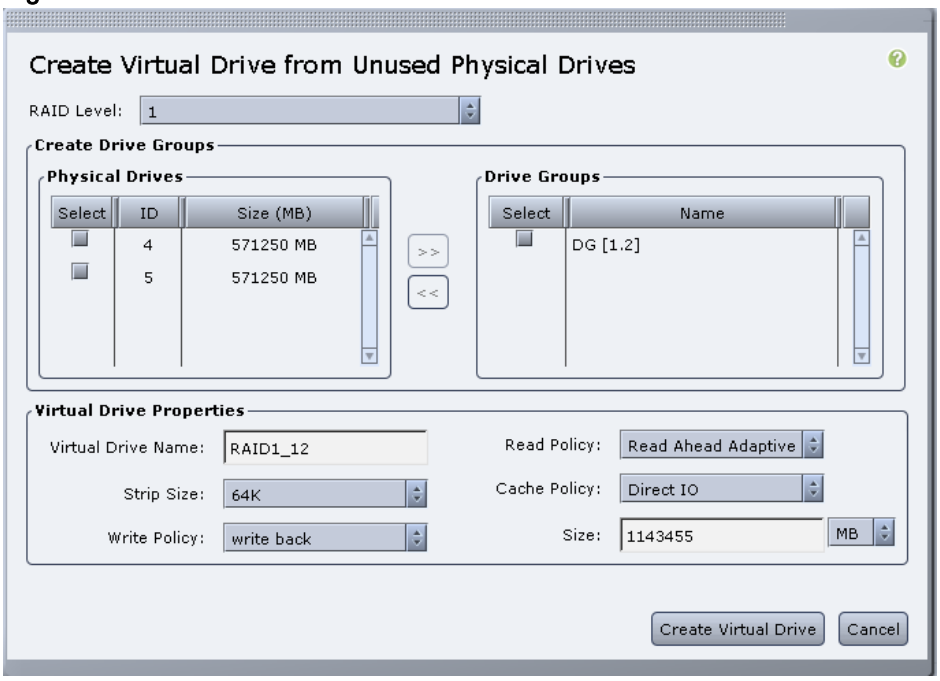
**Figure 37 Cisco CIMC – RAID Controller Overview**




2. Click Create Virtual Drive from Unused Physical Drives

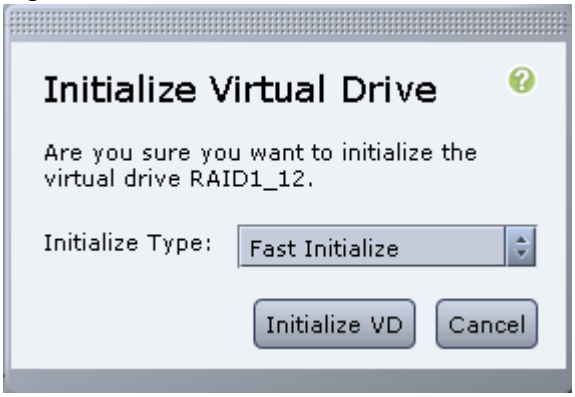
3. Choose RAID Level 1 and Select the Disks and Click >> to add them in the Drive Groups

Figure 38 Cisco CIMC – Create Virtual Drive




4. Click Create Virtual Drive to create Virtual Drive
5. Click the Virtual Drive Info
6. Click Initialize

Figure 39 Cisco CIMC – Initialize Virtual Drive

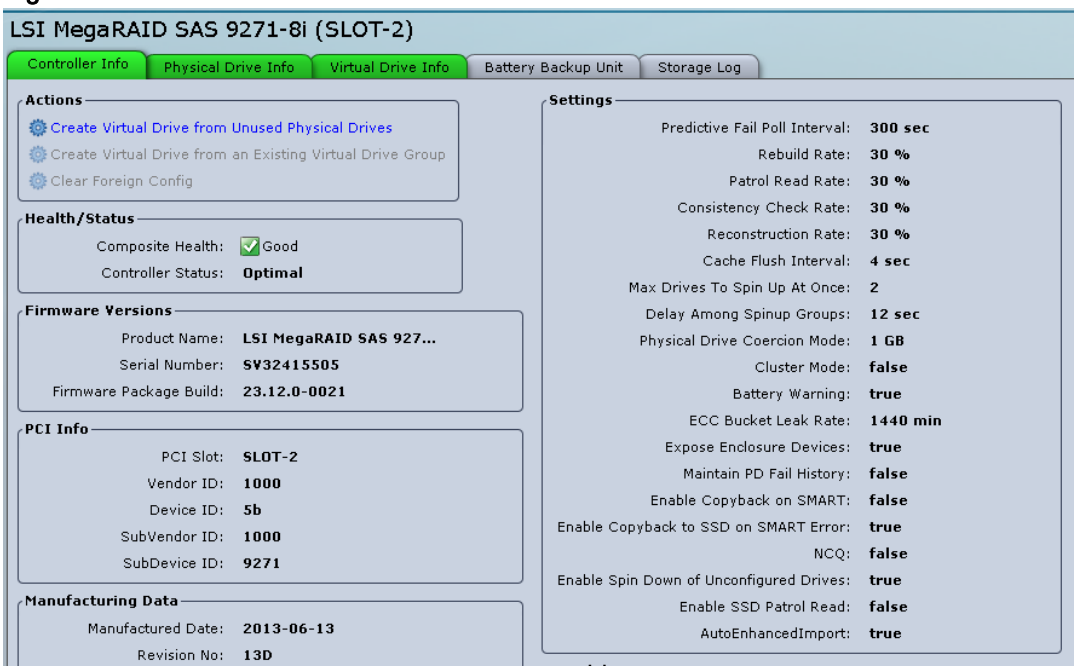



7. Click Initialize VD

You can set up the RAID0 with all the unused internal disks from the CIMC web browser to use for VSAN with VMware ESXi.

8. On the Control Pane Click Storage tab

Figure 40 Cisco CIMC – RAID Controller Overview



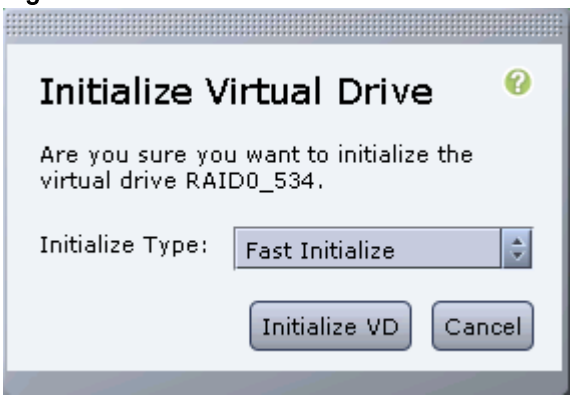

9. Click Create Virtual Drive from Unused Physical Drives
10. Choose RAID Level 1 and Select the Disks and Click >> to add them in the Drive Groups
11. Click Create Virtual Drive to create Virtual Drive
12. Click the Virtual Drive Info

Figure 41 Cisco CIMC – RAID Controller Virtual Drive Info



13. Click Initialize

**Figure 42 Cisco CIMC – Initialize Virtual Drive**

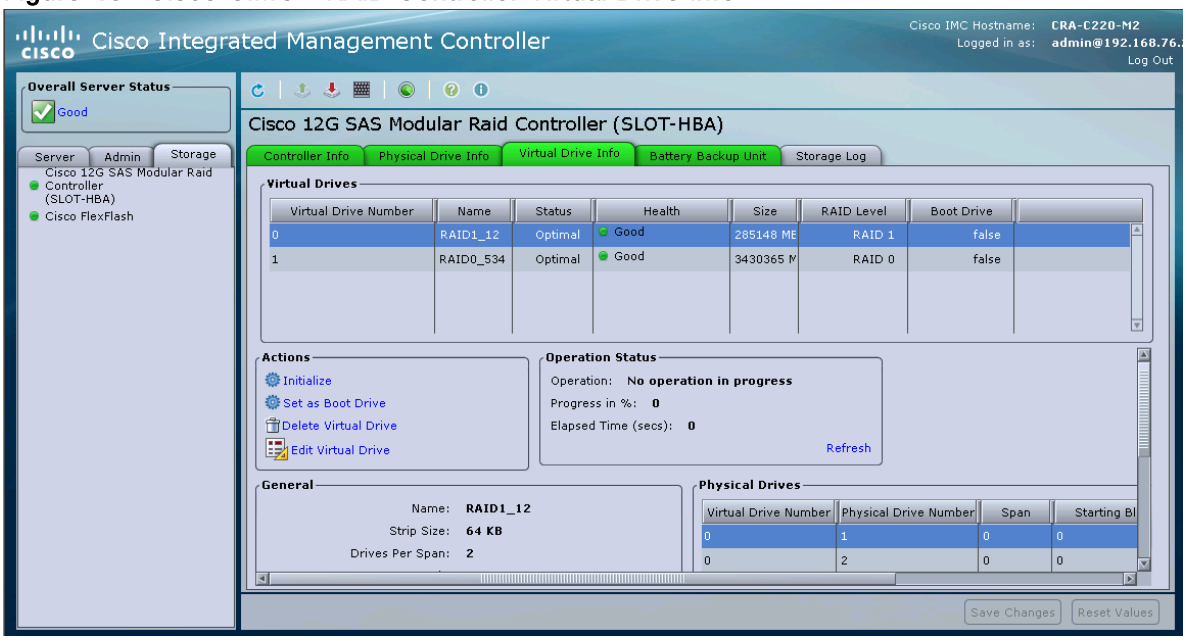



14. Click Initialize VD

## Define the Boot Define

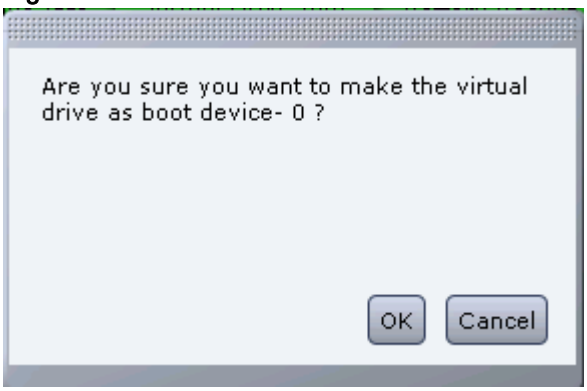
1. Select Virtual Drive 0
2. Click Set as Boot Drive

**Figure 43 Cisco CIMC – RAID Controller Virtual Drive Info**



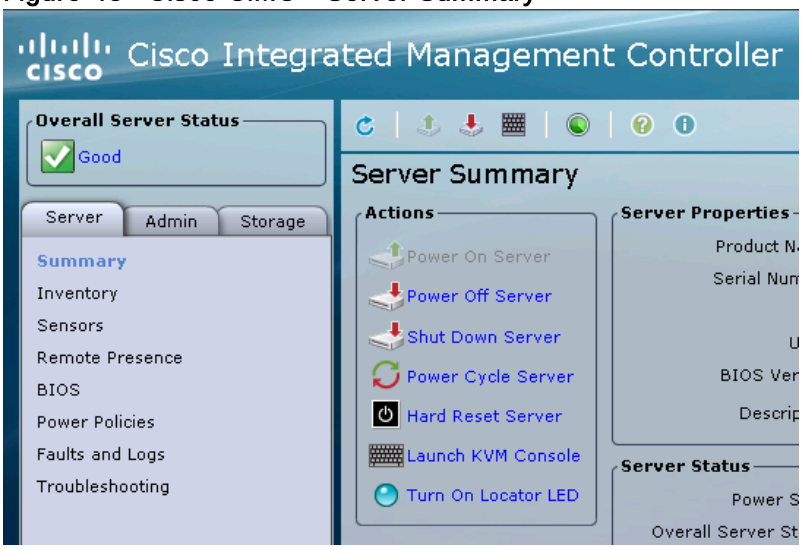

3. Click OK

**Figure 44 Cisco CIMC – Make Virtual Drive as Boot Device**




4. Reboot the server From Server --> Summary → Hard Reset Server

**Figure 45 Cisco CIMC – Server Summary**




## EMC VNX Storage Configuration

This section describes the configuration of the EMC VNX storage in the Management Pod for NFS access only and details the following:

- Initial Configuration
- Datamover configuration
- Storage Pool configuration
- Filesystem and NFS share configuration

The basic installation and configuration of EMC VNX storage is done by the EMC service technician at delivery time. Please inform the person to use the following information for the configuration:

## Initial Storage Setup

The initial setup of the base VNX5400 is done using the VNX Installation Assistant for File/Unified (VIA). The initial setup of the expansion arrays (block only) is performed using the Unisphere Storage System Initialization Wizard. Additionally, Unisphere CLI is required. Both tools are available for download from the tools section from EMC's Online Support Website: https://support.emc.com/



These tools are only available to EMC personnel and EMC's Authorized Service Providers. The initialization wizards are in the latest toolkit and Unisphere CLI is separate.



Refer to EMC's documentation "Getting Started with VNX Installation Assistant for File/Unified" and "EMC VNX VNX5400 Block Installation Guide" for more detailed information.

With VIA, the IP addresses of the VNX Control Station as well as the storage processors will be specified for just the Base array. Note that the IP addresses must be in the IP range of the management network and each VNX array within a multi-array HANA appliance must have its own dedicated IP addresses as per Table 15 .

The following Information is used in VIA for the setup of the VNX arrays in this Cisco UCS Integrated Infrastructure with EMC VNX Storage.

**Table 15 Information Required to Setup EMC VNX in the Management POD**

| Name | Variable |
|---|---|
| IP address Control Station | <<var_mgmt_vnx_cs1_ip>> |
| Hostname Control Station | <<var_mgmt_vnx_cs1_hostname>> |
| IP address SP-A | <<var_mgmt_vnx_spa_ip>> |
| Hostname SP-A** | <<var_mgmt_vnx_spa_hostname>> |
| IP address SP-B | <<var_mgmt_vnx_spb_ip>> |
| Hostname SP-B** | <<var_mgmt_vnx_spb_hostname>> |
| Netmask of the Management Network | <<var_mgmt_netmask>> |
| Gateway | <<var_mgmt_gw>> |
| Primary DNS Server | <<var_nameserver_ip>> |
| NTP Server | <<var_global_ntp_server_ip>> |
| DNS Domain | <<var_mgmt_dns_domain_name>> |
| Default Password | <<var_mgmt_vnx_passwd>> |

| Name | Variable |
|---|---|
| VNX Admin User | <<var_mgmt_vnx_user>> |
| VNX Storage Pool Name | <<var_mgmt_storage_pool_name>> |
| VNX LUN Size for ESXi Boot devices | <<var_mgmt_lun_size>> |
| Number of ESXi Boot-LUNs to create | <<var_mgmt_number_luns>> |
| LACP Interface name | <<var_mgmt_vnx_lacp_name>> |
| Logical Interface name for VLAN 177 | <<var_mgmt_vnx_if1_name>> |
| File System Name for ESXi Datastore | <<var_mgmt_vnx_fs1_name>> |
| File System Size for ESXi Datastore | <<var_mgmt_fs_size>> |
| Maximal allowed capacity for the File System | <<var_mgmt_fs_max_capa>> |
| IP Address in the NFS Network for ESXi host 1 | <<var_mgmt_esx1_nfs_ip>> |
| IP Address in the NFS Network for ESXi host 2 | <<var_mgmt_esx2_nfs_ip>> |



** Setting up the SP hostnames is not a part of the VIA process. The hostnames can be specified later within the Unisphere GUI.

In order to run VIA and the Unisphere Storage System Initialization Wizard, a service laptop running Windows needs to be connected to the management LAN.



When the VIA configuration process has completed, it cannot be run again.

The following screen shots show the VIA pre-configuration setup procedure. Use the passwords specified in the worksheet in the pre-installation section of this document.

Figure 46 EMC VIA Setup the Control Station for Accessing the Network

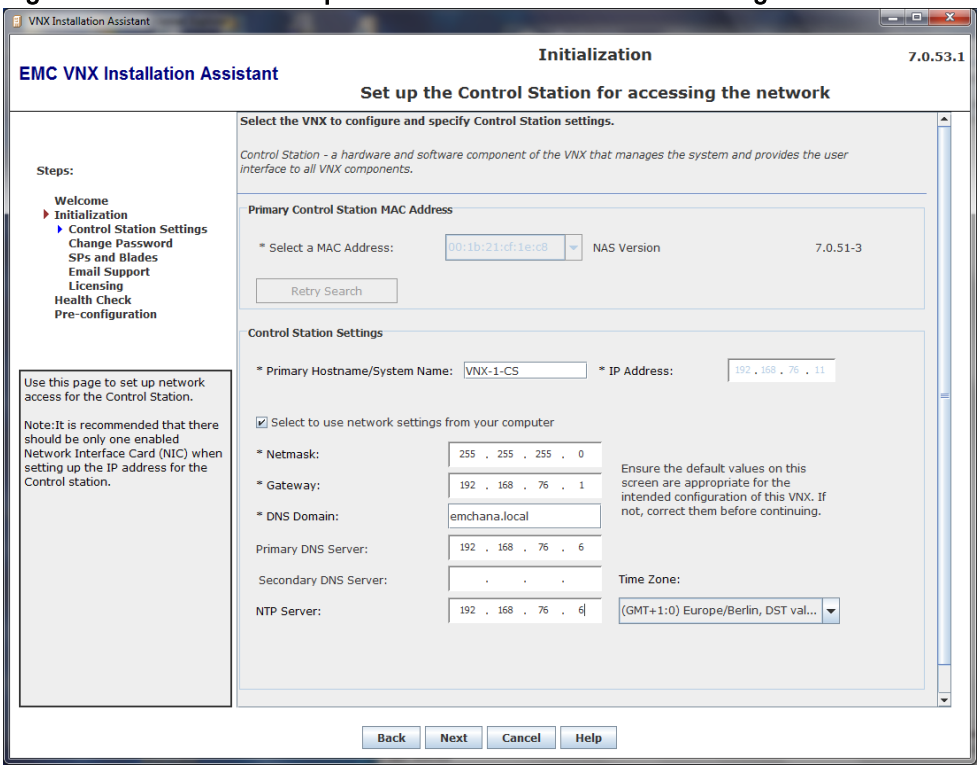



Figure 47 EMC VIA Change the Default Passwords

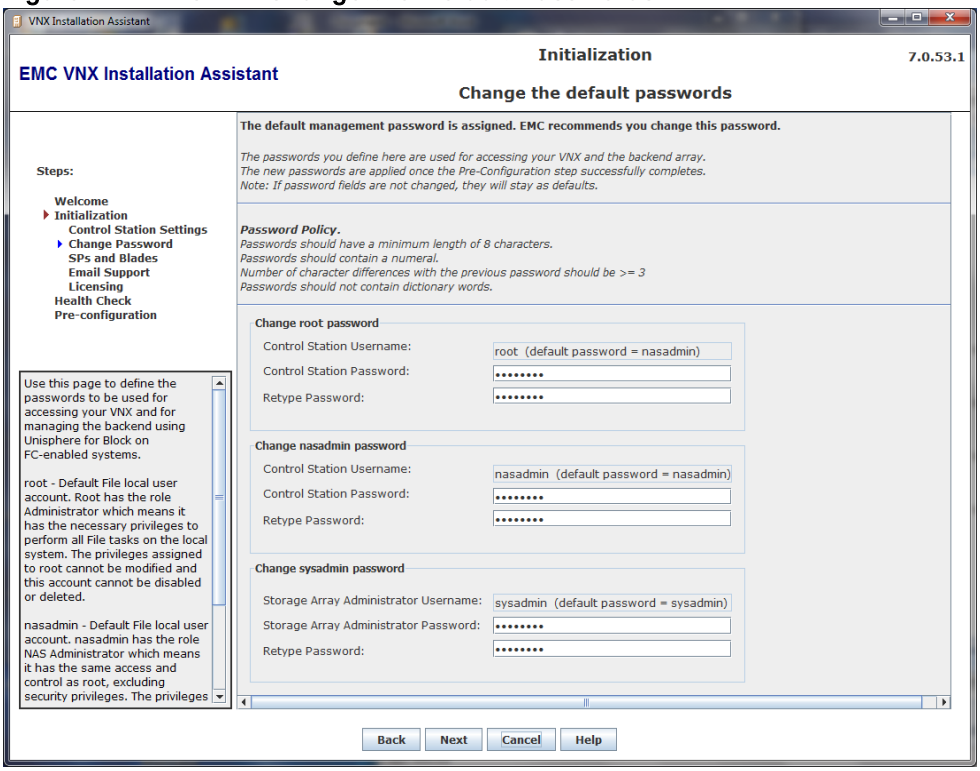


Figure 48 EMC VIA Setting up the Blades and Storage Processors

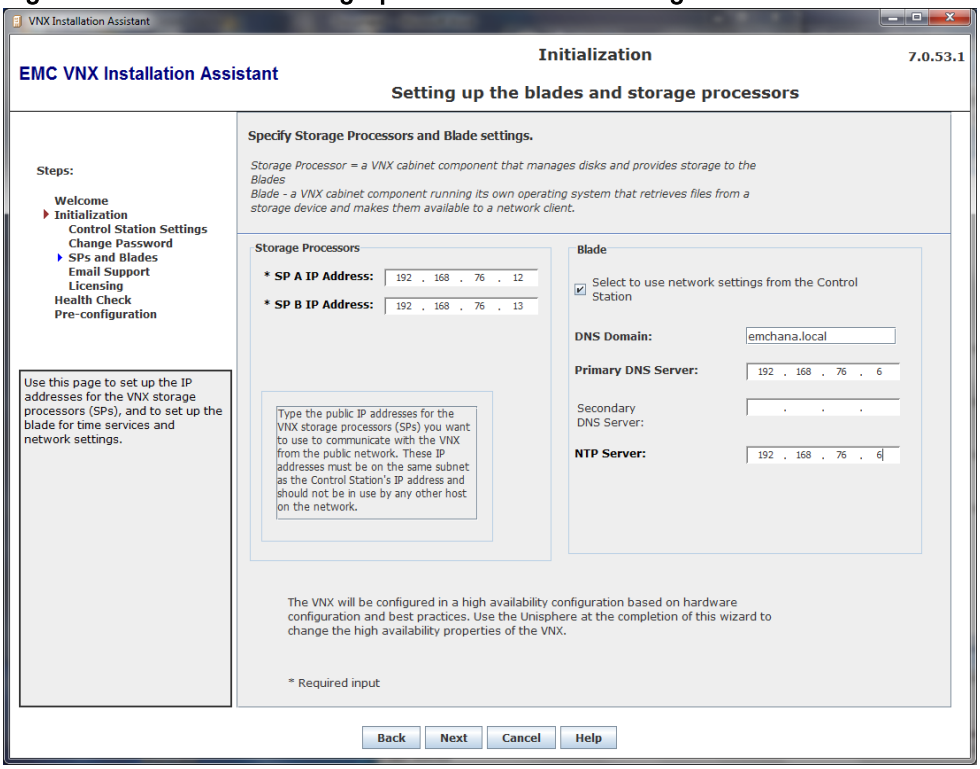



Figure 49 EMC VIA Configuring Email Support and Customer Information

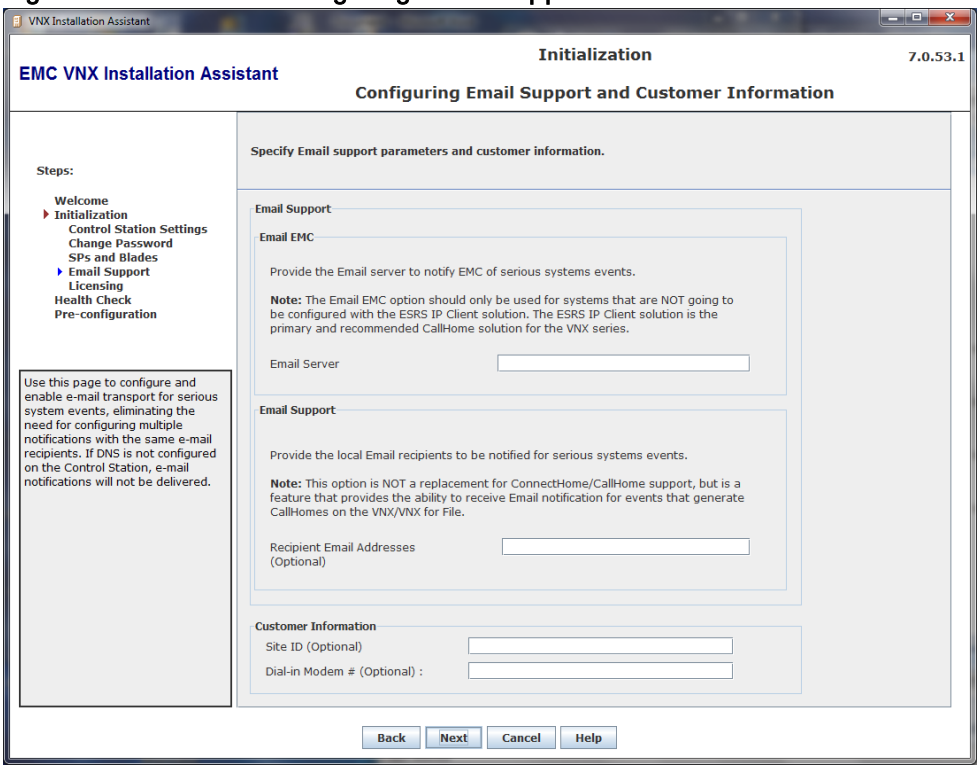


Figure 50 EMC VIA Collecting License Information

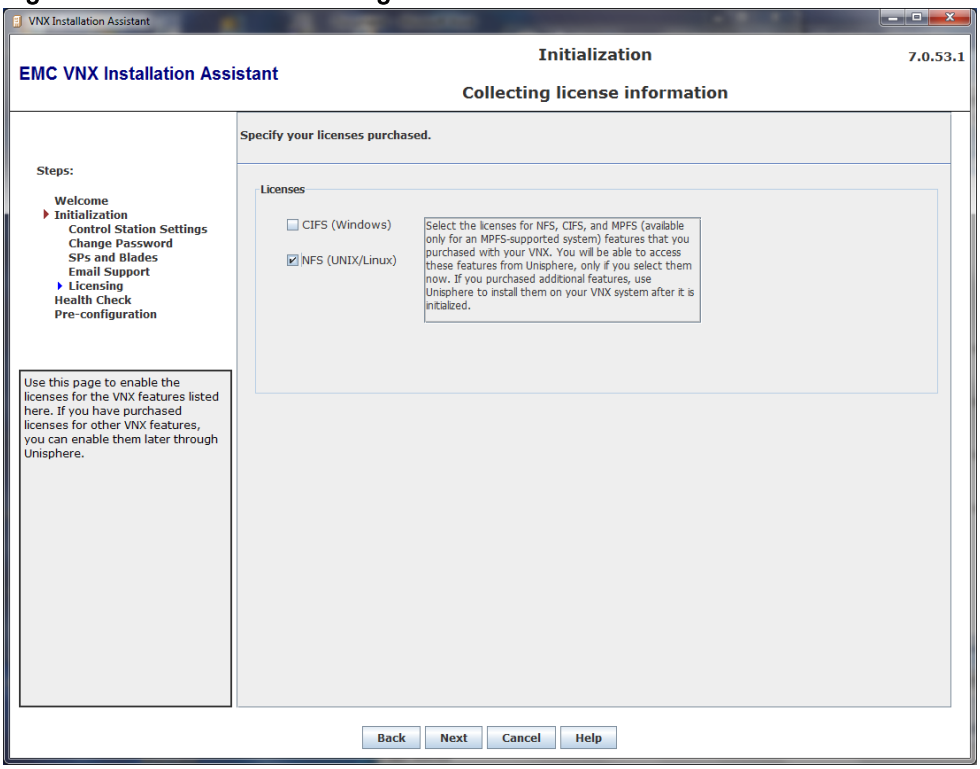



Figure 51 EMC VIA Health Check

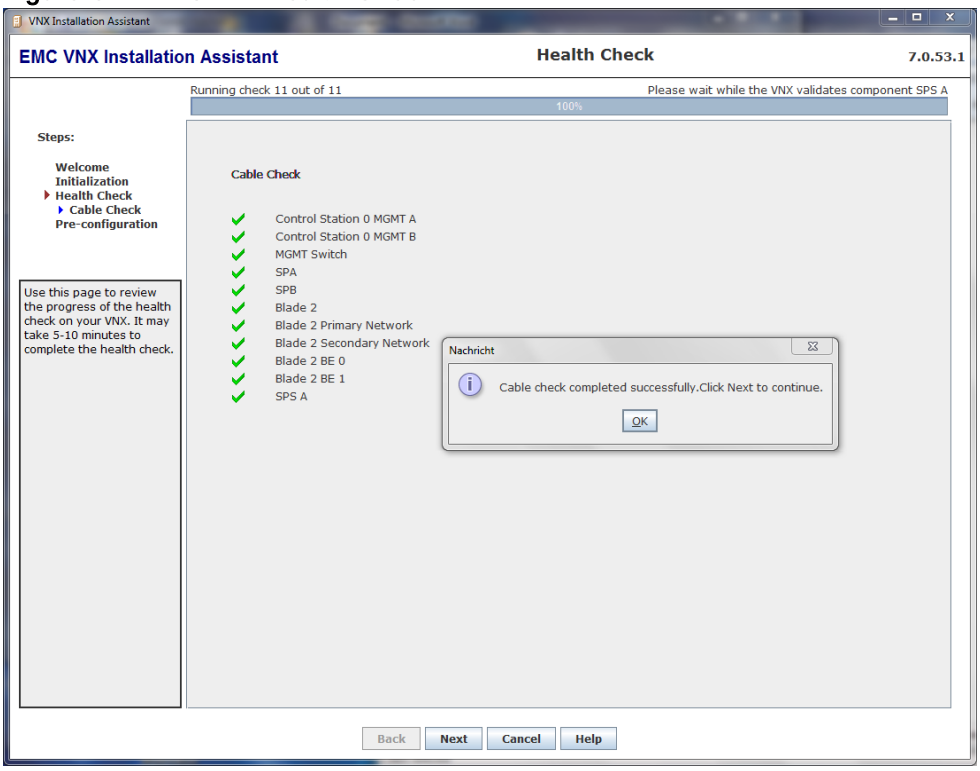


Figure 52 EMC VIA Pre-configuration

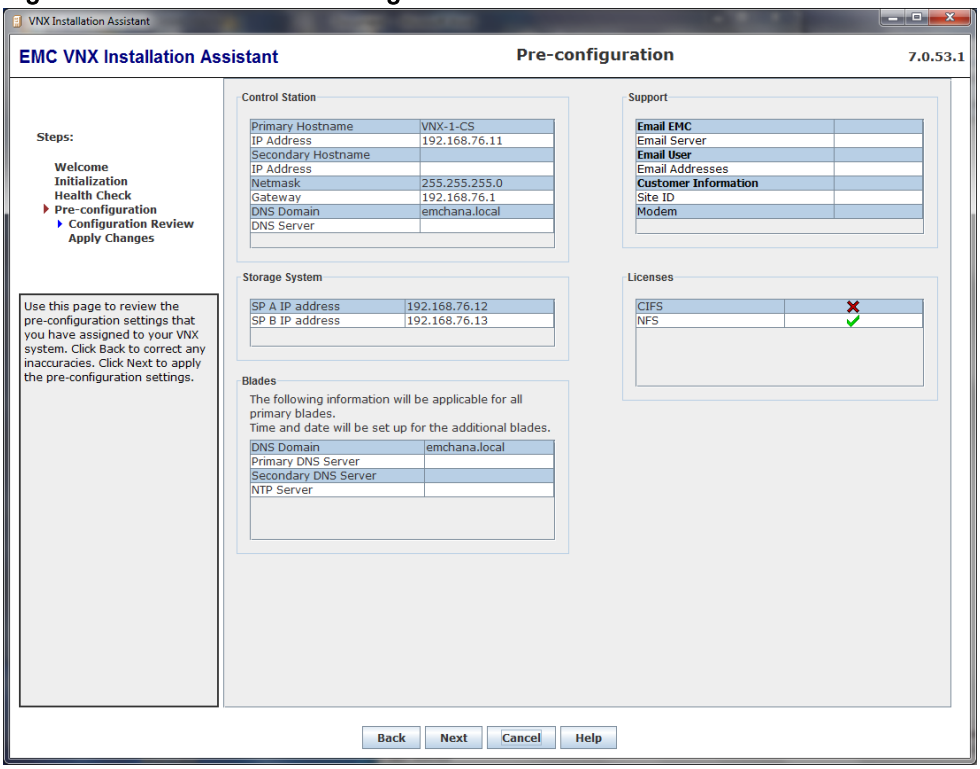



Figure 53 EMC VIA Applying the Specified Configuration Changes

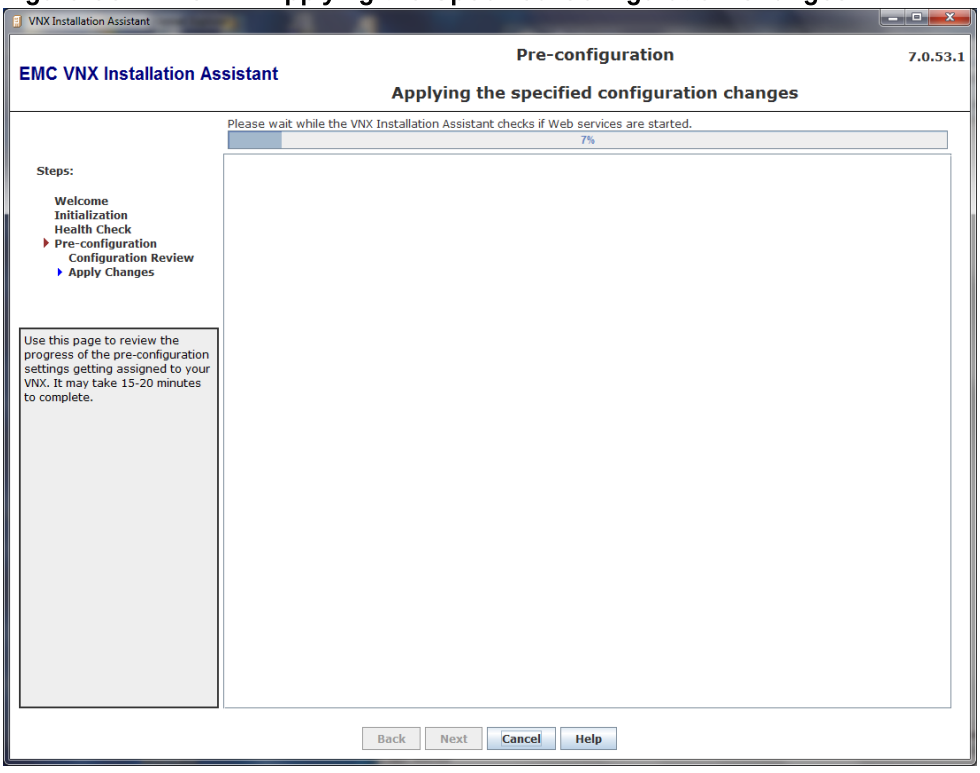
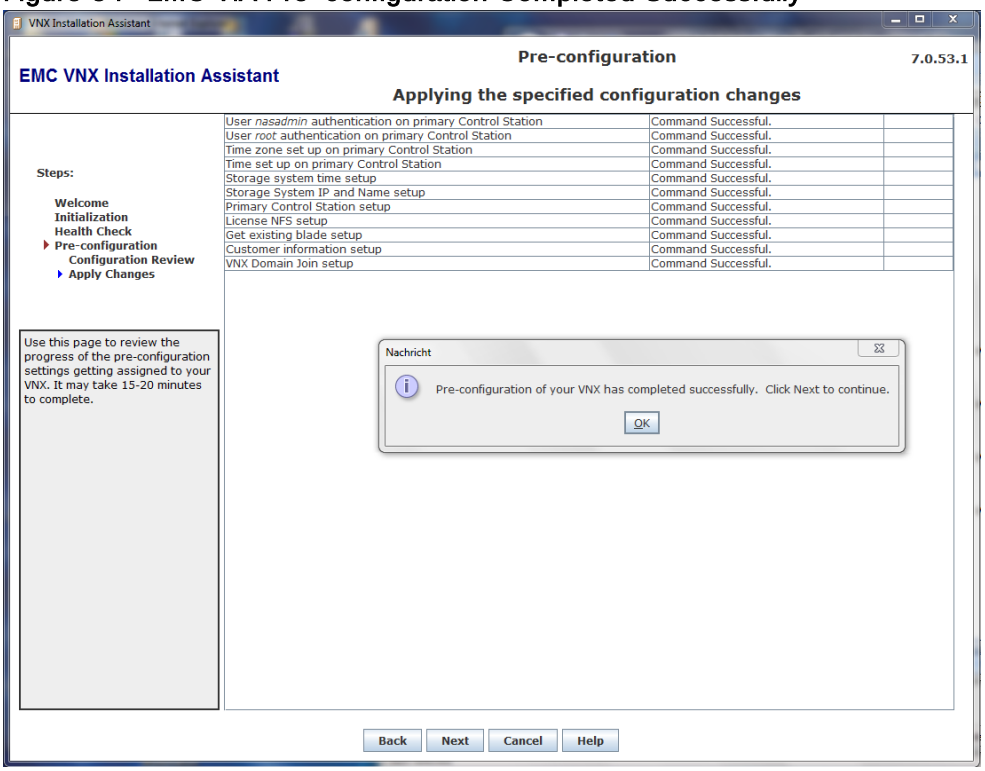


Figure 54 EMC VIA Pre-configuration Completed Successfully




VIA does not work for block-only arrays. These arrays need to be initialized using the Unisphere Storage System Initialization Wizard. Refer to the EMC documentation “EMC VNX Block Installation Guide” for information about how to download and run this tool.

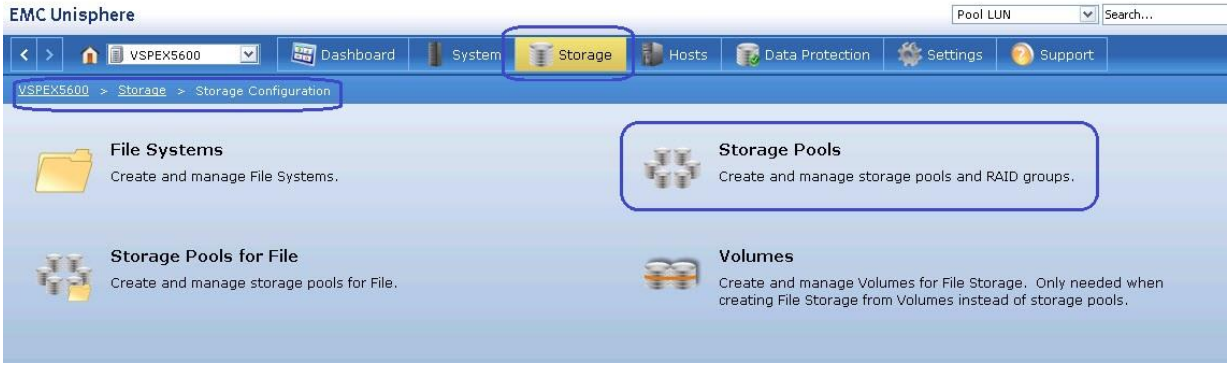
The Storage is now manageable through EMC Unisphere over the network.

## Configure Storage Pool

To create a storage pool and carve boot LUNs on per server basis, complete the following steps:

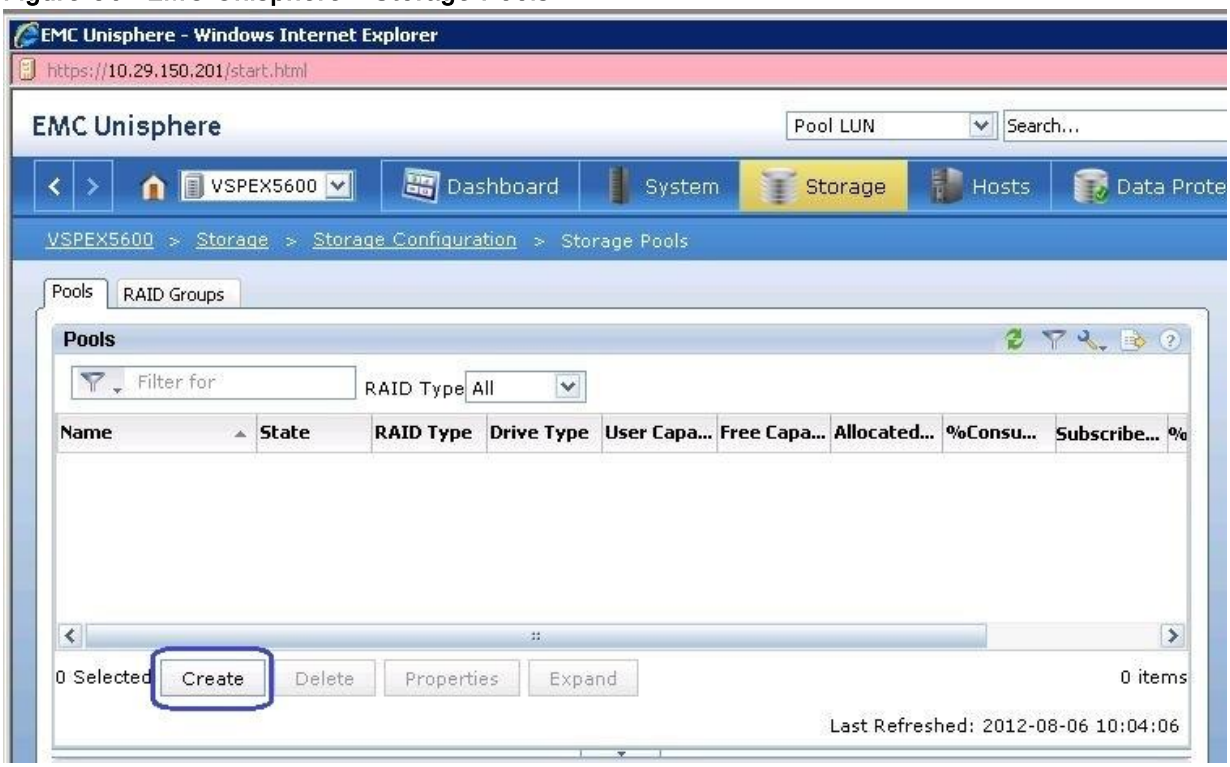
1. Open http://<<var_mgmt_vnx_cs1_ip>>/ in a Web browser
2. Log in to EMC VNX Unisphere GUI with User <<var_mgmt_vnx_user>> and Password <<var_mgmt_vnx_passwd>>
3. Select Mgmt-VNX from the Drop-down list...
4. Click the Storage tab on the top.
5. Select Storage Configuration → Storage Pools.

Figure 55 EMC Unisphere – Storage Configuration




6. From the Storage Pools click Create.

Figure 56 EMC Unisphere – Storage Pools



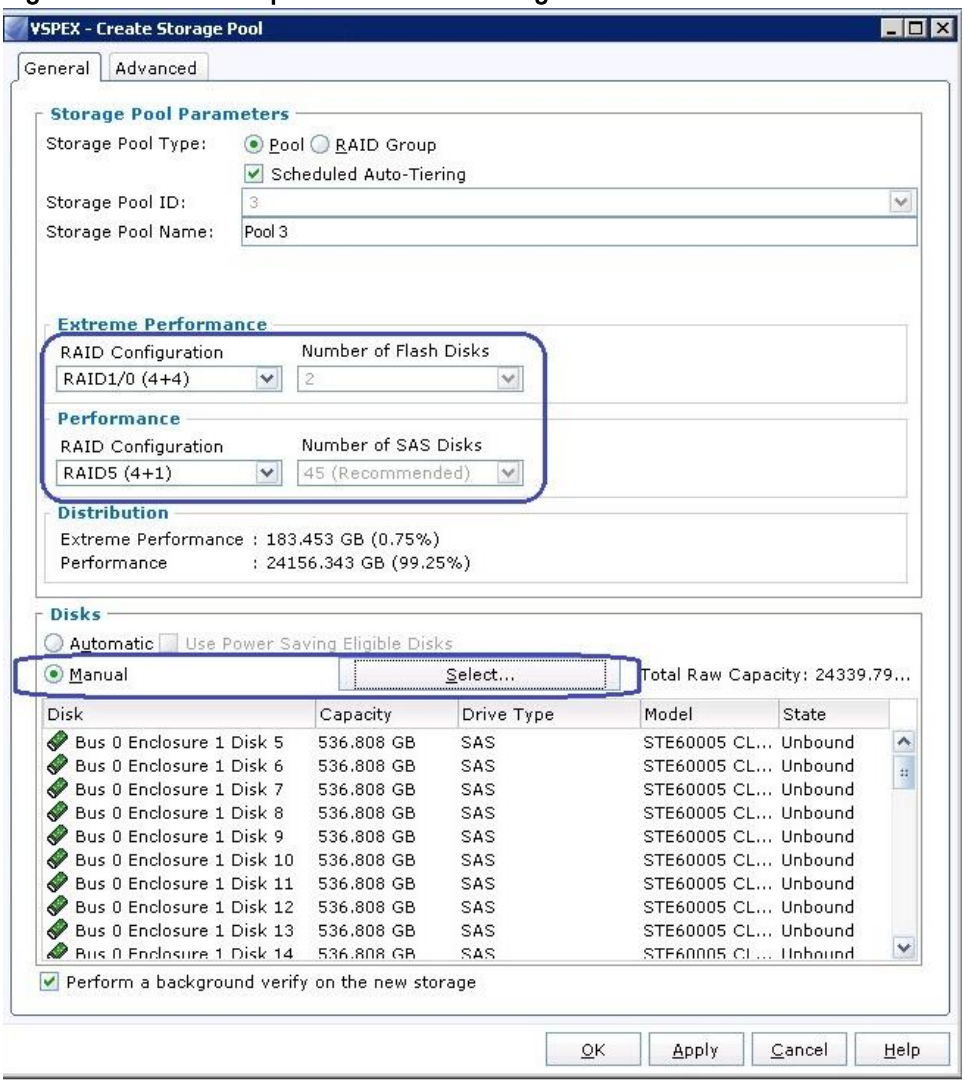

7. Use <<var_mgmt_storage_pool_name>> as Storage Pool Name

8. Select Manual and select <<var_mgmt_number_disks>> SAS drives and add to the pool.

9. Under Performance, select RAID type as RAID5 (4+1) from the drop down list.

10. Number of SAS disks would be automatically populated based on number of disks that you just manually added to the pool.

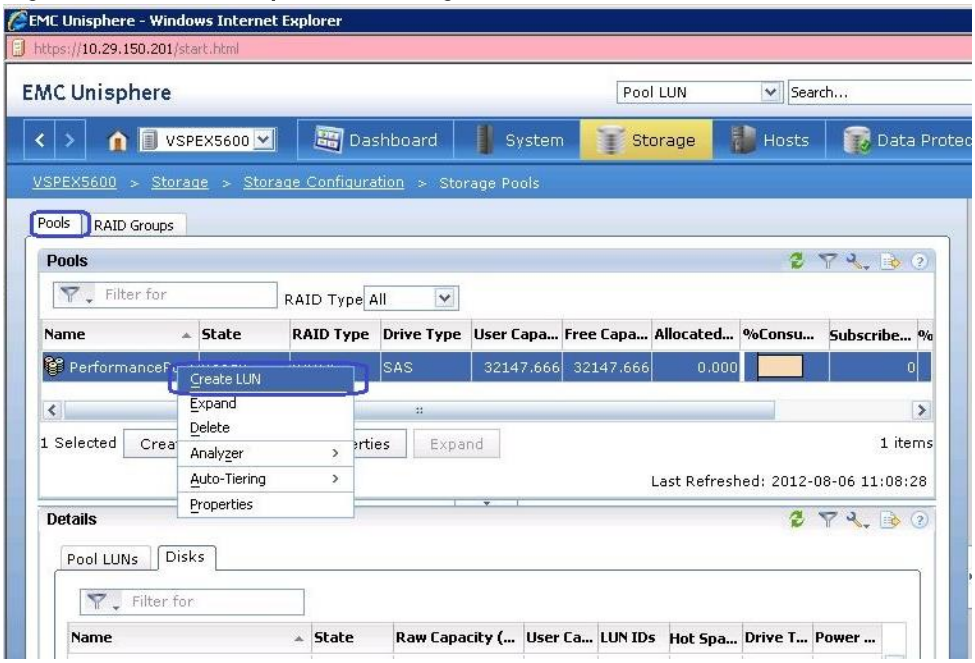
Figure 57 EMC Unisphere – Create Storage Pool




11. Create LUNs from the newly created pool for NFS Datastore;

12. Click Storage and right-click <<var_mgmt_storage_pool_name>> and select Create LUN.

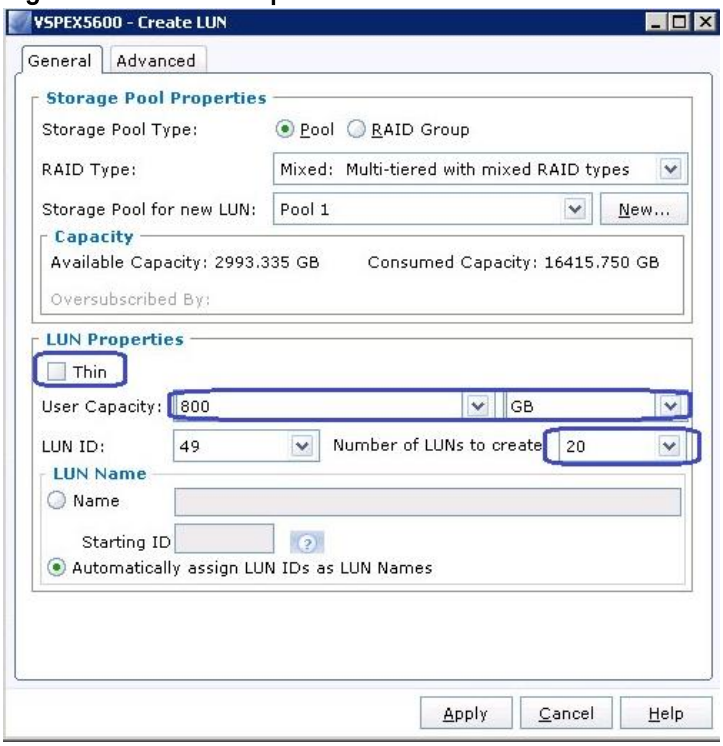
Figure 58 EMC Unisphere – Storage Pools




13. Make sure the Thin check box is unchecked

14. User Capacity is <<var_mgmt_lun_size>>, and number of LUNs to create is <<var_mgmt_number_luns>>.

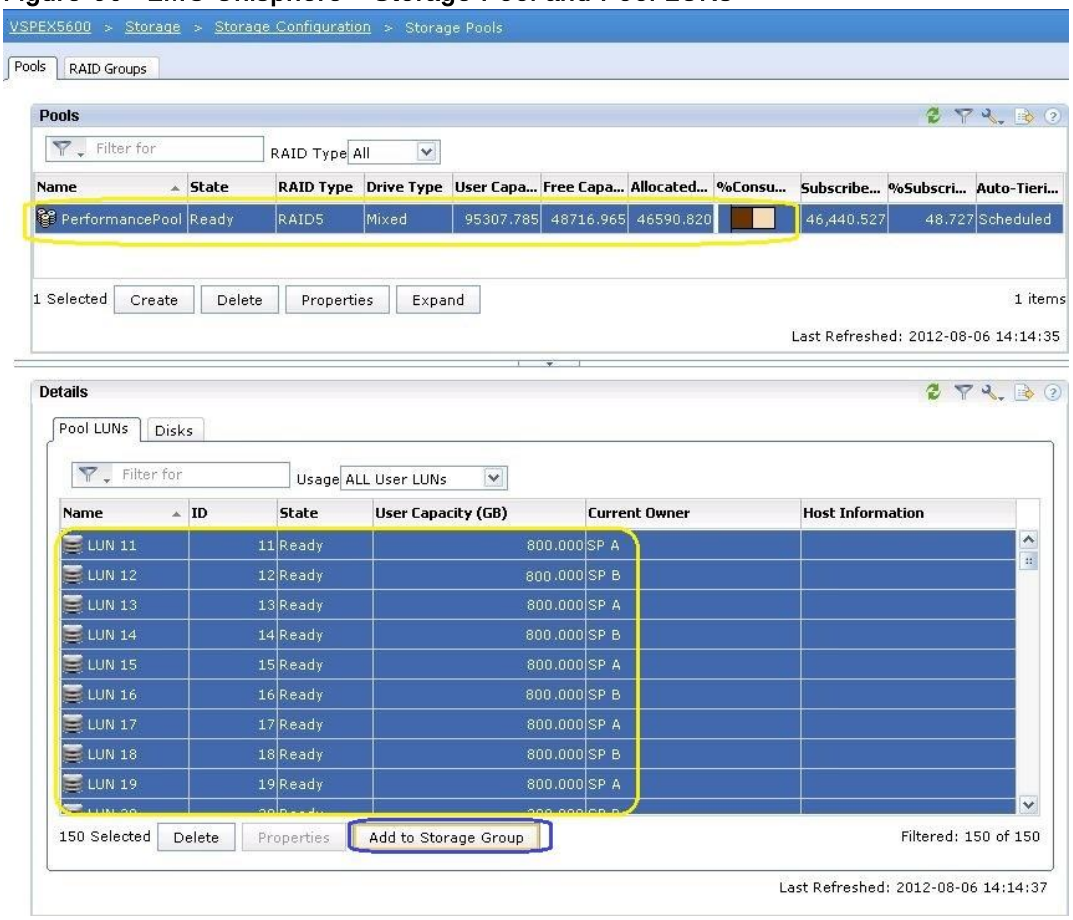
Figure 59 EMC Unisphere – Create LUN



15. Select the pool

16. Select all the newly created LUNs and Click  Add to Storage Group.

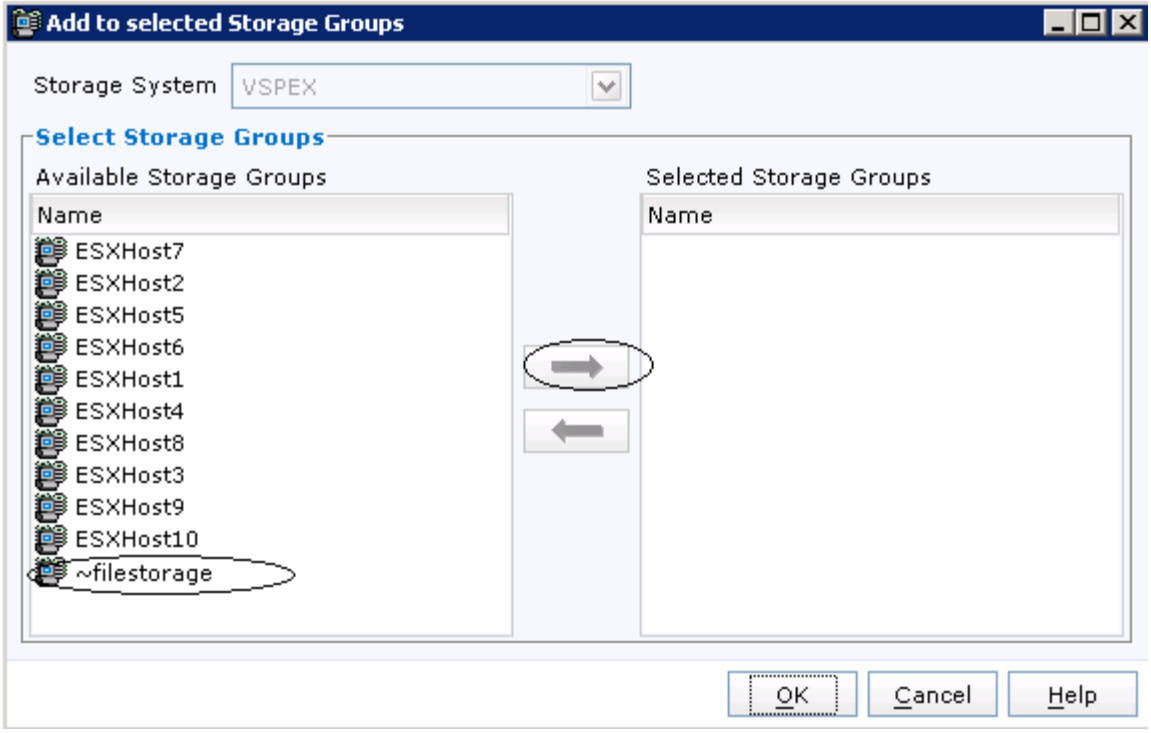
**Figure 60  EMC Unisphere – Storage Pool and Pool LUNs**




17. Select ~filestorage from the Available Storage Groups and click the Right-Arrow

18. When ~filestorage is selected on right hand side, click OK.

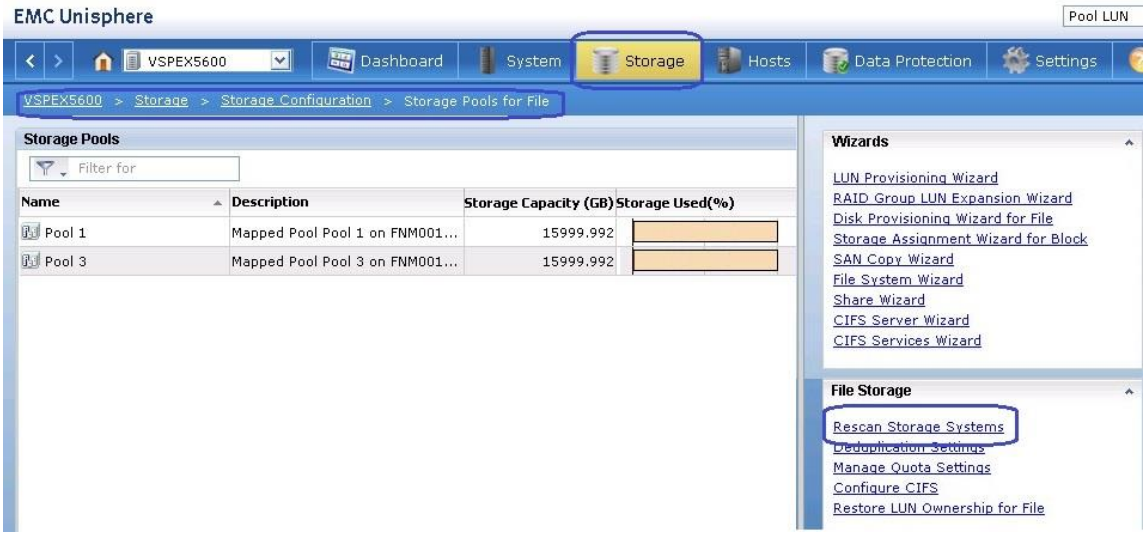
Figure 61 EMC Unisphere – Add to selected Storage Groups




19. Go to Storage → Storage Configuration → Storage Pools for Files, and click Rescan storage systems as shown below. Rescan will take up to 4 minutes.

20. When the rescan finishes (track the progress at "Background task for files" page under System menu), click the Refresh button. The newly created storage pools must be visible on the left side of the window as shown below.

Figure 62 EMC Unisphere – List of Storage Pools for File

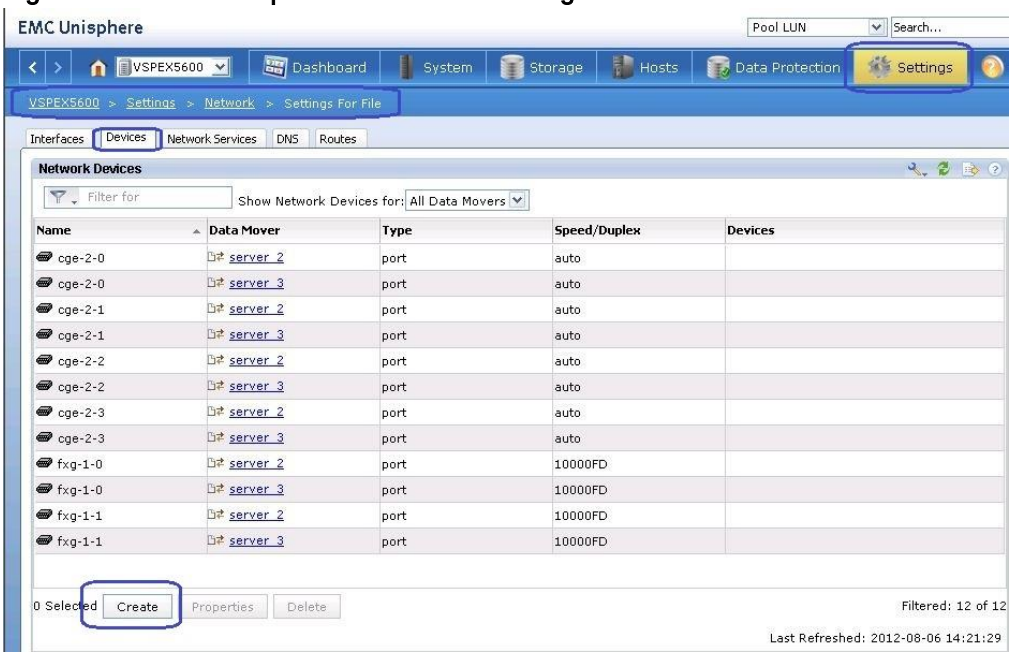


## Configure Network on the Datamover

At this point, the volume is created. The next step is to create the highly available network access for the NFS volume. To Create LACP interface, complete the following steps:

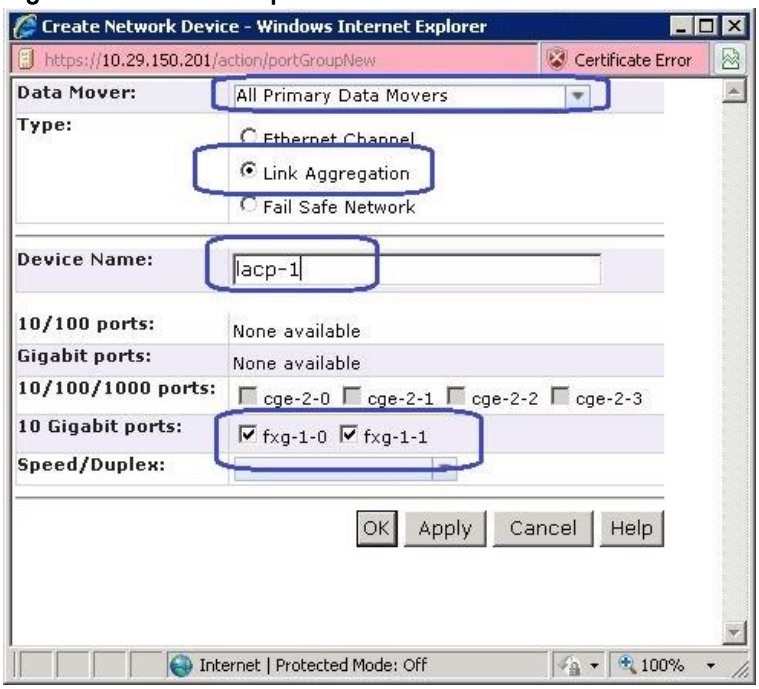
1. Navigate to Settings > Network > and select Settings for File.
2. Click the Devices tab.
3. Click Create.

**Figure 63 EMC Unisphere – Network Settings for File**



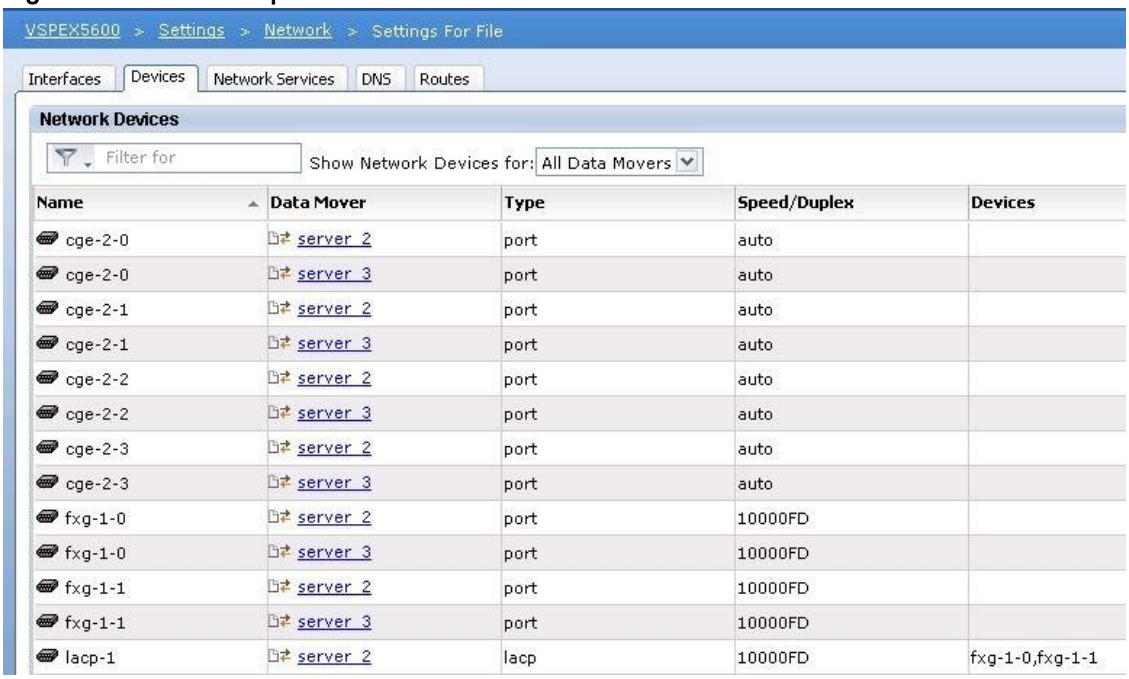

4. In the Data Mover drop-down list, select All Primary Data Movers.
5. Select Type as Link Aggregation.
6. Enter <<var_mgmt_vnx_lacp_name>> as the Device Name.
7. Check the 10 Gigabit ports fxg-1-0 and fxg-1-1.
8. Click OK to proceed to the Network Device creation.

Figure 64 EMC Unisphere – Create Network Device




The screen shot below shows the creation of LACP Network device name as lacp-1.

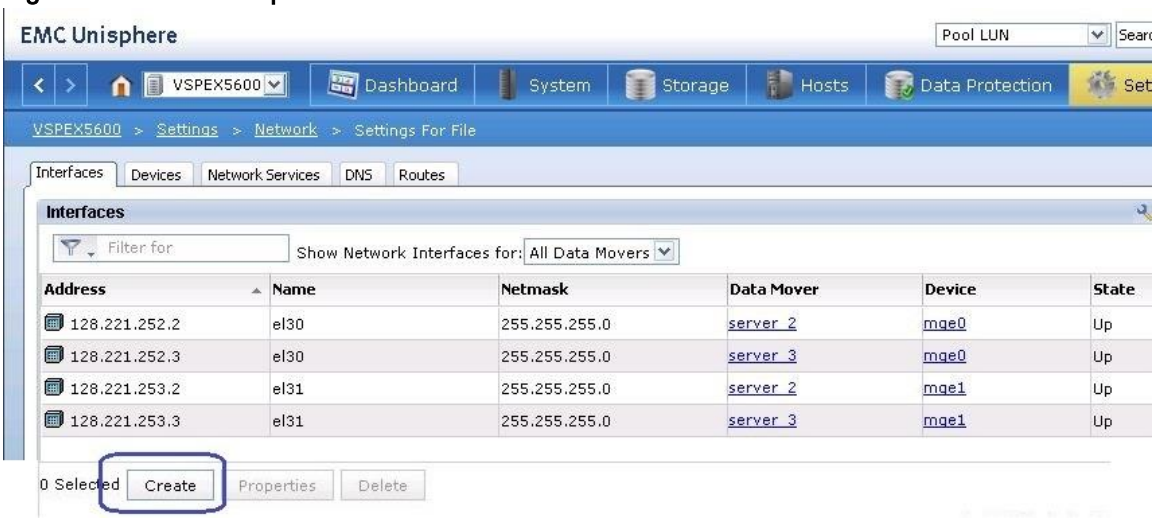
Figure 65 EMC Unisphere – List of Network Devices




| Name | Data Mover | Type | Speed/Duplex | Devices |
|---|---|---|---|---|
| cge-2-0 | server_2 | port | auto | |
| cge-2-0 | server_3 | port | auto | |
| cge-2-1 | server_2 | port | auto | |
| cge-2-1 | server_3 | port | auto | |
| cge-2-2 | server_2 | port | auto | |
| cge-2-2 | server_3 | port | auto | |
| cge-2-3 | server_2 | port | auto | |
| cge-2-3 | server_3 | port | auto | |
| fxg-1-0 | server_2 | port | 10000FD | |
| fxg-1-0 | server_3 | port | 10000FD | |
| fxg-1-1 | server_2 | port | 10000FD | |
| fxg-1-1 | server_3 | port | 10000FD | |
| lacp-1 | server_2 | lacp | 10000FD | fxg-1-0,fxg-1-1 |

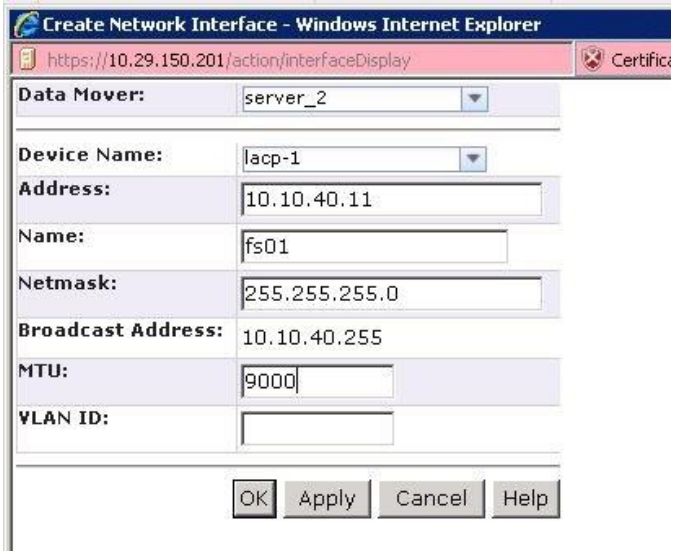
9. From the Settings for File tab, select Interfaces and click Create.

Figure 66 EMC Unisphere – List of Network Interfaces




10. Select Data Mover as server_2.
11. Choose Device name as lacp-1 from the drop down list.
12. Specify <<var_mgmt_vnx_dm2_ip>> as the IP address.
13. Netmask is <<var_mgmt_netmask>>.
14. Enter <<var_mgmt_vnx_if1_name>> as the Interface name.
15. MTU value as 9000 to allow jumbo frames for the lacp interface.
16. Specify <<var_mgmt_esx_nfs_vlan_id>> as the VLAN ID

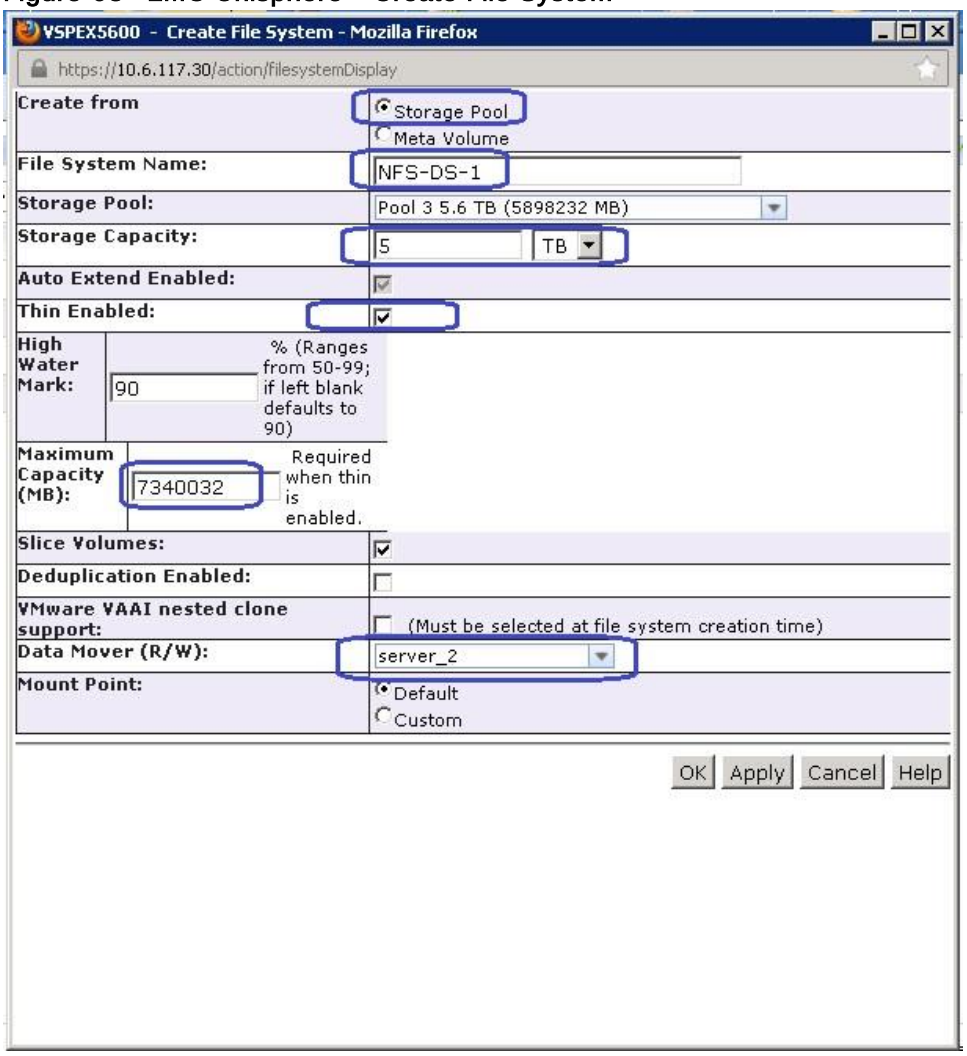
Figure 67 EMC Unisphere – Create Network Interface for NFS VLAN ID



## Create a File System for the NFS Datastore

1. Navigate to Storage > Storage Configuration and select File Systems and click Create.
2. From the Create File System window select Storage Pool.
3. Specify File System Name as <<var_mgmt_vnx_fs1_name>> for Virtual machine datastore.
4. Select Storage Pool from the drop-down list.
5. Specify Storage Capacity as <<var_mgmt_fs_size>>.
6. Check box Thin Enabled.
7. Use <<var_mgmt_fs_max_capa>> as Maximum Capacity (MB).
8. Select Data Mover as Server_2.
9. Click OK.

Figure 68 EMC Unisphere – Create File System



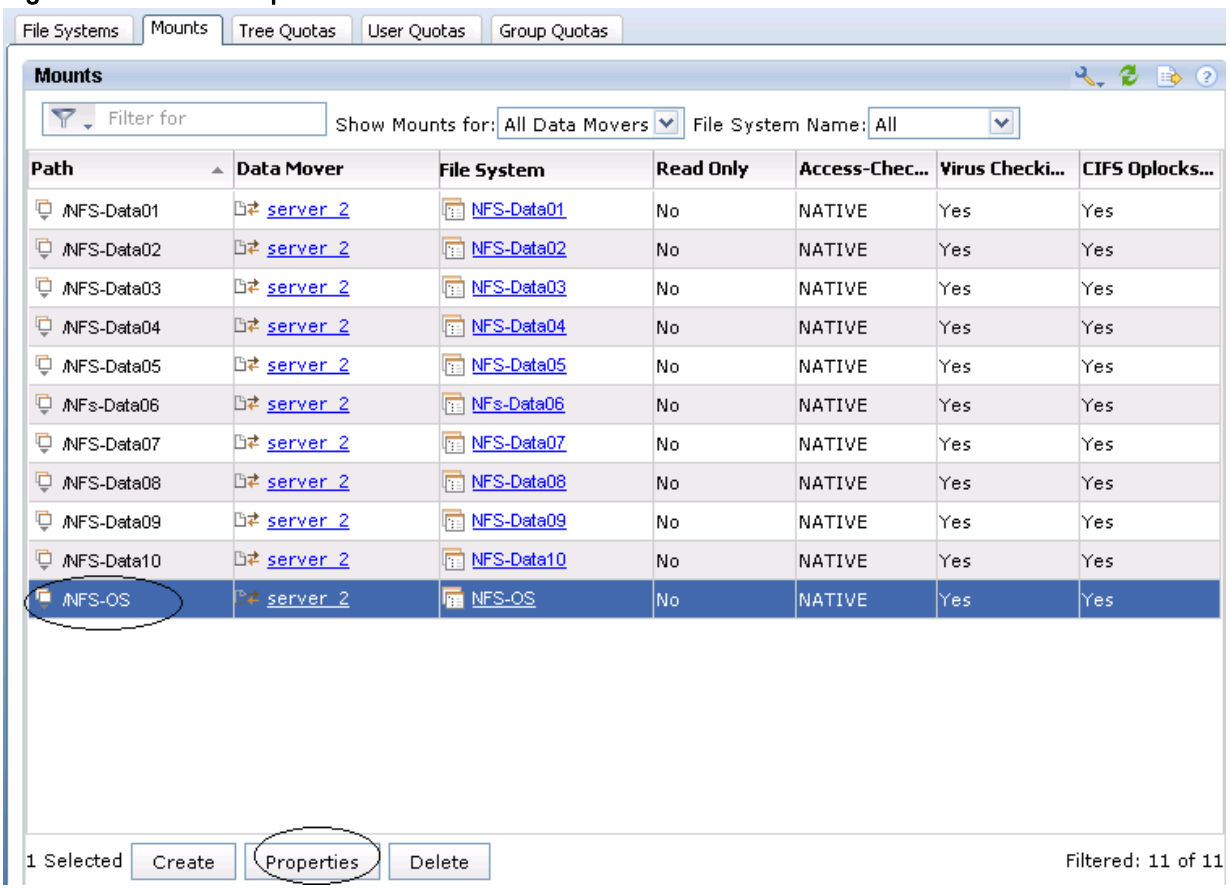

10. Wait until the File system creation process to complete. Verify the process using Background Tasks for File under System menu.

## Enable Direct Writes for All File Systems

1. Select Storage > Storage Configuration > File Systems > click the Mounts tab.

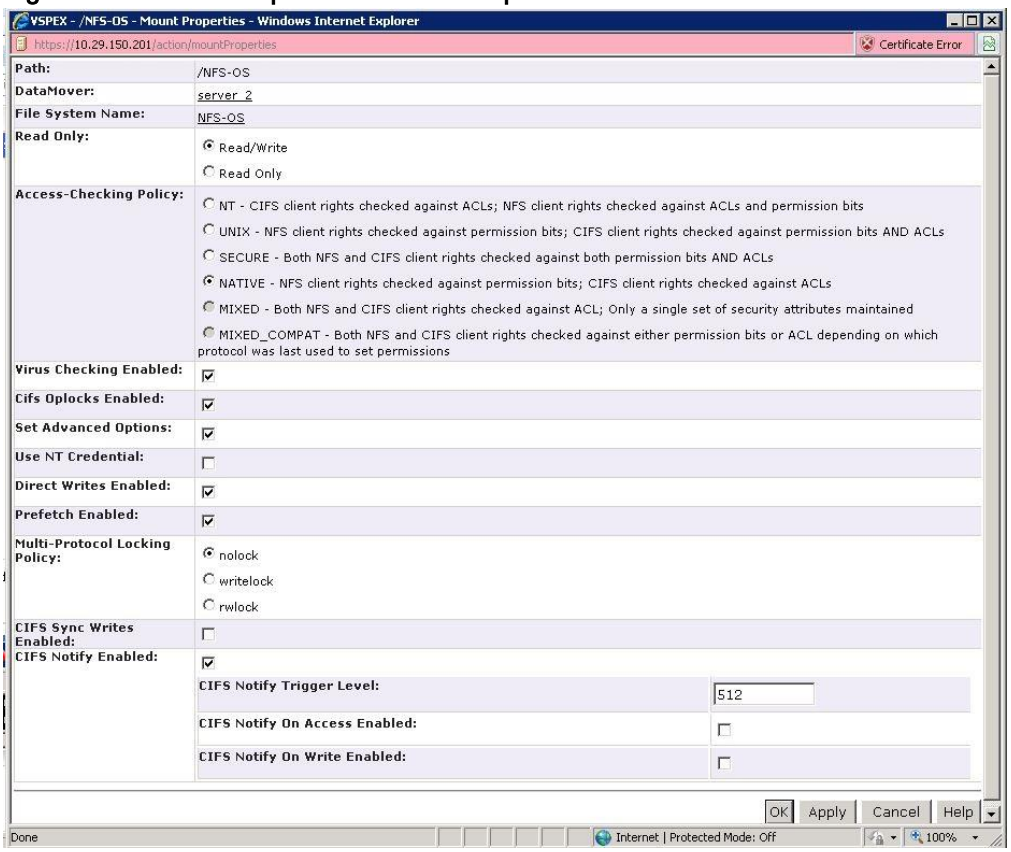
2. Select the path /NFS-DS-1 for the file system NFS-OS and click Properties.

Figure 69 EMC Unisphere – List of Mounts




3. From the /NFS-DS-1 mount properties. Make sure Read/Write & Native Access policy is selected.
4. Select the Set Advanced Options checkbox.
5. Check the Direct Writes Enabled checkbox.
6. Click OK.

Figure 70 EMC Unisphere – Mount Properties




## Create NFS-Export for the File Systems

1. Click Storage > Shared Folders > Select NFS and click Create.

Figure 71 EMC Unisphere – List of NFS shares




2. Select server-2 in Choose Data Mover drop-down list.

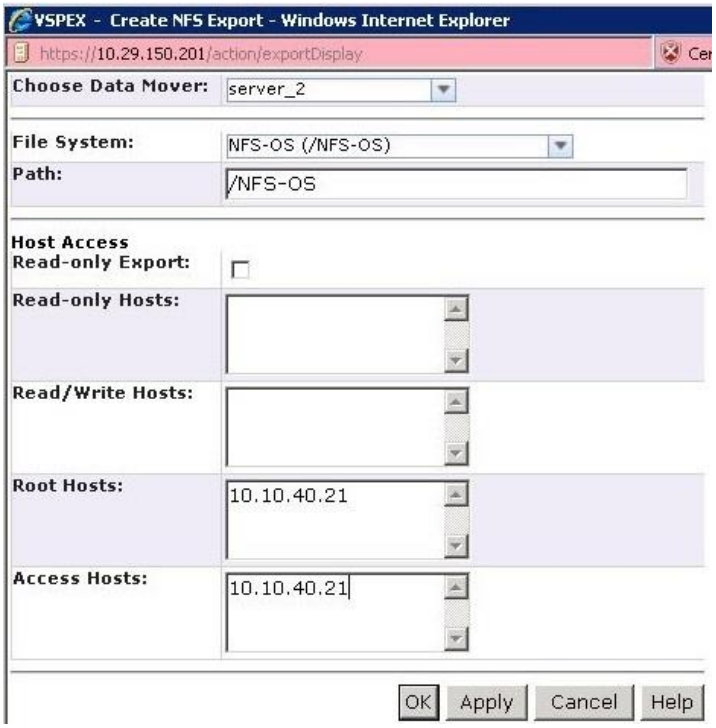
3. Select NFS-OS in File System drop-down.

4. Specify Path as /NFS-DS-1.

5. From the Root Hosts and Access Hosts field add the <<var_mgmt_esx1_nfs_ip>> and <<var_mgmt_esx2_nfs_ip>>. Separate multiple host IP's by : (colon)

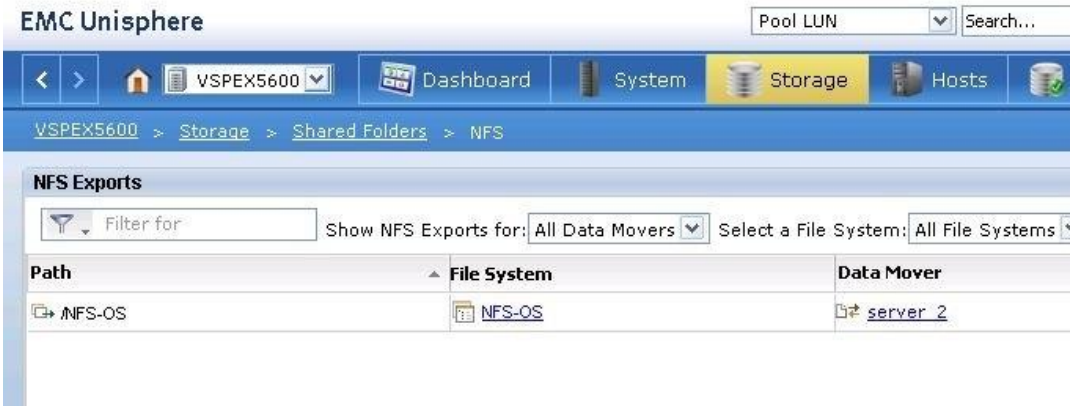
6. Click OK.

Figure 72 EMC Unisphere – Create NFS Export




The NFS Exports created for the NFS file system displays as shown below.

Figure 73 EMC Unisphere – List of NFS Exports




7. Repeat this step for all the NFS File Systems created on the storage array.

## VMware ESXi Installation

This section describes the installation and basic configuration of VMware ESXi 5.5. The process is as follows:

- Installation from ISO-Image
- Initial Configuration
- Setup Management Network via KVM
- ESX configuration with VMware vCenter Client software

Table 16 lists the information used for setting up the VMware ESXi Server in this Cisco UCS Integrated Infrastructure.

**Table 16 Information to Setup VMware ESXi in the Management POD**

| Name | Variable |
|---|---|
| Default Password | <<var_mgmt_passwd>> |
| IP Address for ESXi host 1 | <<var_mgmt_esx1_ip>>. |
| Netmask of the Management Network | <<var_mgmt_netmask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| DNS server 2 IP Address | <<var_nameserver2_ip>> |
| Full Qualified Domain name of ESX host 1 | <<var_mgmt_esx1_fqdn>> |
| IP Address for ESXi host 2 | <<var_mgmt_esx2_ip>>. |
| Full Qualified Domain name of ESX host 2 | <<var_mgmt_esx2_fqdn>> |
| VMkernel Management Network Name | <<var_vmkern_mgmt_name>> |
| Management Network Name for <<var_mgmt_vlan_id>> | <<var_esx_mgmt_network>> |
| Infrastructure Management Network VLAN ID | <<var_management_vlan_id>> |
| NFS Network Name for <<var_mgmt_esx_nfs_vlan_id>> | <<var_esx_vmkernel_nfs>> |
| VMware ESX Storage access Network VLAN ID within the Management POD | <<var_esx_nfs_vlan_id>> |
| VMkernel VMotion Network Name | <<var_vmotion_network>> |

| Name | Variable |
|---|---|
| VMware Vmotion Network VLAN ID within the Management POD | <<var_vmotion_vlan_id>> |
| Nexus1000V Control Network Name | <<var_esx_n1k_control_network>> |
| Cisco Nexus1000V Control Network VLAN ID | <<var_n1k_control_vlan_id>> |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| DataMover IP Address within the MGMT-ESX-NFS-Network | <<var_mgmt_vnx_dm2_ip>> |
| NFS Export Name for Datastore 1 | <<var_mgmt_nfs_volume_path>> |
| Name of the first Datastore on ESXi | <<var_vc_mgmt_datastore_1>> |

To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. From a Browser go to IP address Set for CIMC.
2. In the Navigation Pane Server → Summary.
3. Click  Launch KVM Console.
4. Open with Java JRE installed.
5. Click the Virtual Media Menu.
6. Click Activate Virtual Devices.
7. Click Accept this Session and check the box to Remember this configuration.´

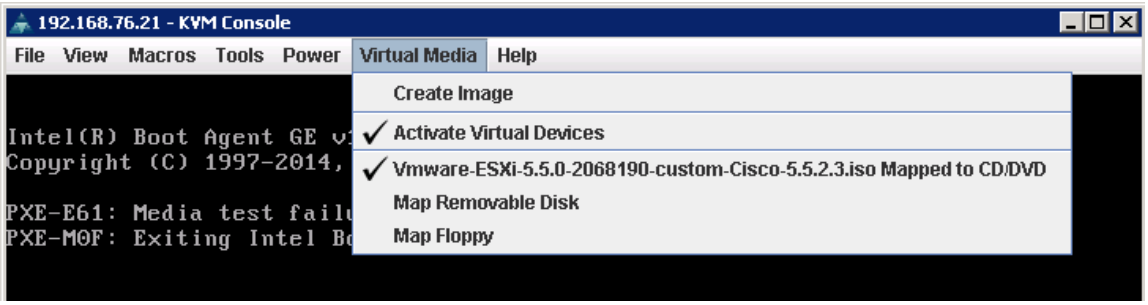
**Figure 74 Cisco CIMC – Allow Unencrypted Virtual Media Session**




8. Click Apply.
9. Click the Virtual Media Menu.
10. Click Map CD/DVD.

11. Browse to the ESXi installer ISO image file and click Open.
12. Download the latest ESXi-5.5.0-*-Custom-Cisco-5.5.*.iso from the VMware web site.
13. Click Map Device.

Figure 75 Cisco CIMC – Virtual Media Menu




14. Power On or PowerCycle the Server.
15. Use the KVM Window to monitor the server boot.
16. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
17. After the installer is finished loading, press Enter to continue with the installation.
18. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
19. Select the Local Disk which was previously created for ESXi and press Enter to continue with the installation.
20. Select the appropriate keyboard layout and press Enter.
21. Enter <<var_mgmt_passwd>> and confirm the root password and press Enter.
22. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
23. After the installation is complete, clear the Mapped checkbox (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.
24. The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.
25. The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Because the media cannot be ejected and it is read-only, simply click Yes to unmap the image.

26. From the KVM tab, press Enter to reboot the server.

## Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host.

### ESXi Host Mgmt-ESX1

To configure the Mgmt-ESX1 host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter <<var_mgmt_passwd>> as the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. From the Configure Management Network menu, select Network Adapters and press Enter.
5. Select the two devices that are connected and configured on the Nexus 9000s and press Enter.
6. Select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the first ESXi host: <<var_mgmt_esx1_ip>>.
9. Enter the subnet mask <<var_mgmt_netmask>> for this ESXi host.
10. Enter the default gateway <<var_mgmt_gw>> for this ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.



Because the IP address is assigned manually, the DNS information must also be entered manually.

15. Enter the IP address of the primary <<var_nameserver_ip>> DNS server.
16. Optional: Enter the IP address of the secondary <<var_nameserver2_ip>> DNS server.
17. Enter the fully qualified domain name (FQDN) <<var_mgmt_esx1_fqdn>> for this ESXi host.
18. Press Enter to accept the changes to the DNS configuration.

19. Press Esc to exit the Configure Management Network submenu.
20. Press Y to confirm the changes and return to the main menu.
21. Select Test Management Network to verify that the management network is set up correctly and press Enter.
22. Press Enter to run the test.  Confirm results of ping.
23. Press Enter to exit the window.
24. Press Esc to log out of the VMware console.

### ESXi Host Mgmt-ESX2

To configure the Mgmt-ESX2 ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter <<var_mgmt_passwd>> as the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. From the Configure Management Network menu, select Network Adapters and press Enter.
5. Select the two devices that are connected and configured on the Nexus 9000s and press Enter.
6. Select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the second ESXi host: <<var_mgmt_esx2_ip>>.
9. Enter the subnet mask <<var_mgmt_netmask>> for this ESXi host.
10. Enter the default gateway <<var_mgmt_gw>> for this ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.



Because the IP address is assigned manually, the DNS information must also be entered manually.

15. Enter the IP address of the primary <<var_nameserver_ip>> DNS server.
16. Optional: Enter the IP address of the secondary <<var_nameserver2_ip>> DNS server.
17. Enter the FQDN for the second <<var_mgmt_esx2_fqdn>> for this ESXi host.
18. Press Enter to accept the changes to the DNS configuration.
19. Press Esc to exit the Configure Management Network submenu.
20. Press Y to confirm the changes and return to the main menu.
21. Select Test Management Network to verify that the management network is set up correctly and press Enter.
22. Press Enter to run the test.
23. Press Enter to exit the window.
24. Press Esc to log out of the VMware console.

## VMware ESXi Configuration with VMware vCenter Client

If the VMware vCenter Server is deployed as a virtual machine on an ESXi server installed as part of this solution, connect directly to an Infrastructure ESXi server using the vSphere Client.

1. Open a web browser on the management workstation and navigate to the <<var_mgmt_esx1_ip>> management IP address.
2. Download and install the vSphere Client.



This application is downloaded from the VMware website and Internet access is required on the management workstation.

### ESXi Host Mgmt-ESX1

3. Open the recently downloaded VMware vSphere Client and enter the IP address of the host Mgmt-ESX1 as the host you are trying to connect to: <<var_mgmt_esx1_ip>>.
4. Enter root for the user name.
5. Enter the <<var_mgmt_passwd>> password.
6. Click Login to connect.
7. Select the host in the inventory.
8. Click the Configuration tab.

9. Click Networking in the Hardware pane.
10. Click Properties on the right side of vSwitch0.
11. Select the Network Adapters Tab and click Add.
12. Select the second LOM or VIC port and click Next
13. Take care that both adapters are listed as Active Adapters and click Next.
14. Review the summary and click Finish.
15. Select the vSwitch configuration and click Edit.
16. From the General tab, change the MTU size to 9000.
17. Click OK to close the properties for vSwitch0.
18. Select the Management Network configuration and click Edit.
19. Change the network label to <<var_vmkern_mgmt_name>> and select the Management Traffic checkbox.
20. If required change the MTU to 1500.
21. Click OK to finalize the edits for Management Network.
22. Select the VM Network configuration and click Edit.
23. Change the network label to <<var_esx_mgmt_network>> and enter <<var_management_vlan_id>> in the VLAN ID (Optional) field.
24. Click OK to finalize the edits for VM Network.
25. Click Add.
26. Select VMkernel and click Next.
27. For Network Label enter <<var_esx_vmkernel_nfs>>.
28. Enter VLAN ID for ESX NFS Network <<var_esx_nfs_vlan_id>>.
29. Click Next.
30. Enter <<var_mgmt_esx1_nfs_ip>> as the IP address and <<var_mgmt_netmask>> as the Netmask.
31. Click Next.

32. Click Finish.
33. Click Add.
34. Select VMkernel and click Next.
35. For Network Label enter <<var_vmotion_network>>.
36. Enter VLAN ID for ESX vMotion Network <<var_vmotion_vlan_id>>.
37. Select the Check-Box Use this port group for vMotion.
38. Click Next.
39. Enter <<var_mgmt_esx1_vmotion_ip>> as the IP address and <<var_mgmt_netmask>> as the Net-mask.
40. Click Next.
41. Click Finish.
42. Click Add.
43. Select Virtual Machine and click Next.
44. For Network Label enter <<var_esx_n1k_control_network>>.
45. Enter VLAN ID for Nexus 1000v Control Network <<var_n1k_control_vlan_id>>.
46. Click Next.
47. Click Finish.
48. Click Close to finish the vSwitch configuration.
49. Click Time Configuration in the Software pane.
50. Click Properties at the upper right side of the window.
51. At the bottom of the Time Configuration dialog box, click Options.
52. In the NTP Daemon Options dialog box, complete the following steps:
    a. Click General in the left pane and select Start and stop with host.
    b. Click NTP Settings in the left pane and click Add.
    c. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of the NTP server and click OK.

d. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes check-box and click OK.

53. In the Time Configuration dialog box, complete the following steps:

    a. Select the NTP Client Enabled checkbox and click OK.

    b. Verify that the clock is now set to approximately the correct time.



The NTP server time may vary slightly from the host time.

### ESXi Host Mgmt-ESX2

54. Open the recently downloaded VMware vSphere Client and enter the IP address of ESXi-Mgmt-02 as the host you are trying to connect to: <<var_mgmt_esx2_ip>>.

55. Enter root for the user name.

56. Enter the <<var_mgmt_passwd>> password.

57. Click Login to connect.

58. Select the host in the inventory.

59. Click the Configuration tab.

60. Click Networking in the Hardware pane.

61. Click Properties on the right side of vSwitch0.

62. Select the Network Adapters Tab and click Add.

63. Select the second LOM or VIC port and click Next.

64. Take care that both adapters are listed as Active Adapters and click Next.

65. Review the summary and click Finish.

66. Select the vSwitch configuration and click Edit.

67. From the General tab, change the MTU size to 9000.

68. Click OK to close the properties for vSwitch0.

69. Select the Management Network configuration and click Edit.

70. Change the network label to <<var_vmkern_mgmt_name>> and select the Management Traffic checkbox.

71. If required change the MTU to 1500.
72. Click OK to finalize the edits for Management Network.
73. Select the VM Network configuration and click Edit.
74. Change the network label to <<var_esx_mgmt_network>> and enter <<var_management_vlan_id>> in the VLAN ID (Optional) field.
75. Click OK to finalize the edits for VM Network.
76. Click Add.
77. Select VMkernel and click Next.
78. For Network Label enter <<var_esx_vmkernel_nfs>>.
79. Enter VLAN ID for ESX NFS Network <<var_esx_nfs_vlan_id>>.
80. Click Next.
81. Enter <<var_mgmt_esx2_nfs_ip>> as the IP address and <<var_mgmt_netmask>> as the Netmask.
82. Click Next.
83. Click Finish.
84. Click Add.
85. Select VMkernel and click Next.
86. For Network Label enter <<var_vmotion_network>>.
87. Enter VLAN ID for ESX vMotion Network <<var_vmotion_vlan_id>>.
88. Select the Check-Box Use this port group for vMotion.
89. Click Next.
90. Enter <<var_mgmt_esx2_vmotion_ip>> as the IP address and <<var_mgmt_netmask>> as the Net-mask.
91. Click Next.
92. Click Finish.
93. Click Add.

94. Select Virtual Machine and click Next.
95. For Network Label enter <<var_esx_n1k_control_network>>.
96. Enter VLAN ID for Nexus 1000v Control Network <<var_n1k_control_vlan_id>>.
97. Click Next.
98. Click Finish.
99. Click Close to finish the vSwitch configuration.
100. Click Time Configuration in the Software pane.
101. Click Properties at the upper right side of the window.
102. At the bottom of the Time Configuration dialog box, click Options.
103. In the NTP Daemon Options dialog box, complete the following steps:
    a. Click General in the left pane and select Start and stop with host.
    b. Click NTP Settings in the left pane and click Add.
    c. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of the NTP server and click OK.
    d. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes check-box and click OK.
104. In the Time Configuration dialog box, complete the following steps:
    a. Select the NTP Client Enabled checkbox and click OK.
    b. Verify that the clock is now set to approximately the correct time.



The NTP server time may vary slightly from the host time.

## Mount the Datastore

For this solution, use a NFS share from a storage connected to the Management Pod as the datastore to store the virtual machines.

### ESXi Hosts Mgmt-ESX1 and Mgmt-ESX2

1. From vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Storage in the Hardware pane.

4. From the Datastore area, click Add Storage to open the Add Storage wizard.
5. Select Network File System and click Next.
6. Enter the IP address for <<var_mgmt_vnx_dm2_ip>> as Server.
7. Enter Volume path <<var_mgmt_nfs_volume_path>> for the NFS export.
8. Make sure that the Mount NFS read only checkbox is NOT selected.
9. Enter <<var_mgmt_datastore_1>> as the datastore name.
10. Click Next to continue with the NFS datastore creation.
11. Click Finish to finalize the creation of the NFS datastore.

## VMware Management Tool deployment

This section describes the installation of VMware vCenter Server.

For detailed information about installing a vCenter Server, click:

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

Table 17 list the information used for setting up the VMware vCenter Server in this Cisco UCS Integrated Infrastructure.

**Table 17 Information to Setup VMware vCenter Server**

| Name | Variable |
|---|---|
| Global default administrative password | <<var_mgmt_passwd>> |
| Name of the first Datastore on ESXi | <<var_mgmt_datastore_1>> |
| Virtual Center Server IP address | <<var_vc_ip_addr>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Virtual Center Server Hostname | <<var_vc_hostname>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| Name of the first DataCenter in Virtual Center | <<var_vc_datacenter_name>> |
| Name of the Host Cluster for the Management Hosts | <<var_vc_mgmt_cluster_name>> |
| Name of the first Host Cluster for the managed system | <<var_vc_cluster1_name>> |

| Name | Variable |
|---|---|
| Full Qualified Domain name of ESX host 1 | <<var_mgmt_esx1_fqdn>> |
| Full Qualified Domain name of ESX host 2 | <<var_mgmt_esx2_fqdn>> |

The following section provide the high-level configuration steps to configure the vCenter server.



Based on your requirements, you will have to choose between the VMware vCenter Server 5.5 running on a Windows System, or VMware vCenter Server 5.5 appliance delivered as OVA from VMware. For this Cisco UCS Integrated Infrastructure CVD, the VMware vCenter Server Appliance is used.

## Deploy the VMware vCenter Server Appliance

The VMware vCenter Server appliance OVA file can be downloaded from the VMware web site. To deploy the VMware vCenter Server Appliance, complete the following steps:

1. Open the recently downloaded VMware vSphere Client and enter the IP address of Mgmt-ESX1 as the host you are trying to connect to: <<var_mgmt_esx1_ip>>.
2. Enter root for the user name.
3. Enter the <<var_mgmt_passwd>> password.
4. Click Login to connect.
5. Click File and select Deploy OVF Template.
6. Click Browse ... and select the recently downloaded VMware vCenter Server appliance file.
7. Click Open to close the Window.
8. On the Source page Click Next.
9. On the OVF Template Details page check the information and click Next.
10. Enter a valid name for the virtual Machine in the Name field and click Next.
11. Select <<var_mgmt_datastore_1>> as the destination storage for the virtual machine files and click Next.
12. On the Disk Format page select Thick Provisioning Lazy Zeroed and click Next.
13. For Network 1 select Management Network as the Destination Network and click Next.
14. Check the summary information and click Finish.

The virtual machine is created.

15. Select the new virtual machine in the inventory and launch the virtual machine console.
16. Power on the virtual machine.
17. Move the cursor to Login and press Enter.
18. Login with the user root and the password vmware.
19. On the command line enter YaSZT network and press Enter.
20. Select Network Card and press Enter.
21. Move the cursor to Edit and press Enter.
22. Move the cursor to ( ) Statically assigned IP Address and press Enter and then Tab.
23. In the IP Address Section insert <<var_vc_ip_addr>> and press Tab.
24. In the Subnet Mask field insert <<var_mgmt_netmask>> and press Tab.
25. In the Hostname field insert <<var_vc_hostname>>.
26. Move the cursor to Next and press Enter.
27. Check the information in the Network Settings page.
28. Move the cursor to Routing.
29. In the Default Gateway section insert <<var_mgmt_gw>>.
30. Move the cursor to OK and press Enter.
31. On the command line enter logout and press Enter.
32. Make sure you can ping <<var_vc_ip_addr>> from a system on the network.

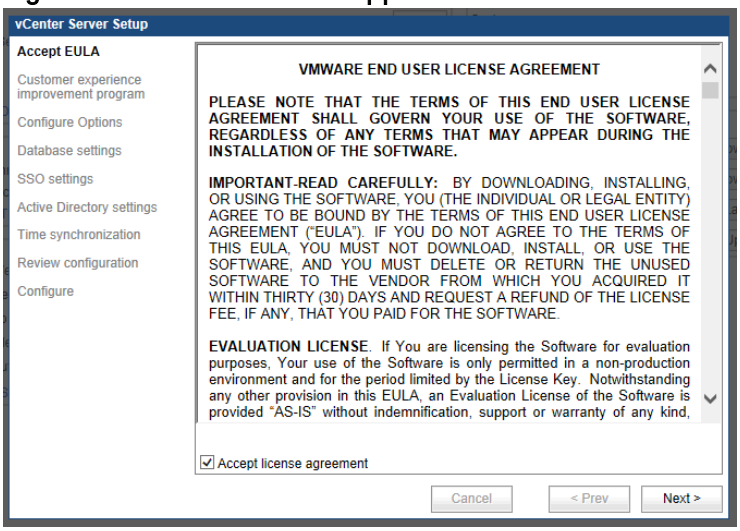
## Configure VMware vCenter Server Appliance

The VMware vCenter server appliance is deployed and can be reached from the network. To configure the VMware vCenter Server Appliance, complete the following steps:

1. Open a Web browser and navigate to https://<<var_vc_ip_addr>>:5480/ .
2. Log in with the user root and the password vmware.
3. Click the checkbox to Accept License Agreement.

4. Click Next.

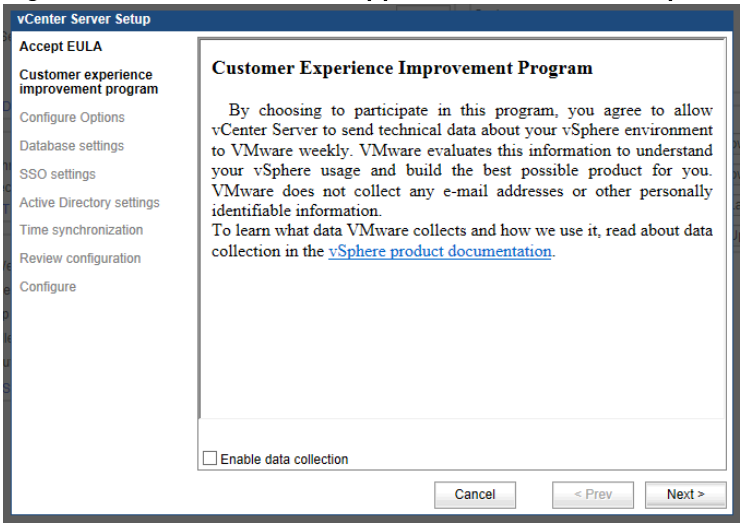
Figure 76 vCenter Server Appliance - EULA




5. Make your selection for the Customer Experience Improvement Program.

6. Click Next.

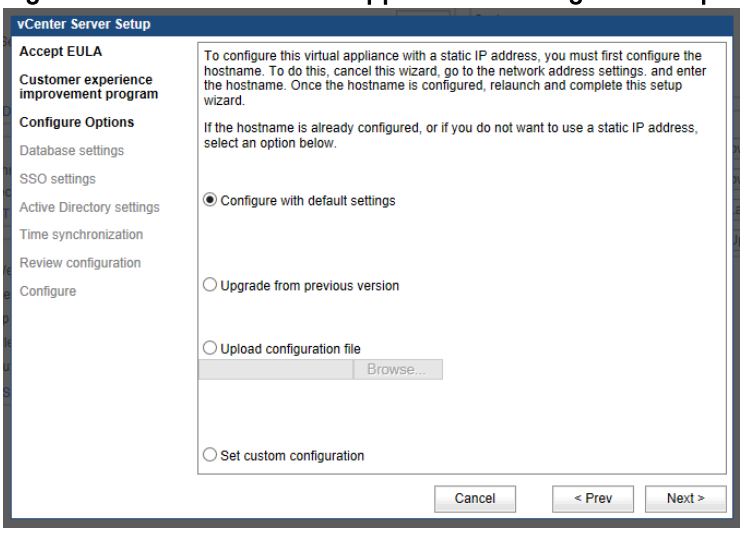
Figure 77 vCenter Server Appliance - Customer Experience Improvement Program




7. Select Configure with default settings.

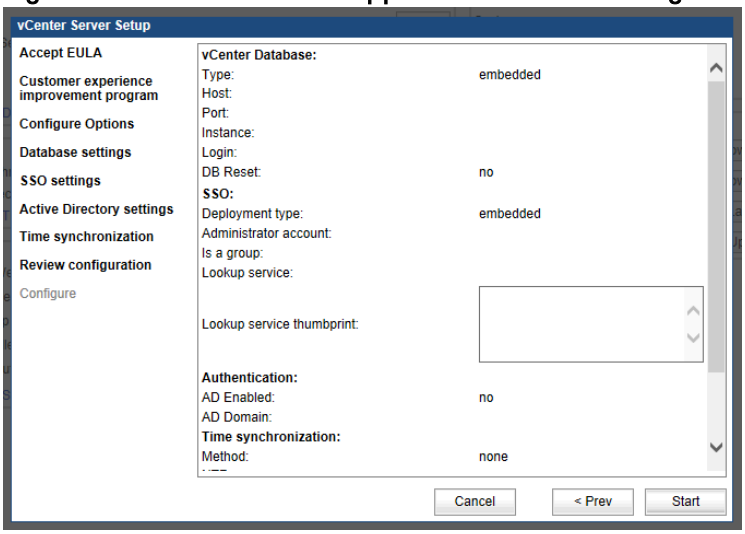
8. Click Next.

Figure 78 vCenter Server Appliance – Configuration Option




9. Click Start.

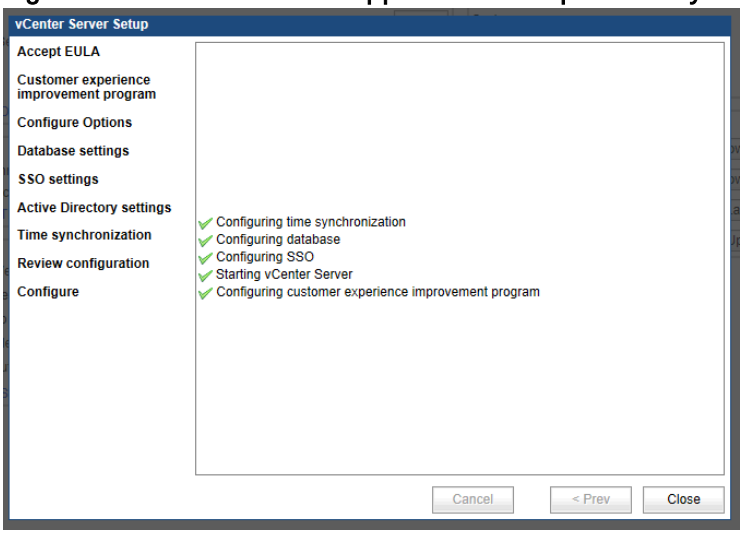
Figure 79 vCenter Server Appliance – Review Configuration




The System is configuring the services.

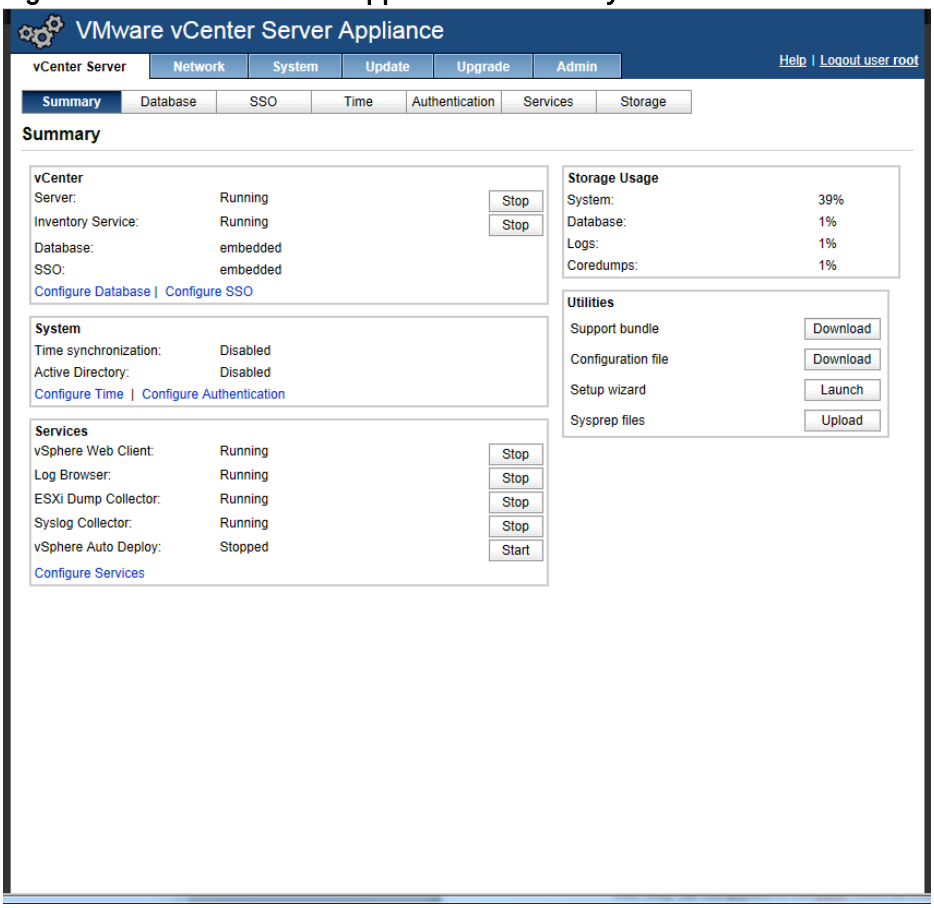
10. Click Close.

Figure 80 vCenter Server Appliance – Setup Summary




The Summary screen displays the status of all VMware vCenter Services managed by this system.

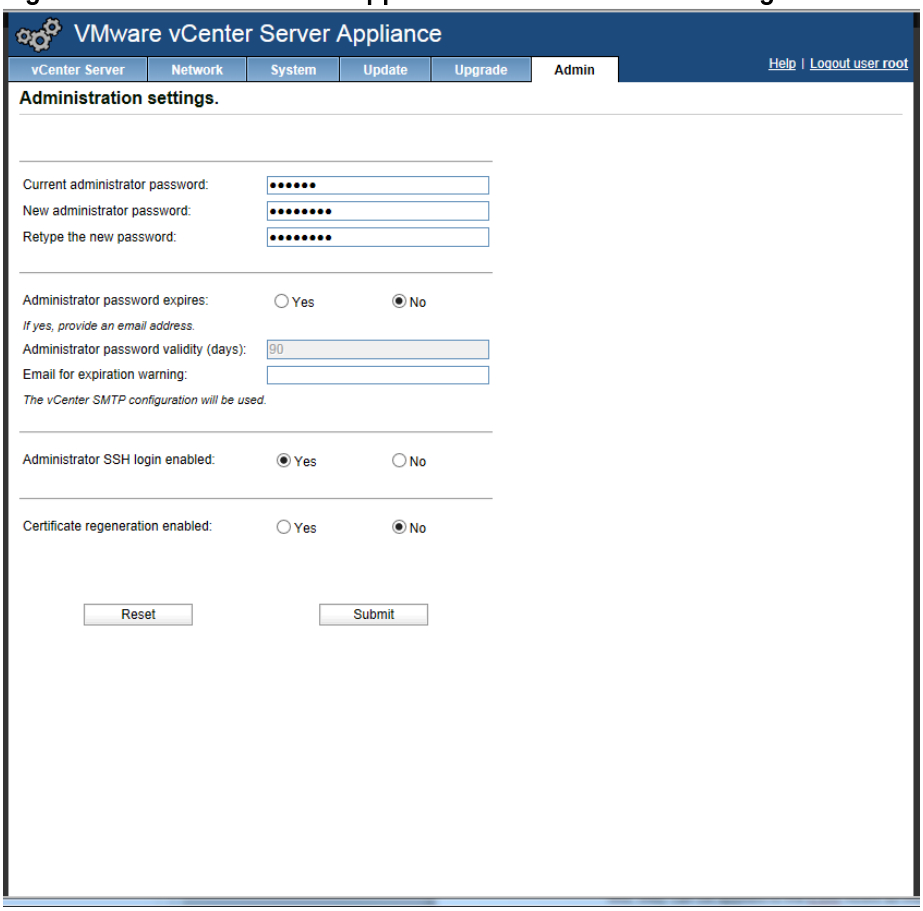
Figure 81 vCenter Server Appliance – Summary screen




11. Click the Admin Tab.

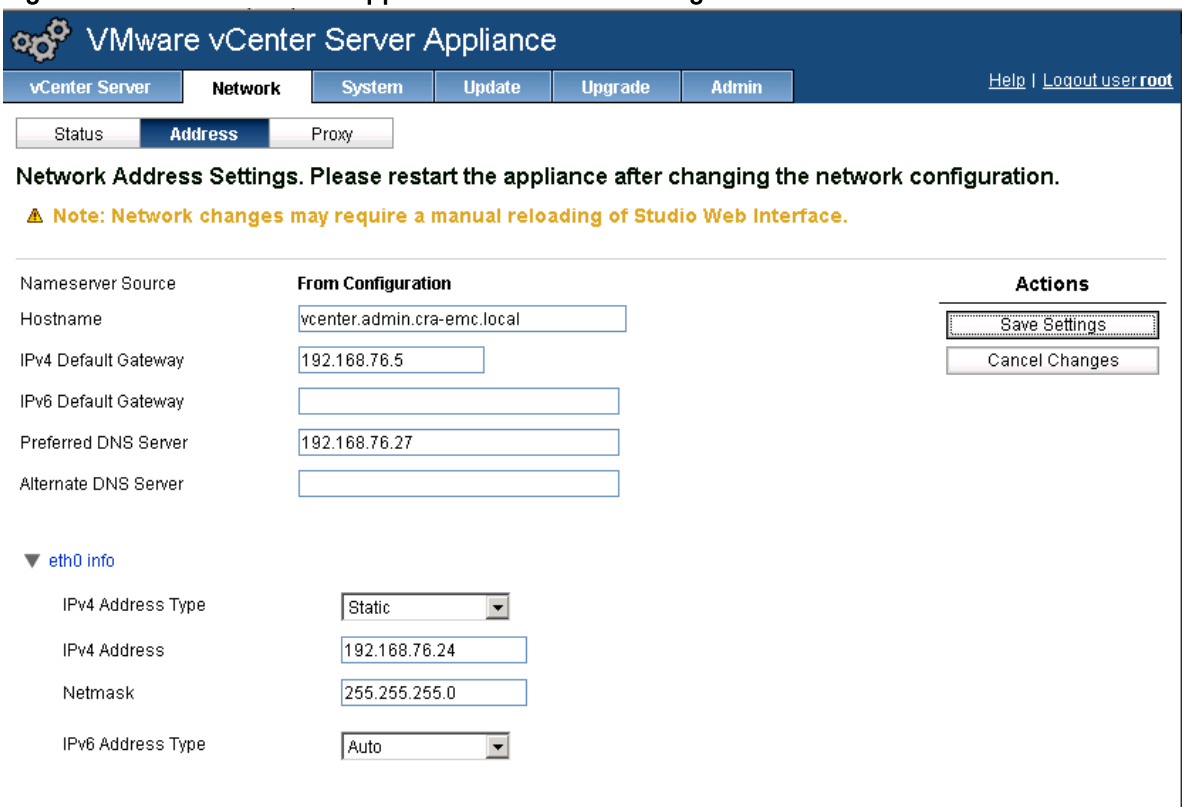
12. Enter vmware as the current administrator password.
13. Enter <<var_mgmt_passwd>> as the New administrator password and in the Retype field.
14. Select No in the Administrator password expires section.
15. Click Submit.

Figure 82 vCenter Server Appliance – Administration settings



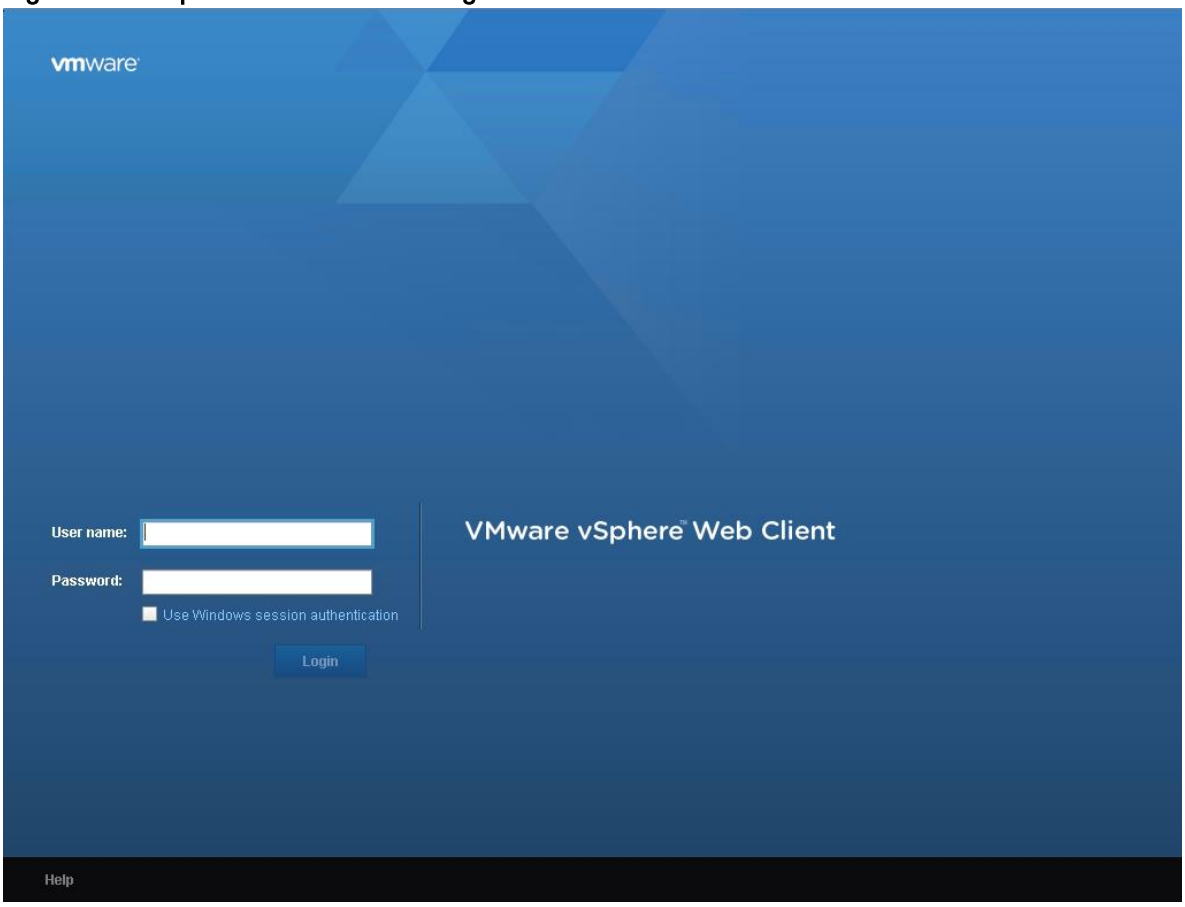

16. Click the Network Tab.
17. Click Address.
18. Enter <<var_vc_hostname>> as the Hostname of this vCenter Server.
19. Click Save Settings.

Figure 83 vCenter Server Appliance – Network Settings



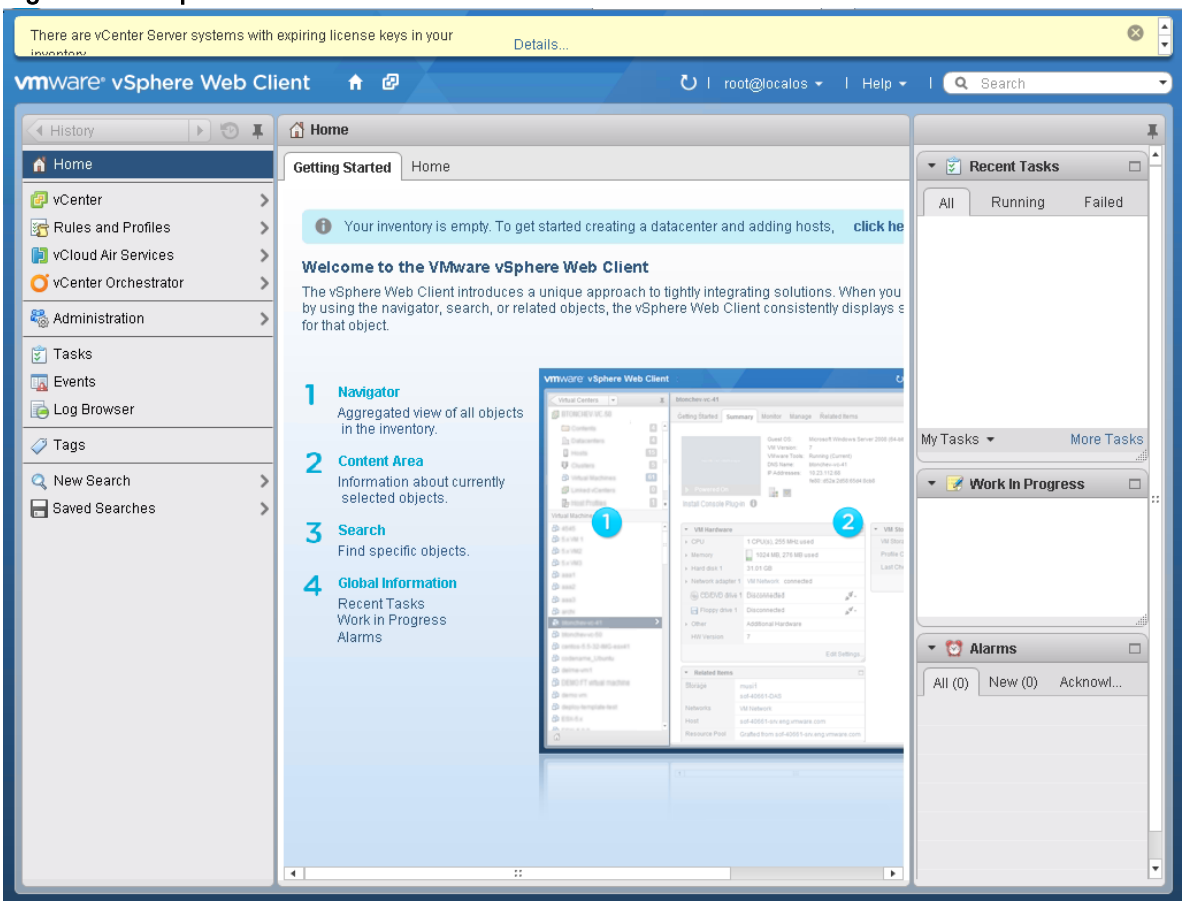

20. Open a new web browser and go to https://<<var_vc_ip_addr>>:9443/ to open the VMware vSphere Web Client.

Figure 84 vSphere Web Client – Logon Screen




21. If the VMware Remote Console Plug-In displays, select Allow.
22. Enter root as the User name.
23. Enter <<var_mgmt_passwd>> as the Password .
24. Click Login.

**Figure 85 vSphere Web Client – Home Screen**




25. When the login process is successful, close the web browser with the configuration page https://<<var_vc_ip_addr>>:5480>>/.

## Apply vSphere License Keys

To perform license maintenance, log into the vSphere Web Client and complete the following steps:

1. Click Administration.
2. Click Licenses.
3. Click the +-Sign to add a License key.
4. Enter the license keys.
5. Click Next.
6. Check the License Key is valid.
7. Click Finish.

8. Click the vCenter Server Systems tab.
9. Click <<var_vc_hostname>>.
10. Click Assign License Key.
11. Select the new License Key for this vCenter Server.
12. On the Top Left side click Home.

## Configure vCenter

To perform the configuration, log into the vSphere Web Client, and complete the following steps:

Define a new Datacenter and a new Cluster

1. Click vCenter.
2. Click Datacenters.
3. In the Objects pane click the +-Sign.
4. Enter <<var_vc_datacenter_name>> as the Datacenter name.
5. Select <<var_vc_hostname>> as the vCenter Server system.
6. Click OK.
7. Right-click <<var_vc_datacenter_name>>.
8. Select New Cluster.
9. Enter <<var_vc_mgmt_cluster_name>>.
10. Enable and configure all features you require (none were used in this CVD).
11. Click OK.
12. Right-click <<var_vc_datacenter_name>>.
13. Select New Cluster.
14. Enter <<var_vc_cluster1_name>>.
15. Enable and configure all features you require (none were used in this CVD).
16. Click OK.
17. Click the Home sign to go back to the Home screen.

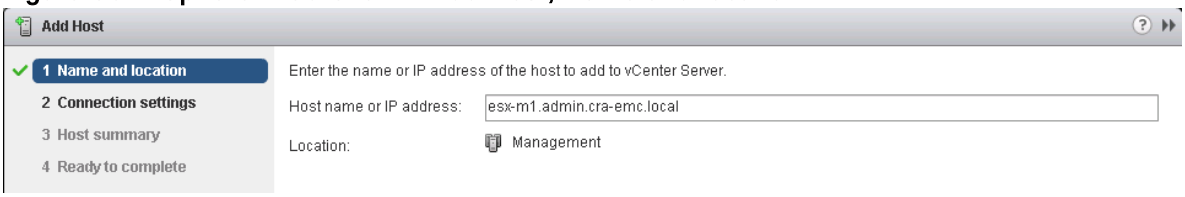
## Add ESX hosts M1 and M2 to vCenter

The ESX servers in the management POD are added into the vCenter, using a production environment. Use a vCenter that is not deployed as a VM on one of the managed nodes.

To add the ESX hosts, log into the vSphere Web Client and complete the following steps:

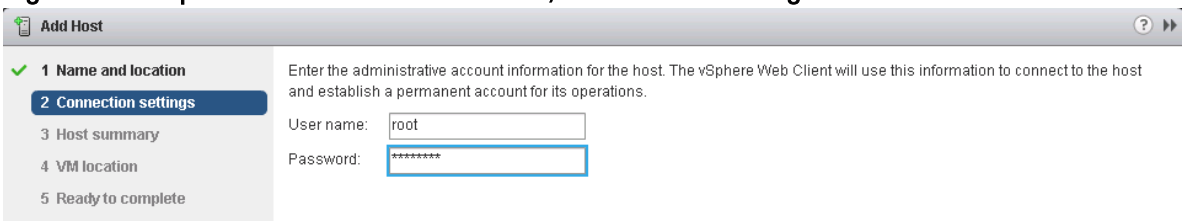
1. Click Hosts and Clusters in the Home Screen.
2. Click the Arrow left of <<var_vc_dc_name>> on the left pane.
3. Right-click <<var_vc_mgmt_cluster_name>>.
4. Select Add Host.
5. Enter <<var_mgmt_esx1_fqdn>> in the Hostname or IP Address field.

**Figure 86 vSphere Web Client – Add Host, Name and location**



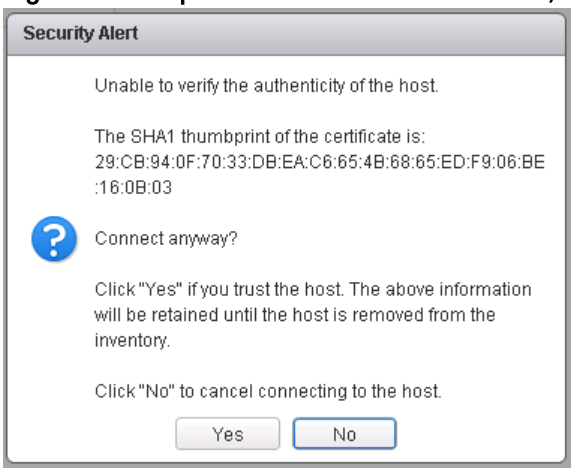

6. Click Next.
7. Enter root as the User name and <<var_mgmt_passwd>> as the Password.

**Figure 87 vSphere Web Client – Add Host, Connection settings**



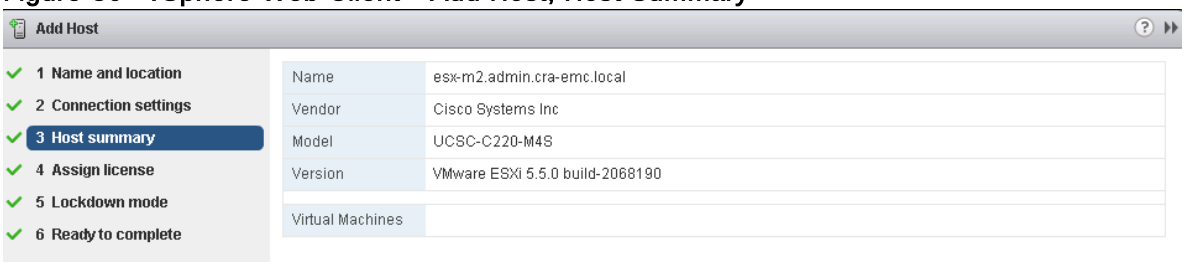

8. Click Next.
9. Click Yes to Accept the Certificate.

**Figure 88 vSphere Web Client – Add Host, Accept Security Alert**




10. Review the Host Summary and click Next.

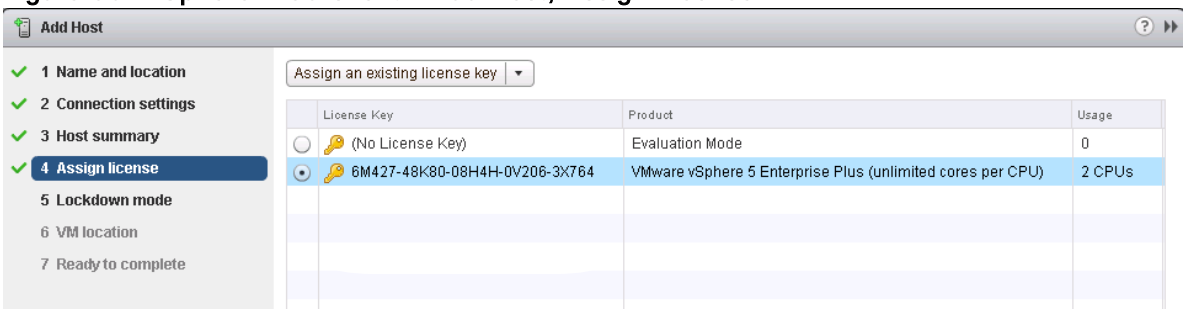
**Figure 89 vSphere Web Client – Add Host, Host Summary**




11. Select a License Key to be used by this host.

12. Click Next.

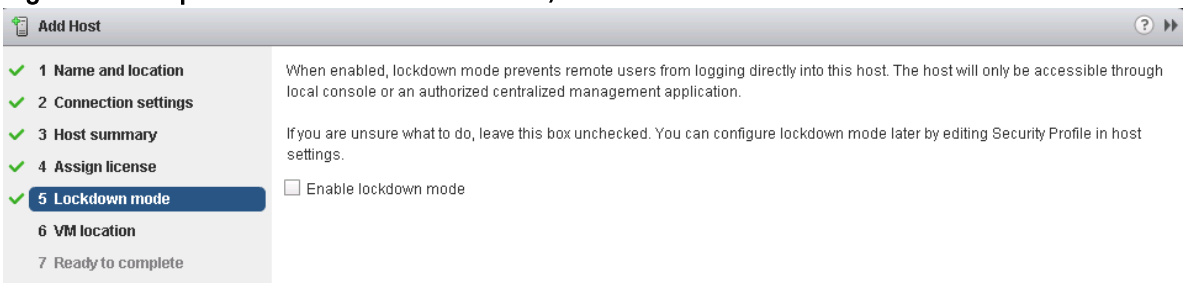
**Figure 90 vSphere Web Client – Add Host, Assign License**




13. Leave the checkbox for Lockdown Mode unchecked.

14. Click Next.

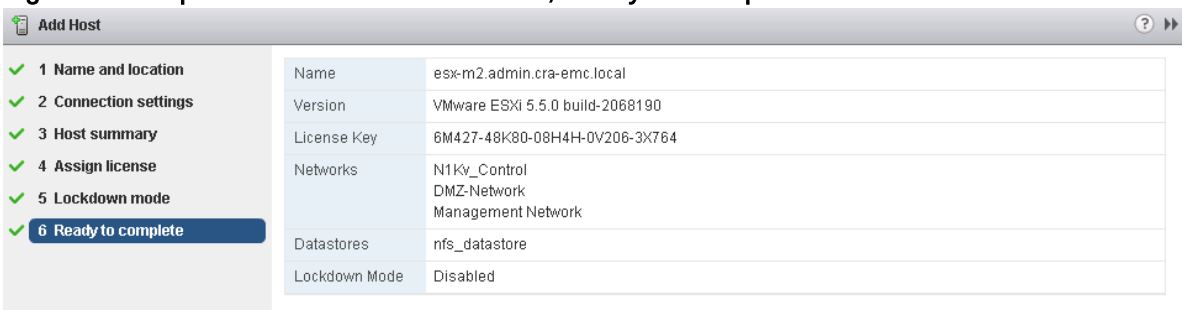
**Figure 91 vSphere Web Client – Add Host, Lockdown Mode**




15. On the VM Location Screen click Next.

16. Review the Information and click Finish.

**Figure 92 vSphere Web Client – Add Host, Ready to Complete**




17. Repeat this step with the second ESX host <<var_mgmt_esx2_fqdn>>.

## Install and Configure the Cisco Nexus1000V Virtual Switch Update Manager and Virtual Supervisor Module

This section details how to setup the Cisco Nexus1000V Virtual Switch Update Manager (VSUM) and the Virtual Supervisor Module (VSM).

The Cisco Virtual Switch Update Manager OVF is available on cisco.com for download.

Table 18 lists the information used to setup the Cisco Nexus1000V in this Cisco UCS Integrated Infrastructure.

**Table 18 Information to Setup Cisco Nexus1000V**

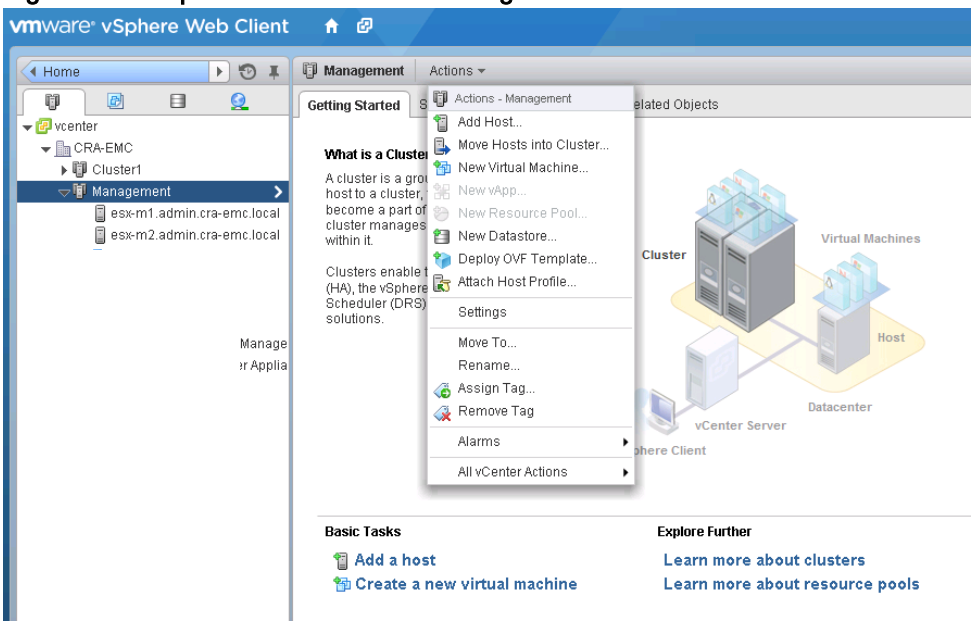
| Name | Variable |
|---|---|
| Name of the Host Cluster for the Management Hosts | <<var_vc_mgmt_cluster_name>> |
| Name of the first DataCenter in Virtual Center | <<var_vc_datacenter_name>> |
| Name of the first Datastore on ESXi | <<var_vc_mgmt_datastore1>> |
| Cisco Virtual Switch Update Manager IP Address | <<var_n1k_vsum_ip>> |

| Name | Variable |
|---|---|
| Management network default Gateway | <<var_mgmt_gw>> |
| Virtual Center Server IP address | <<var_vc_ip_addr>> |
| Global default administrative password | <<var_mgmt_passwd>> |
| Name of the first DataCenter in Virtual Center | <<var_vc_dc_name>> |
| Management Network Name for <<var_mgmt_vlan_id>> | <<var_esx_mgmt_network>> |
| Nexus1000V Switch Domain ID | <<var_n1k_domain_id>> |
| Nexus1000V Virtual Switch Name | <<var_n1k_switch_name>> |
| Nexus1000V Virtual Switch Supervisor Modul IP Address | <<var_n1k_vsm_ip>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Nexus1000V Admin User Password | <<var_n1k_passwd>> |

To deploy and configure Cisco Nexus1000V, complete the following steps::

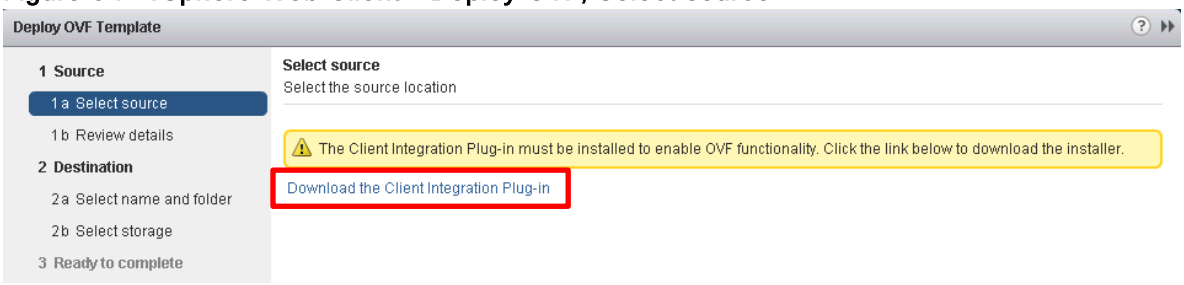
1. Log in to the vSphere Web Client.
2. Click Hosts and Clusters in the Home Screen.
3. Click the <<var_vc_mgmt_cluster_name>>.
4. Click Actions and select Deploy OVF Template.

**Figure 93 vSphere Web Client – Management Cluster Action Menu**



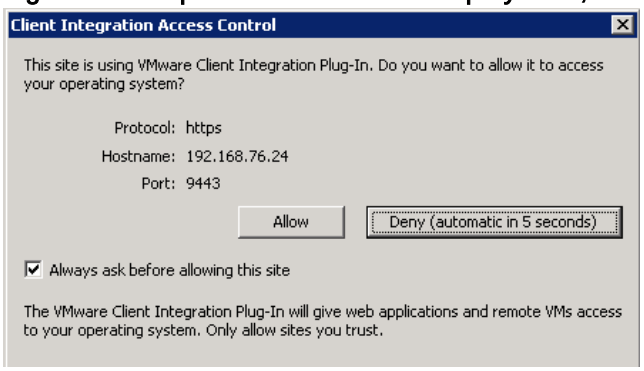

For the next steps, the Client Integration Plug-In is required. If displayed, click Download the Client integration Plug-In and follow the installation steps. A restart of the web browser is required. Repeat the step 1-4 after installing the Plug-In.

**Figure 94 vSphere Web Client – Deploy OVF, Select source**



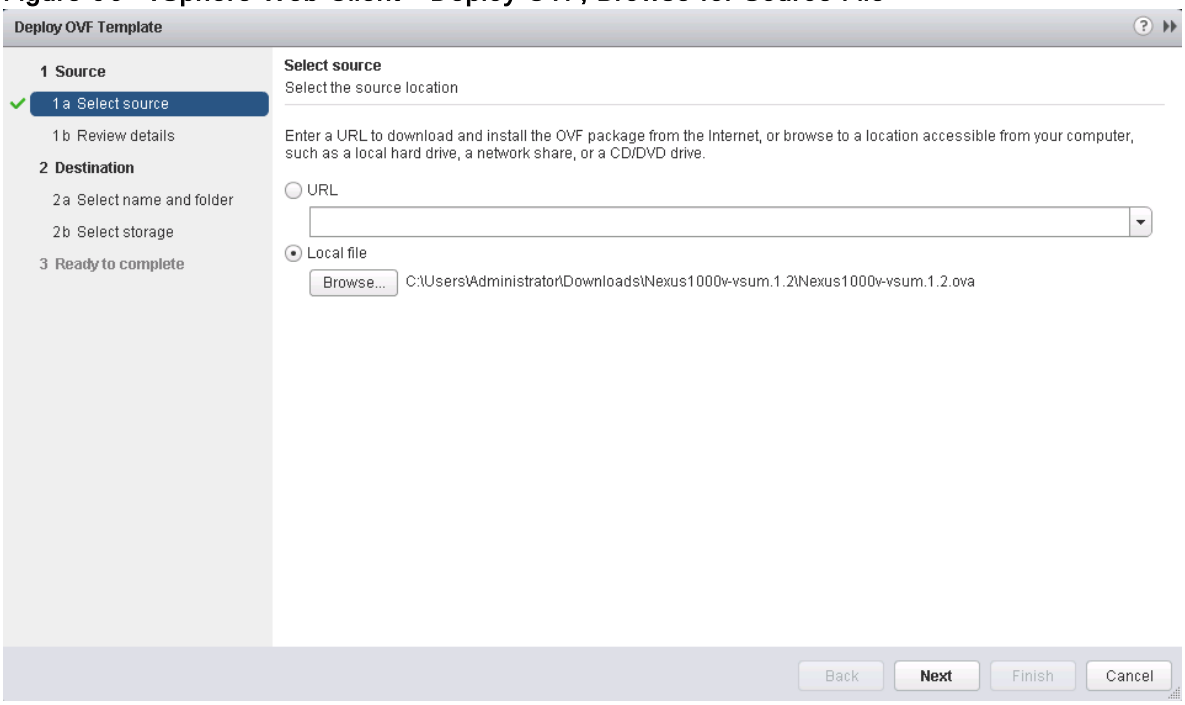

5. Click Allow.

**Figure 95 vSphere Web Client – Deploy OVF, Allow Access**



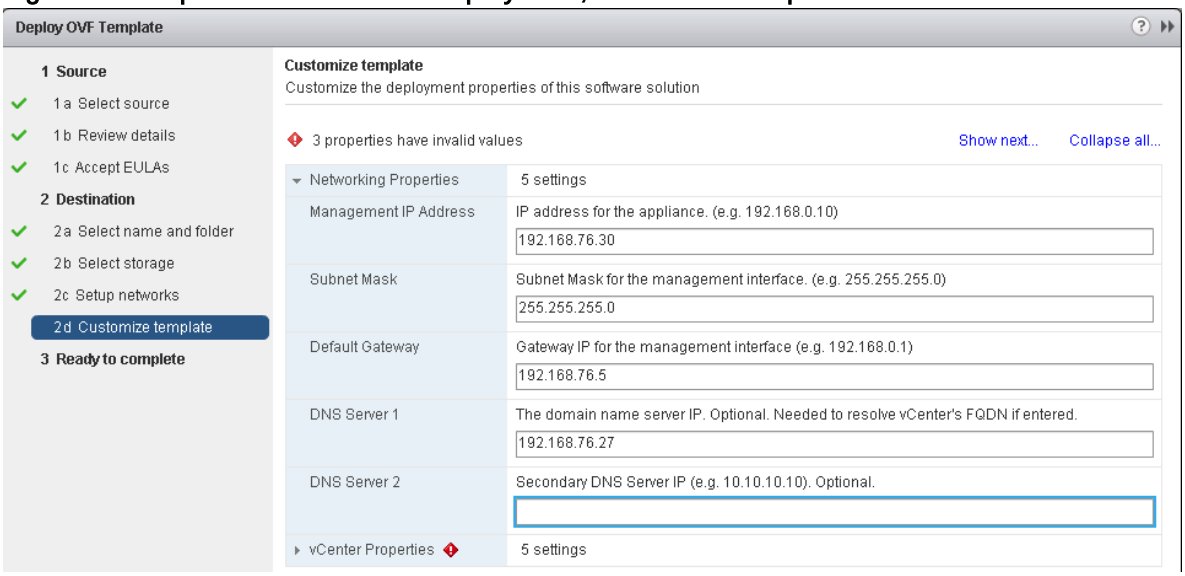
6. Click Browse and select the Nexus1000v Virtual Switch Update Manager OVA file.
7. Select the requires Nexus1000v-vsum file.

**Figure 96 vSphere Web Client – Deploy OVF, Browse for Source File**



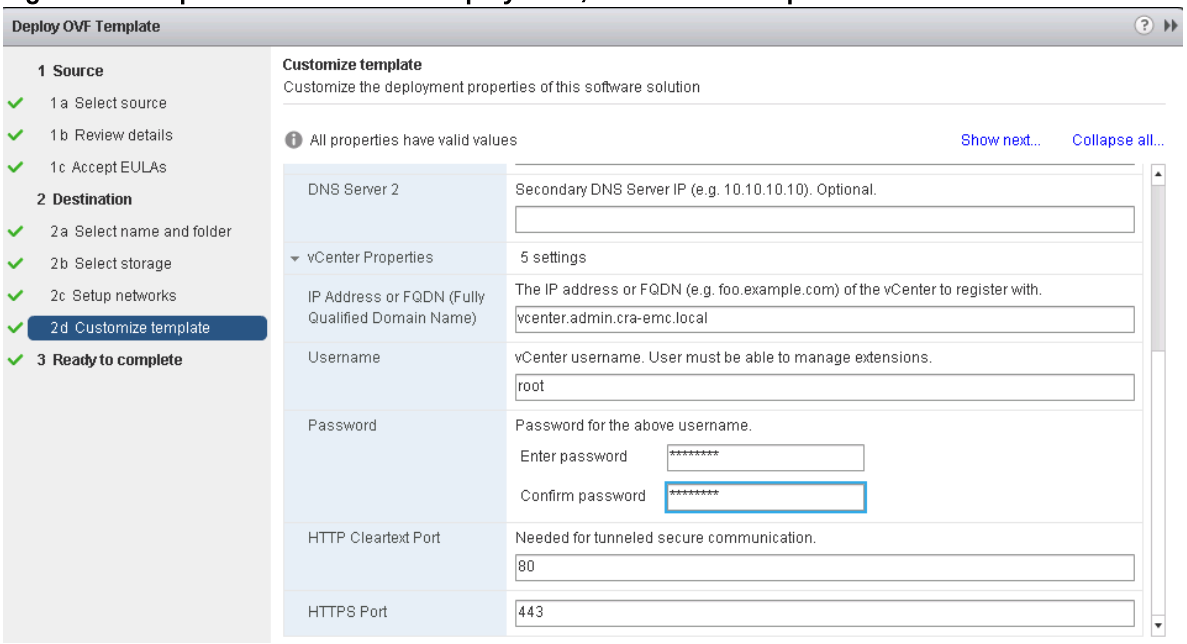

8. Review the Details.
9. Click Next.
10. Accept EULA and click Next.
11. Select <<var_vc_datacenter_name>> as the destination.
12. Click Next.
13. Select <<var_vc_mgmt_datastore1>> as the Storage.
14. Click Next.
15. Select Management Network from the Drop-down list for Management.
16. Click Next.
17. Enter <<var_n1k_vsum_ip>> as the Management IP Address.
18. Enter <<var_mgmt_gw>> as the Default Gateway.

**Figure 97 vSphere Web Client – Deploy OVF, Customize template Part 1**




19. Enter <<var_vc_ip_addr>> as the vCenter IP Address .
20. Enter root as Username.
21. Enter <<var_mgmt_passwd>> as the Password and Confirm it.
22. Click Next.

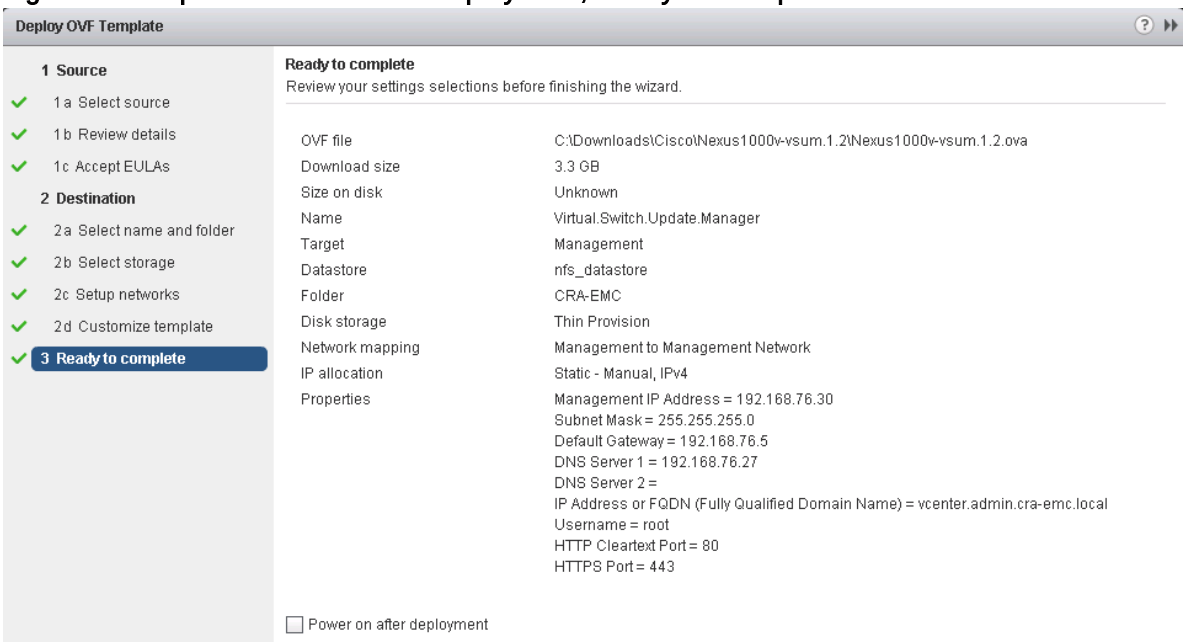
**Figure 98 vSphere Web Client – Deploy OVF, Customize template Part 2**




23. Review the Information.

24. Click Finish.

**Figure 99 vSphere Web Client – Deploy OVF, Ready to Complete**





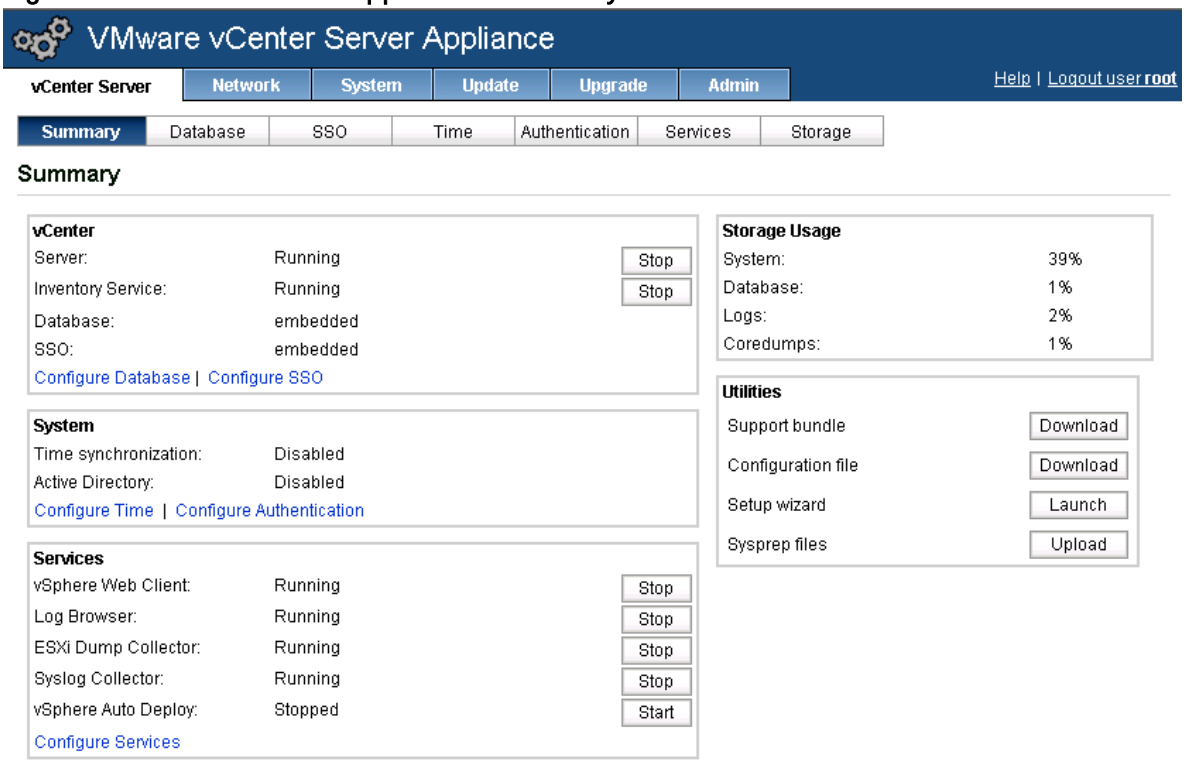

After the Virtual Switch Update Manager is installed and the VM is completely booted, the vSphere Web Client service must be restarted on the vCenter Server Appliance.

25. Log in to the vCenter Server (through a Web Browser) and restart the vSphere Web Client Service.

26. In the Services Section Click Stop in the right of vSphere Web client.

27. As the service is stopped Click Start to restart the Service.

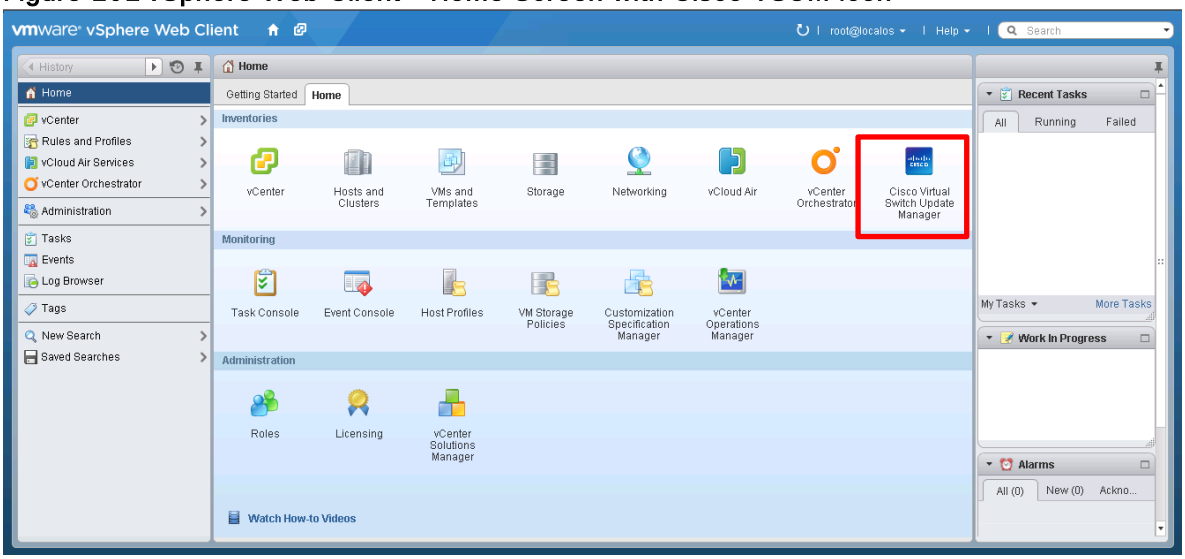
**Figure 100 vCenter Server Appliance – Summary**




28. Log in to the vSphere Web Client.

In the Home Screen the Cisco Virtual Switch Update Manager is now available.

**Figure 101 vSphere Web Client – Home Screen with Cisco VSUM Icon**

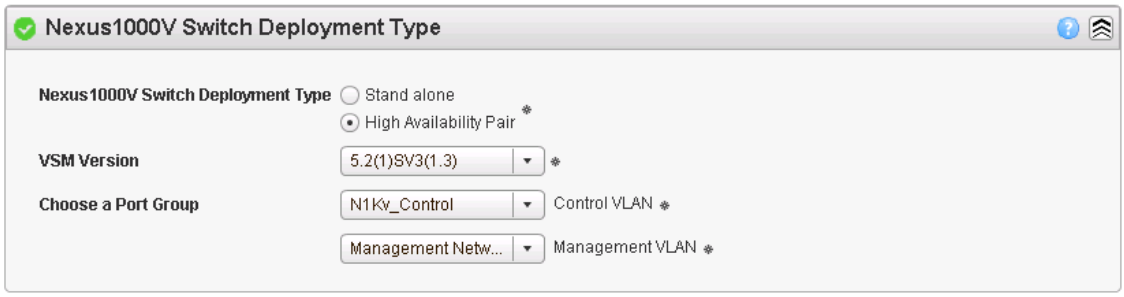


## Install Cisco Nexus 1000v VSM

The Cisco Nexus1000V VSM must be deployed on the ESX hosts in the Management Pod and not on one of the Managed ESXi servers. To install VSM VM, complete the following steps:

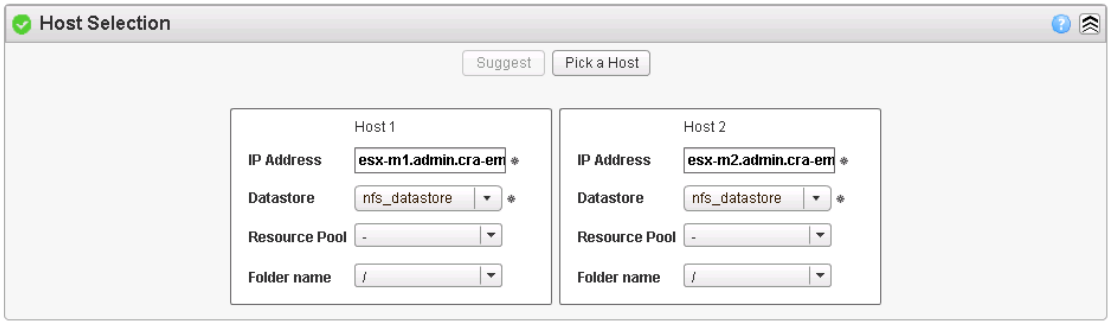
1. Click the Cisco Virtual Switch Update Manager logo.
2. Click Nexus 1000V in the Basic Tasks Section.
3. Click <<var_vc_dc_name>> as the available Datacenter.
4. In the Nexus1000V Switch Deployment Process Section, select I want to deploy new control lane (VSM).
5. In the Nexus1000V Switch Deployment Type section, select High Availability Pair.
6. Select the latest version from the VSM Version drop-down menu.
7. Select <<var_esx_n1k_control_network>> as the Control VLAN.
8. Select <<var_esx_mgmt_network>> as the Management VLAN.

**Figure 102 vSphere Web Client – Deploy N1K, Deployment Type**




9. In Host Selection Section, click Suggest. The install picks the two ESX hosts in the Management Cluster.

**Figure 103 vSphere Web Client – Deploy N1K, Host Selection**




10. In the Switch Configuration Section, enter <<var_n1k_domain_id>> as the Domain ID.

11. Select Management IP Address as the Deployment Type.

**Figure 104 vSphere Web Client – Deploy N1K, Switch Configuration**




12. In the Virtual Supervisor Module (VSM) configuration section:

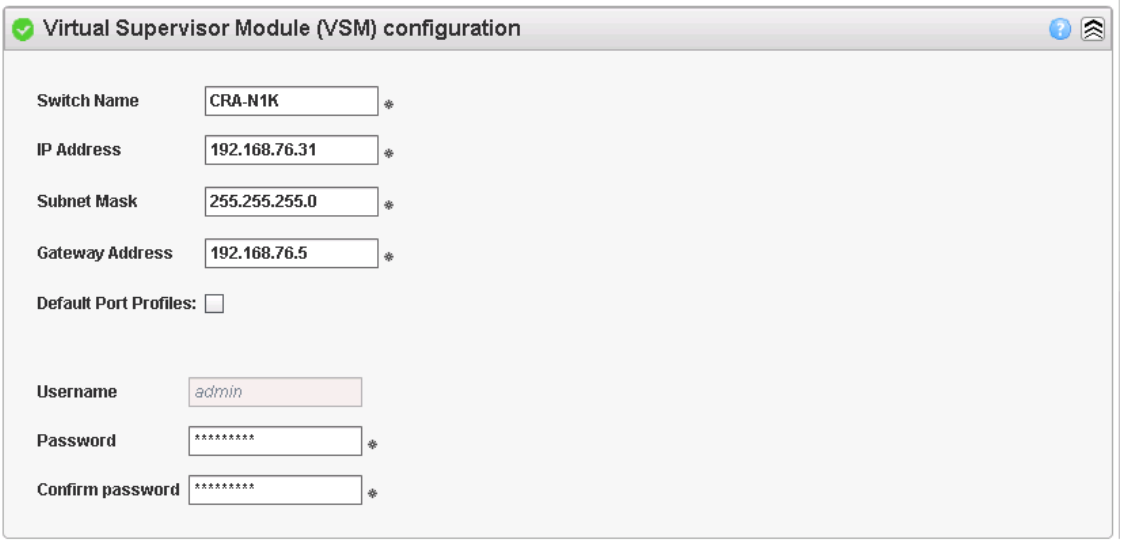
    a. Enter <<var_n1k_switch_name>> as the Switch Name.

    b. Enter <<var_n1k_vsm_ip>> as the IP Address.

    c. Enter <<var_mgmt_netmask>> as the Subnet Mask.

    d. Enter <<var_n1k_passwd>> as Password and confirm it.

**Figure 105 vSphere Web Client – Deploy N1K, VSM configuration**

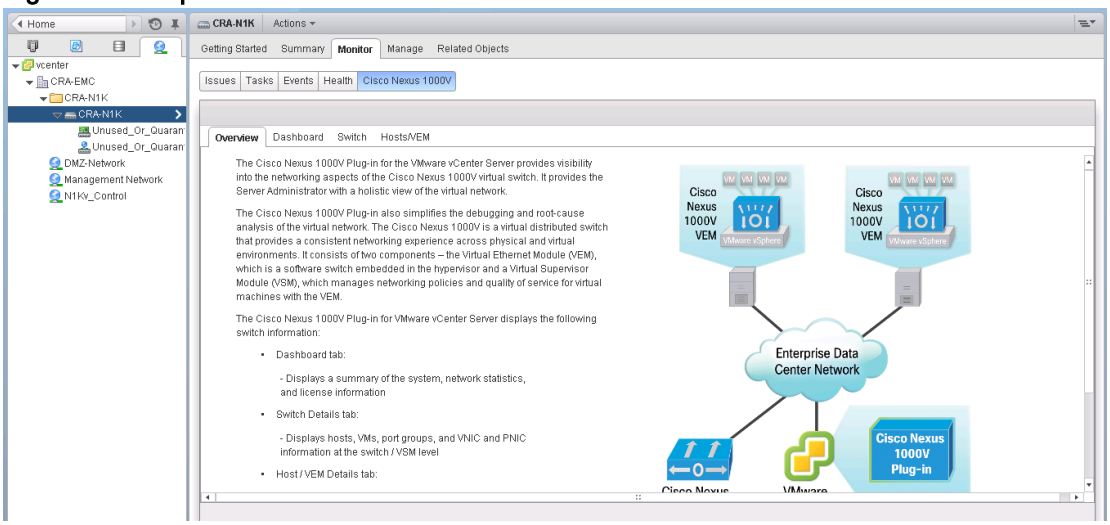



13. Click Finish.

The deployment of the primary VSM and secondary VSM will take a few minutes.

As part of the VSM deployment, the VSUM will also create the required components in the Network section of vCenter.

**Figure 106 vSphere Web Client – Network View**




14. Validate the connection on the Nexus1000V VSM using “show svs connection” and make sure that operational status is “connected” and sync status is “Complete” as shown below:

```
CRA-N1K# show svs connections


connection vCenter:
    ip address: 192.168.76.24
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: CRA-EMC
    admin:
    max-ports: 12000
    DVS uuid: 45 b6 1a 50 98 2a 4d 0a-74 be d0 99 d4 e3 08 7a
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 5.5.0 build-2442329
    vc-uuid: 5A627872-AF18-4FAB-8910-7E0E9068376D
    ssl-cert: self-signed or not authenticated
```

```
CRA-N1K#
```

## Install and Configure EMC Secure Remote Services

This section provides a high-level overview of the EMC SRS system. EMC SRS is mandatory for this solution. For detailed information about EMC SRS System, contact EMC

If you have an EMC SRS system installed you can use this system to register the EMC VNX storages and skip the installation process in this section.

The EMC Secure Remote Services installation file can be loaded from the EMC web site.

Table 19 lists the information to setup the Cisco UCS Central system in this Cisco UCS Integrated Infrastructure.

**Table 19 Information to Setup Cisco UCS Central**

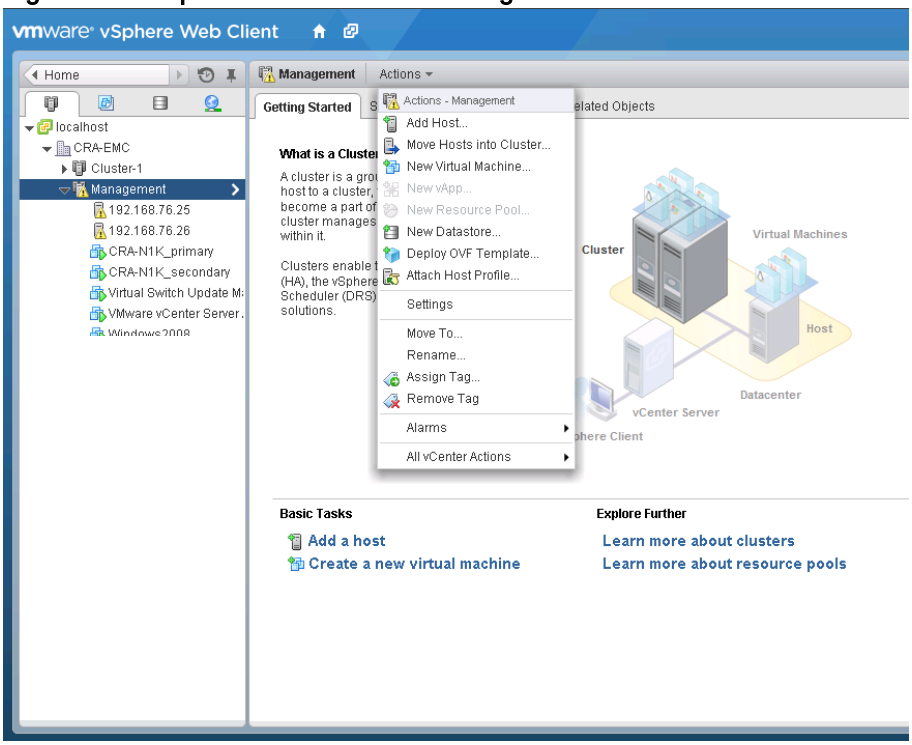
| Name | Variable |
|---|---|
| Name of the Host Cluster for the Management Hosts | <<var_vc_mgmt_cluster_name>> |
| Name of the first Data Center in Virtual Center | <<var_vc_datacenter_name>> |
| Name of the first Datastore on ESXi | <<var_vc_mgmt_datastore_1>> |
| Management Network Name for <<var_mgmt_vlan_id>> | <<var_esx_mgmt_network>> |
| EMC Secure Remote Service Virtual Machine Name | <<var_esx_emcsrs_vm_name>> |
| Management network Netmask | <<var_mgmt_mask>> |
| EMC Secure Remote Service IP Address | <<var_emcsrs_ip> |
| EMC Secure Remote Service hostname | <<var_emcsrs_hostname>> |
| DNS domain name | <<var_mgmt_dns_domain_name>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| DNS server 2 IP Address | <<var_nameserver2_ip>> |
| Global default administrative password | <<var_mgmt_passwd>> |
| Infrastructure Management IP for EMC VNX5400-M01 Control Station | <<var_mgmt_vnx_cs1_ip>> |
| IP address for EMC VNX5400-M1 Storage Processor A | <<var_mgmt_vnx_spa_ip>> |

| Name | Variable |
|---|---|
| IP address for EMC VNX5400-M1 Storage Processor B | <<var_mgmt_vnx_spb_ip>> |
| Default Admin User on the EMC VNX | <<var_mgmt_vnx_user>> |
| Password for the Admin User | <<var_mgmt_vnx_passwd>> |

To deploy and configure EMC Secure Remote Service, complete the following steps:

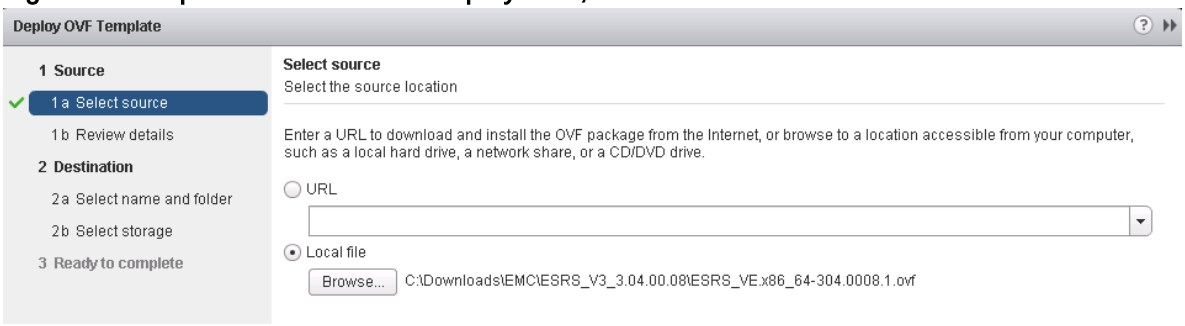
1. Log in to the vSphere Web Client.
2. Click Hosts and Clusters in the Home Screen.
3. Click the <<var_vc_mgmt_cluster_name>>.
4. Click Actions and select Deploy OVF Template.

**Figure 107 vSphere Web Client – Management Cluster Action Menu**



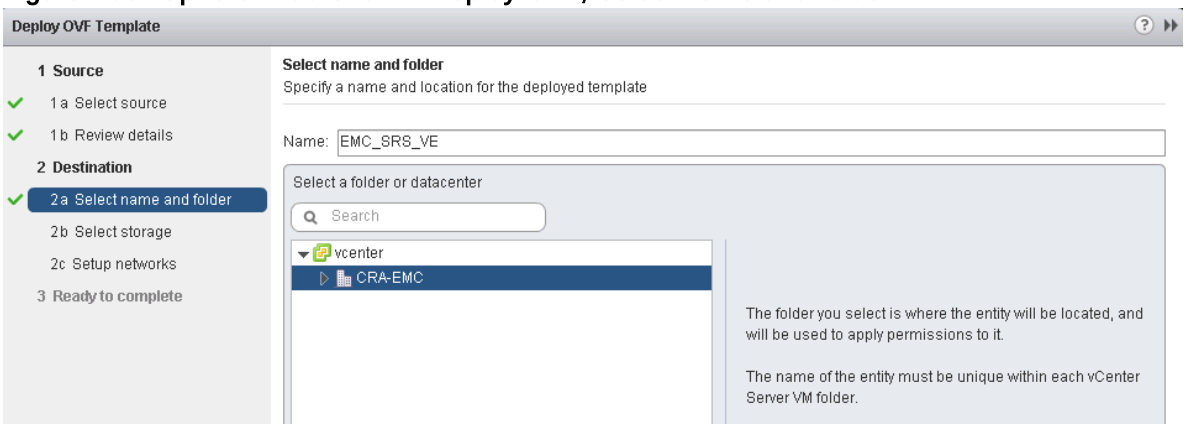

5. Click Browse and select the EMC Solution Enabler OVA file.

**Figure 108 vSphere Web Client – Deploy OVF, Browse for Source File**



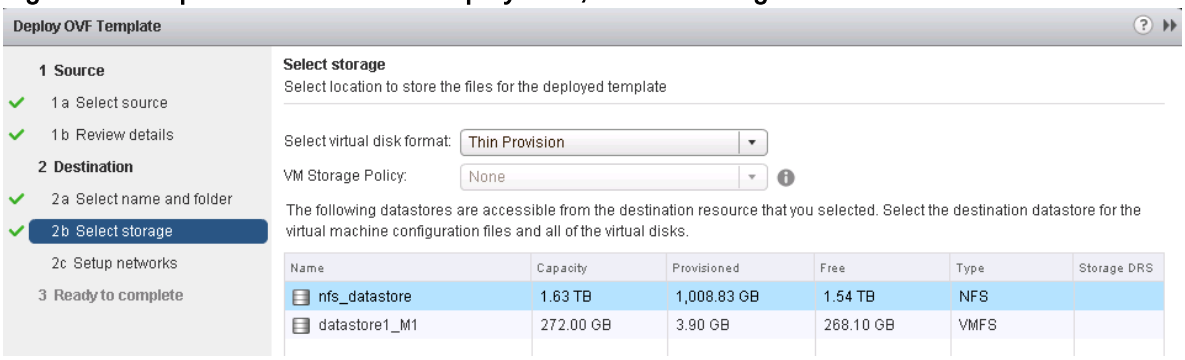

6. Review the details.
7. Click Next.
8. Review the EULA, click Accept.
9. Click Next.
10. Enter <<var_esx_emcsrs_vm_name>> as the name.
11. Select <<var_vc_datacenter_name>> as destination.
12. Click Next.

**Figure 109 vSphere Web Client – Deploy OVF, Select name and folder**




13. Select <<var_vc_mgmt_datastore_1>> as the Storage.
14. Click Next.

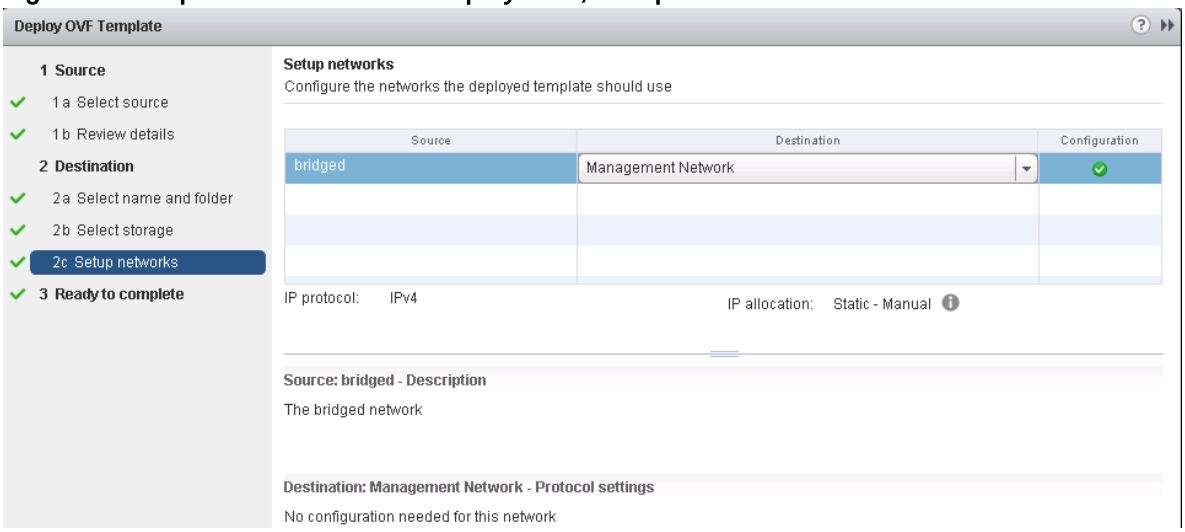
**Figure 110 vSphere Web Client – Deploy OVF, Select Storage**




15. Select <<var_esx_mgmt_network>> as the Destination for both Sources.

16. Click Next.

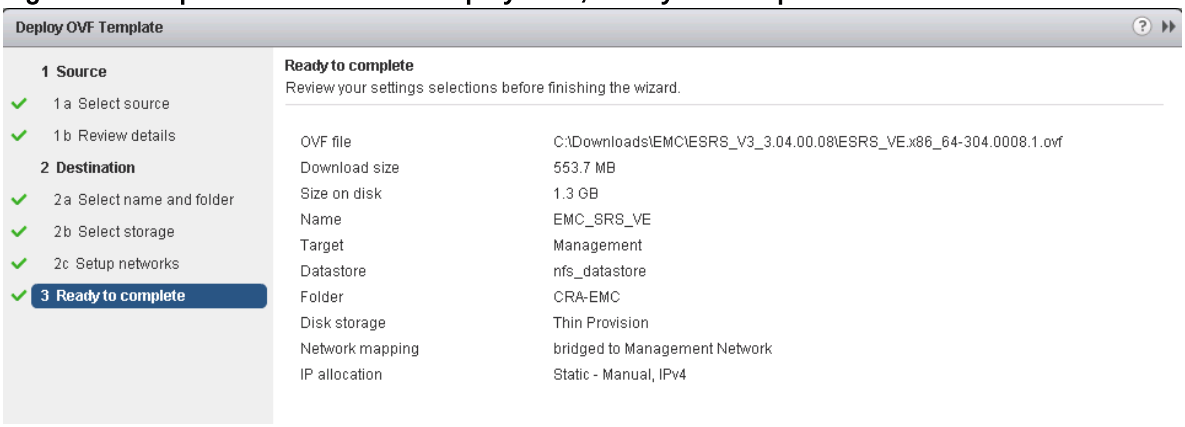
**Figure 111 vSphere Web Client – Deploy OVF, Setup Networks**




17. Review the information.

18. Click Finish.

**Figure 112 vSphere Web Client – Deploy OVF, Ready to Complete**



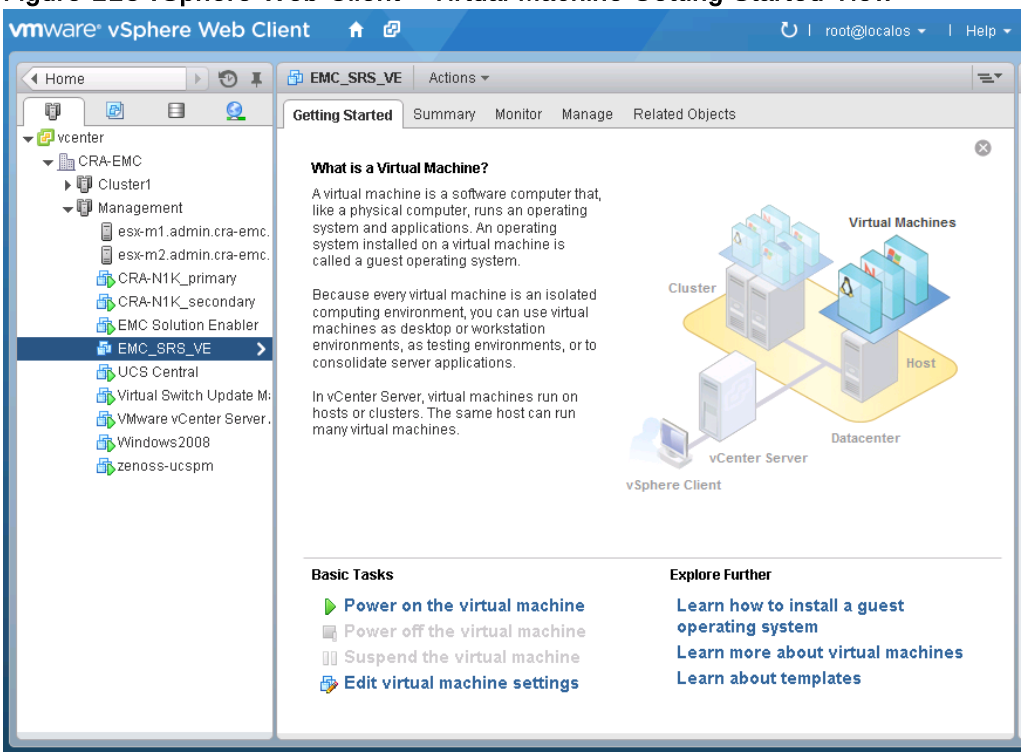

19. Select Hosts and Clusters in the Home screen.

20. Open Management Cluster.

21. Select <<var_esx_emcsrs_vm_name>> Virtual Machine.

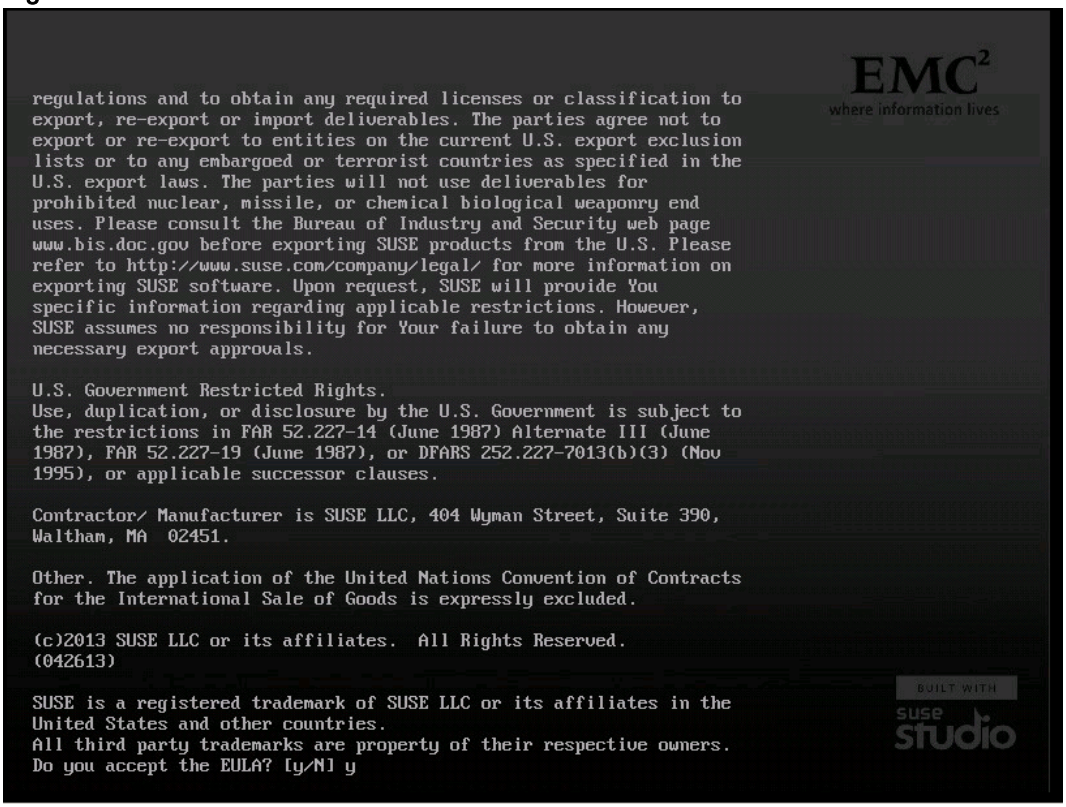
22. Power On the VM.

**Figure 113 vSphere Web Client – Virtual Machine Getting Started View**



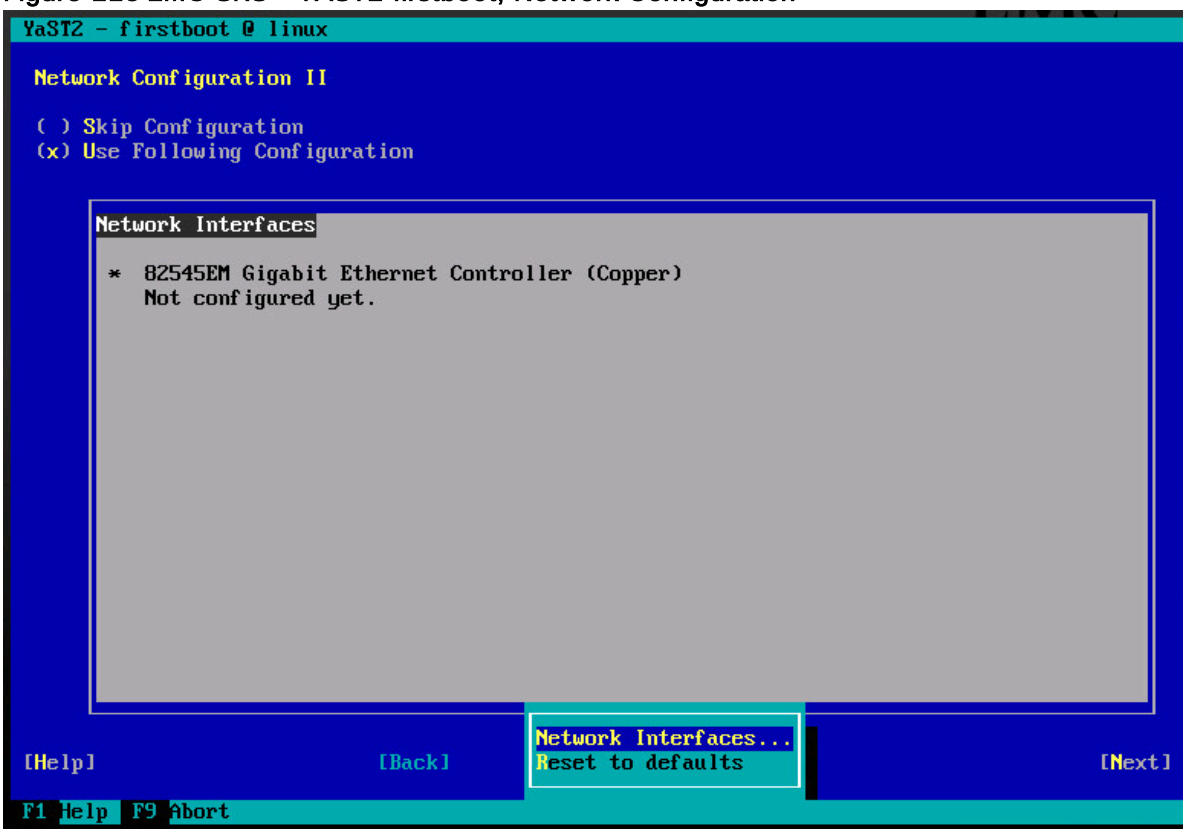

23. Scroll down and press y to accept the License Agreement.

Figure 114 EMC SRS – YAST2 firstboot EULA




24. Select Use the following Configuration and Network Interfaces.

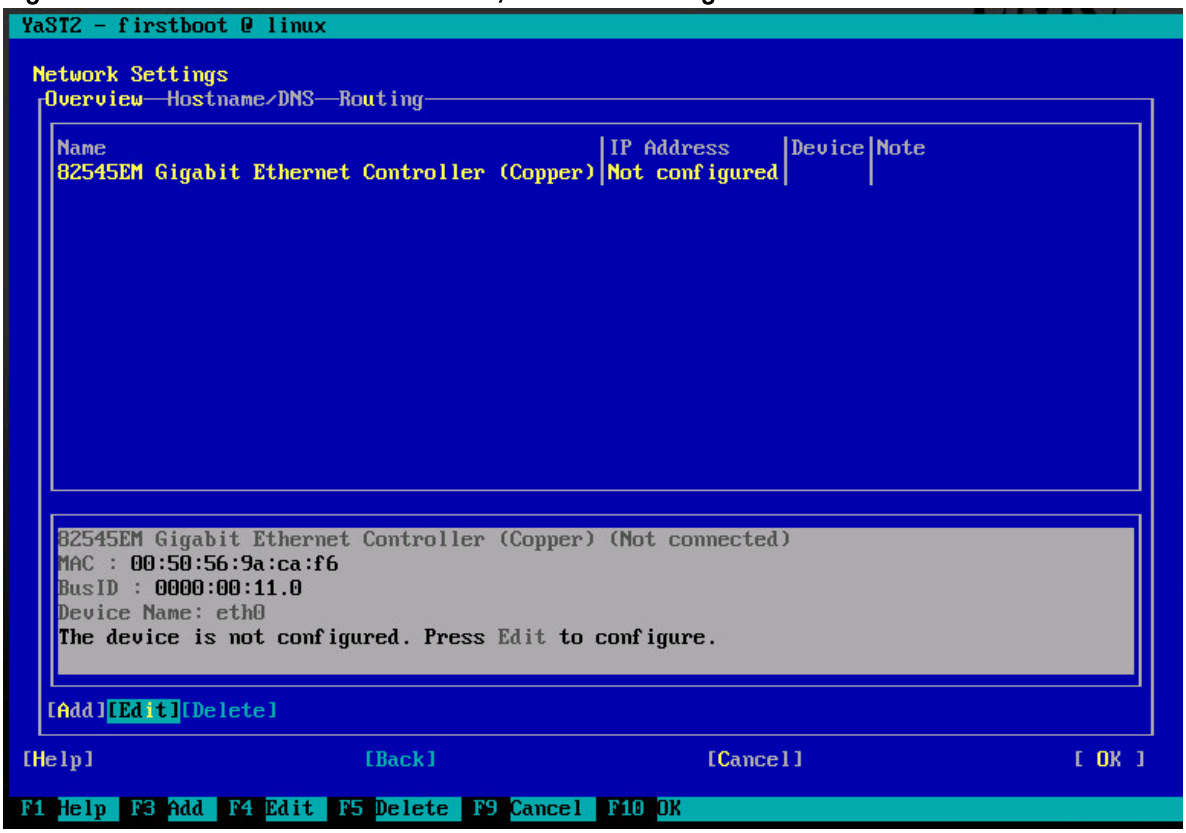
Figure 115 EMC SRS – YAST2 firstboot, Network Configuration




25. Select the listed Network card.

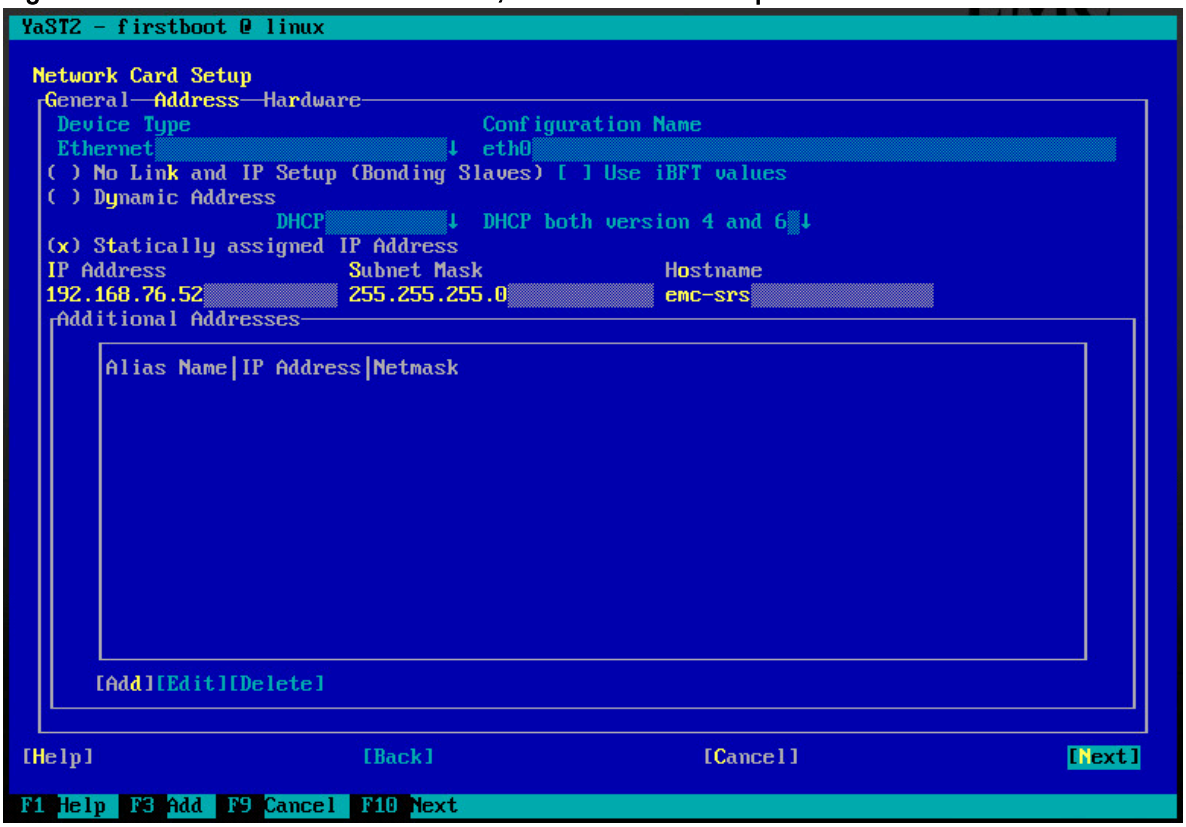
26. Select Edit and press Enter.

Figure 116 EMC SRS – YAST2 firstboot, Network Settings




27. Select Statically assigned IP Address.
28. Enter <<var_emcsrs_ip> as the IP Address.
29. Enter <<var_mgmt_mask>> as the Subnet Mask.
30. Enter <<var_emcsrs_hostname>> as the Hostname.
31. Select Next and press Enter.

Figure 117 EMC SRS – YAST2 firstboot, Network Card Setup




32. In the Hostname/DNS section:

    a. Enter <<var_emcsrs_hostname>> as the Hostname.

    b. Enter <<var_mgmt_dns_domain_name>> as the Domain Name.

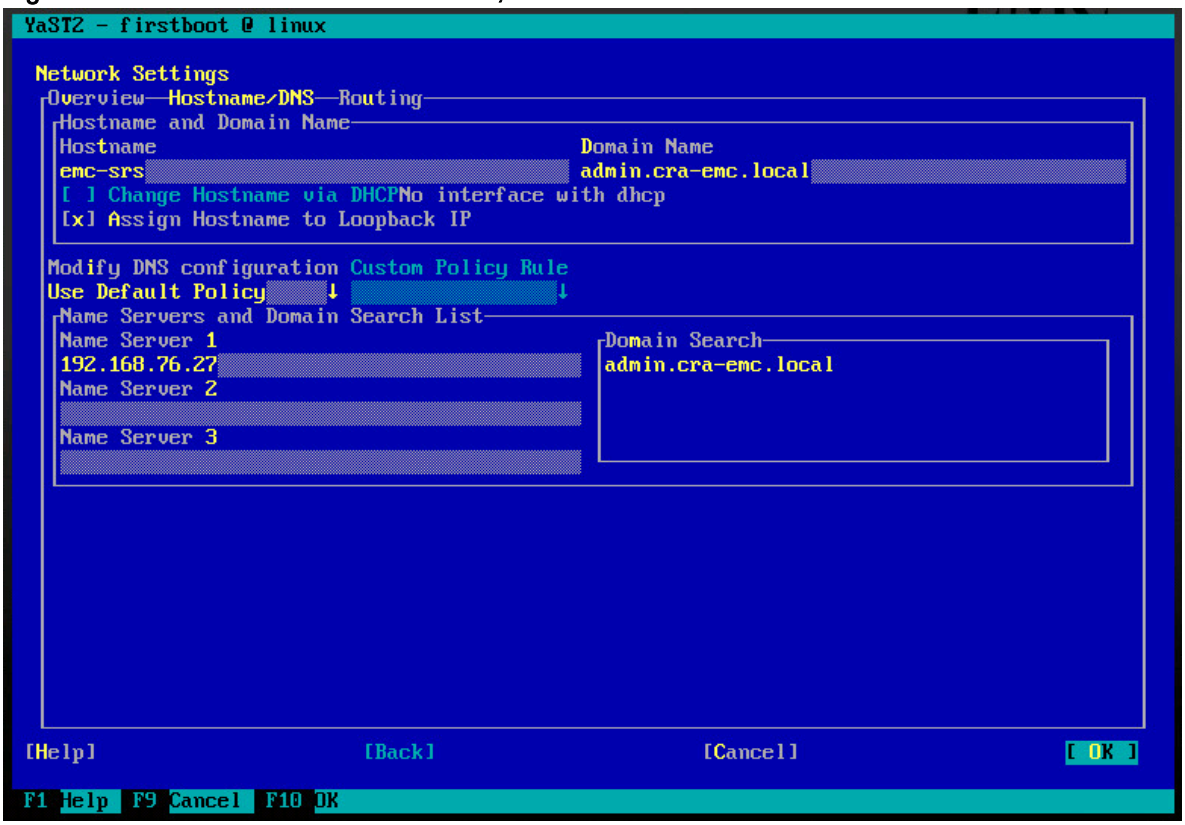
    c. Enter <<var_nameserver_ip>> as the Name Server 1.

    d. Enter <<var_nameserver2_ip>> as the Name Server 2.

    e. Enter <<var_mgmt_dns_domain_name>> in the Domain Search field.

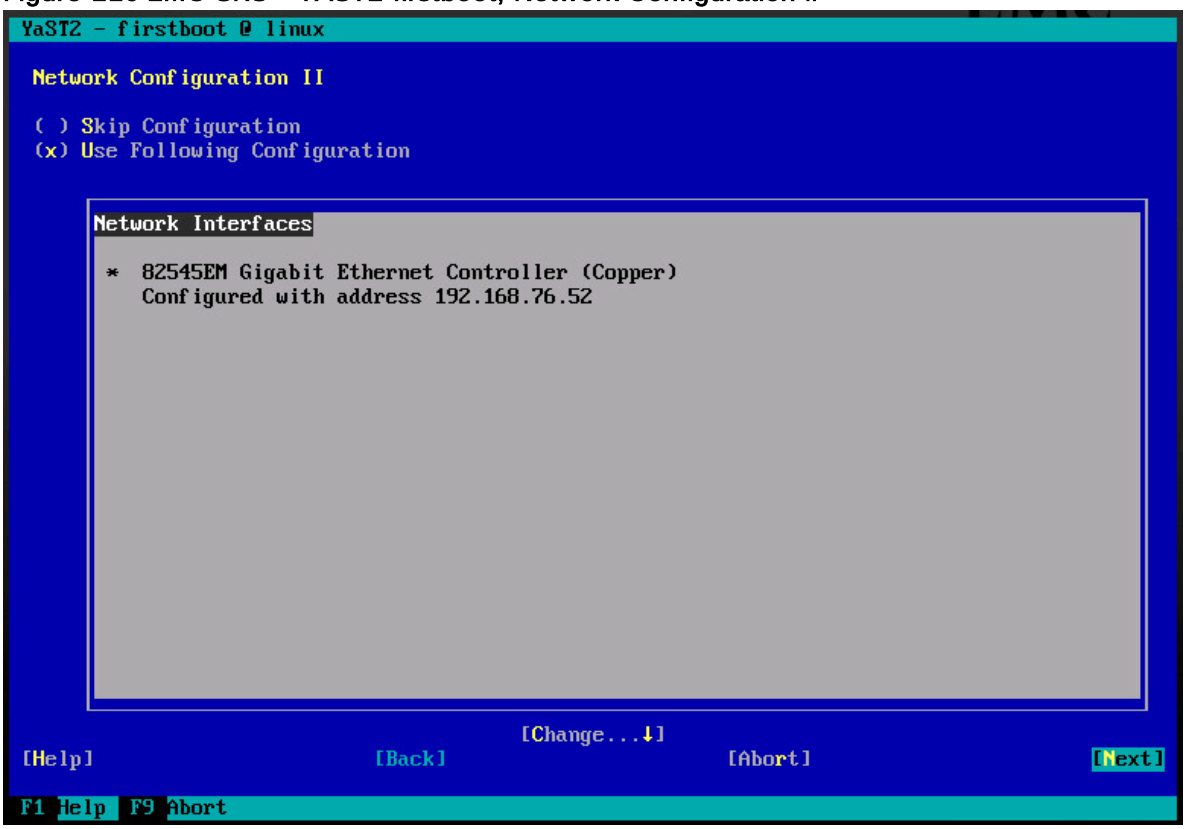
    f. Select OK and press Enter.

Figure 118 EMC SRS – YAST2 firstboot, Hostname/DNS




33. Select Next and press Enter.

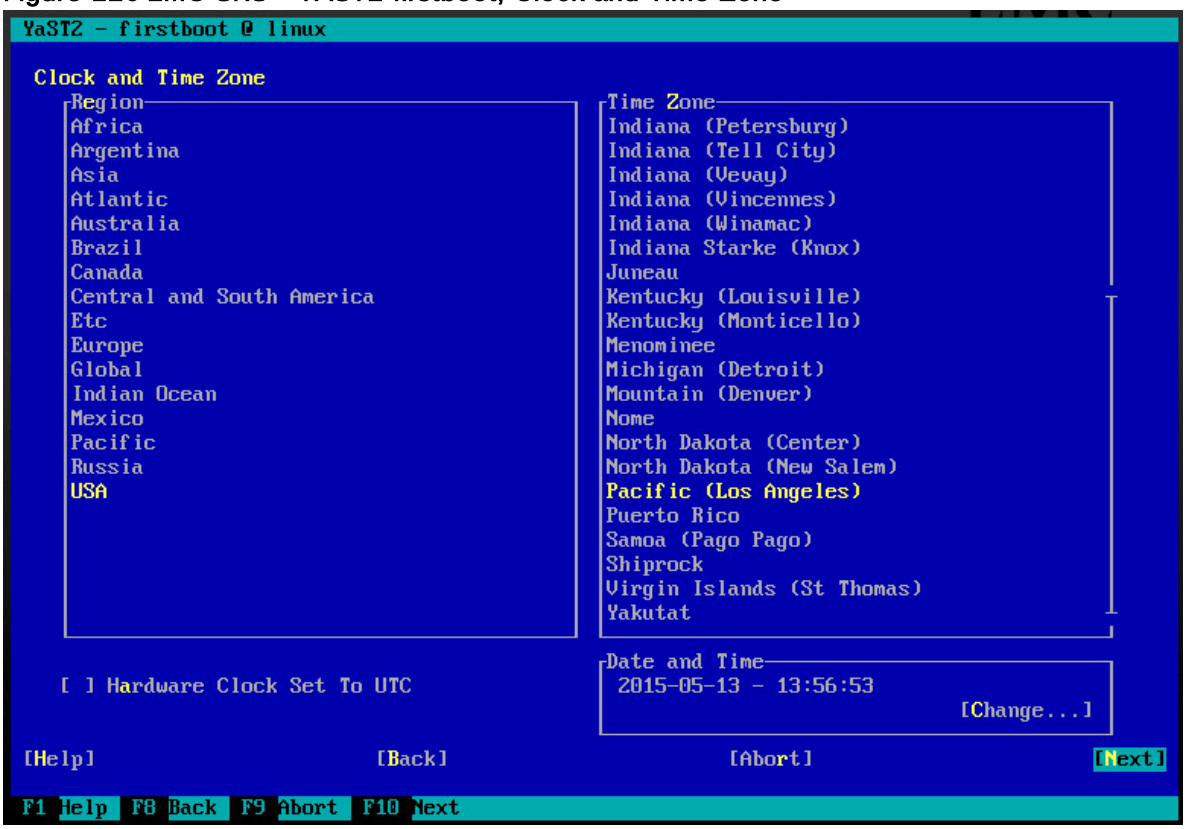
Figure 119 EMC SRS – YAST2 firstboot, Network Configuration II




34. Select the correct Time Zone.

35. Select Next and press Enter.

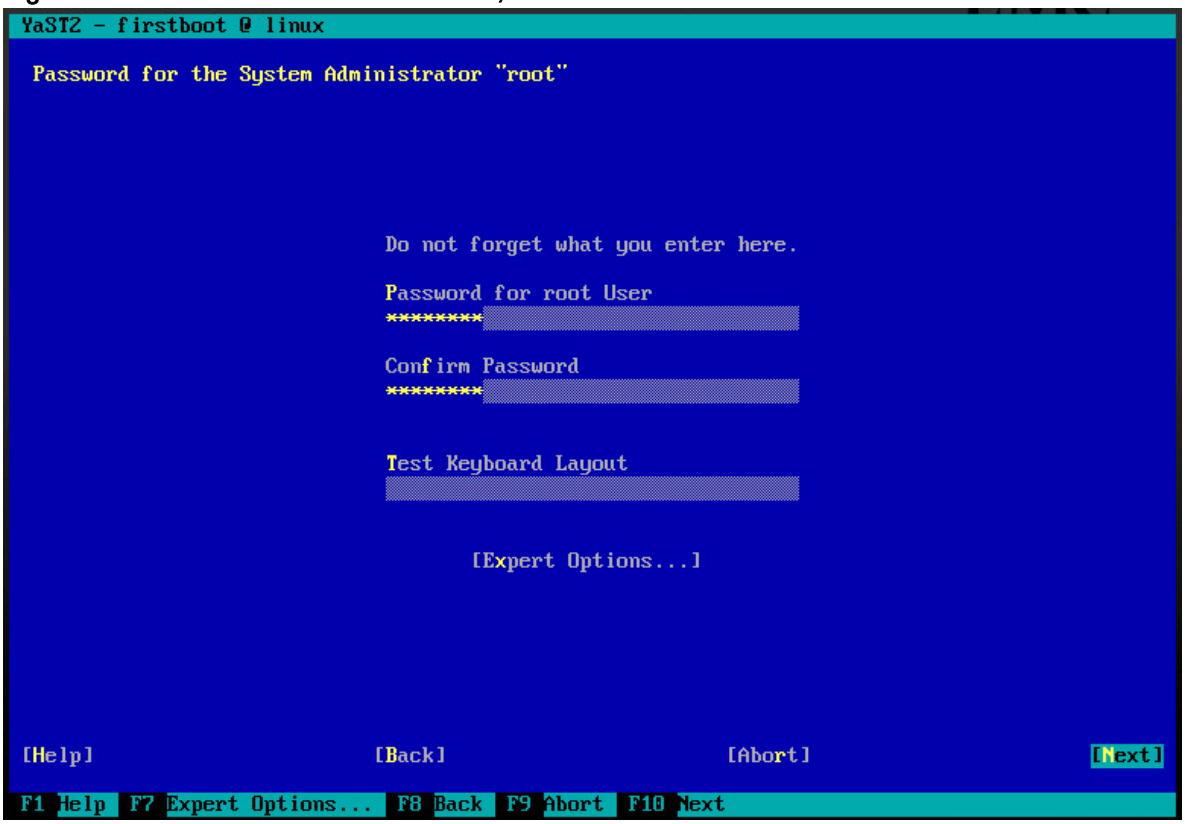
Figure 120 EMC SRS – YAST2 firstboot, Clock and Time Zone




36. Enter <<var_mgmt_passwd>> as the Password for root User and confirm it.

37. Select Next and press Enter.

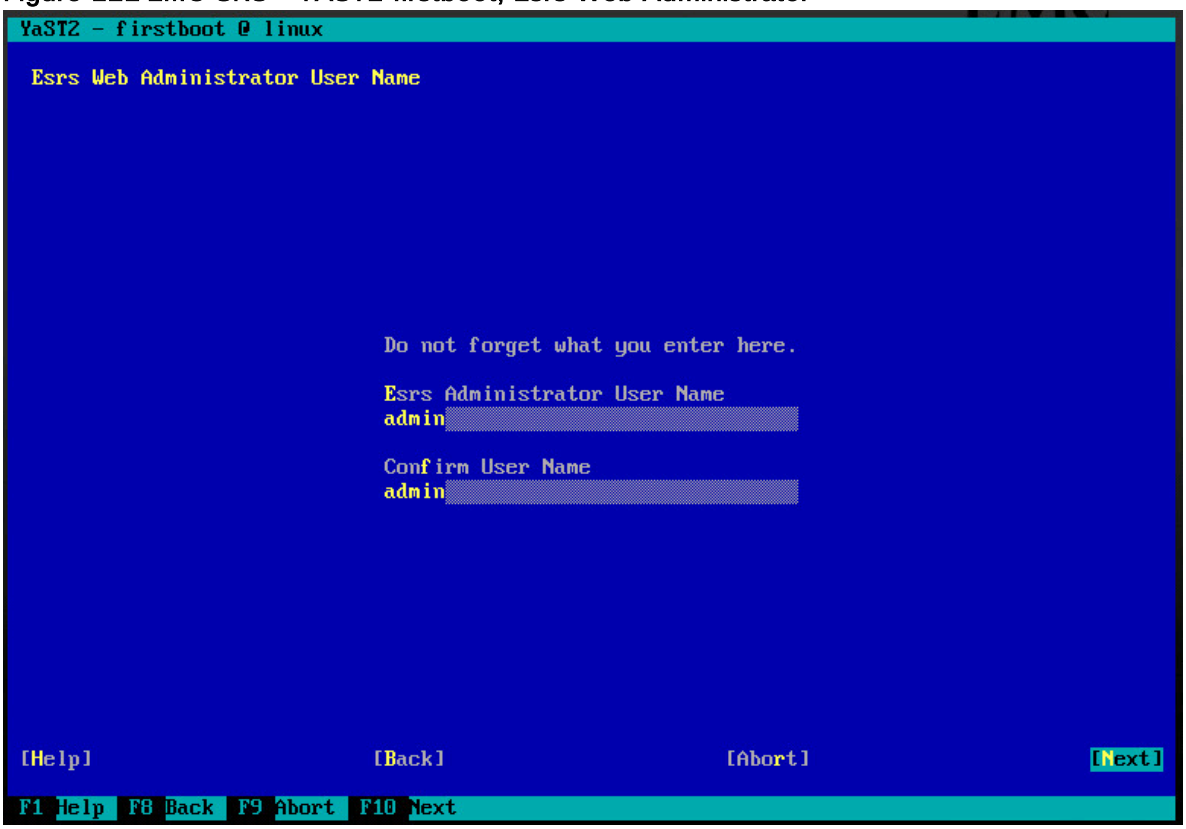
Figure 121 EMC SRS – YAST2 firstboot, Password for root




38. Enter <<var_emcsrs_admin_name>> as the Esrs Administrator User Name and confirm it.

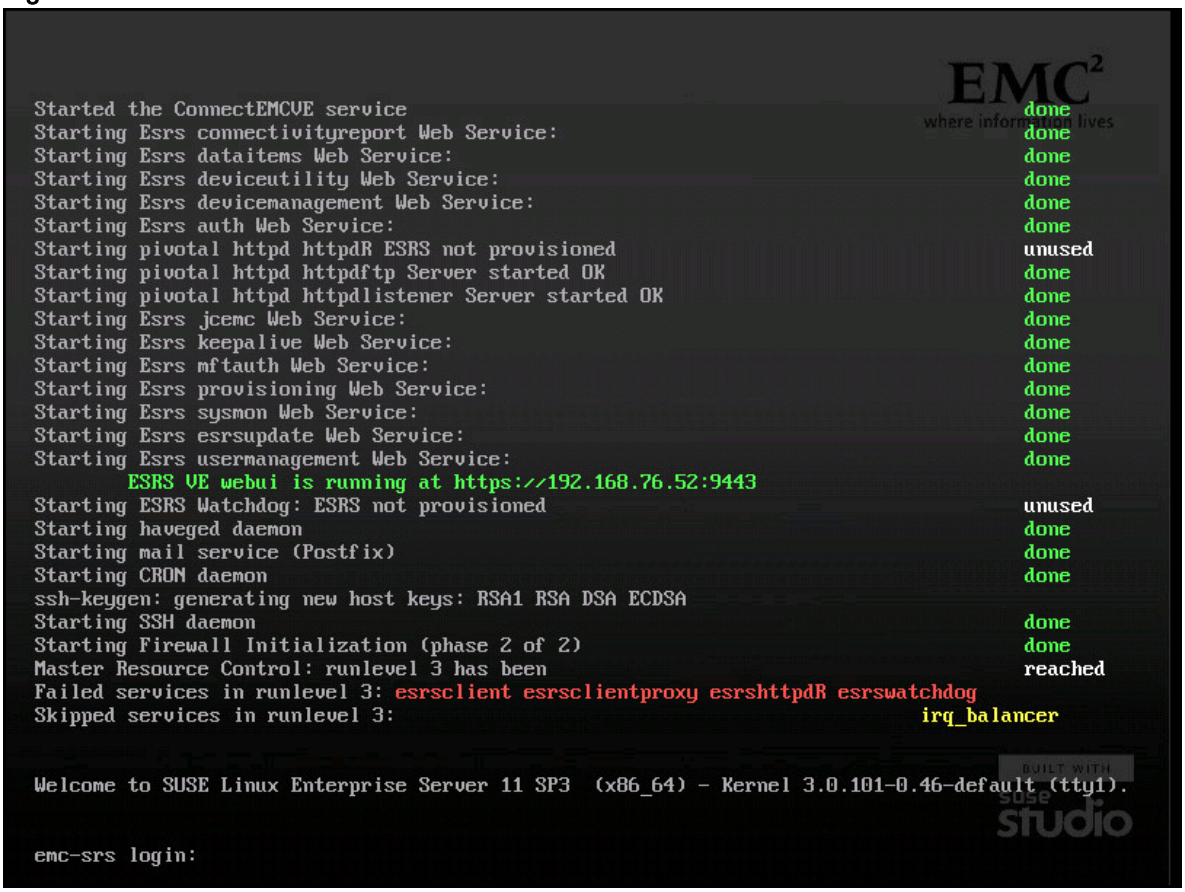
39. Select Next and press Enter.

Figure 122 EMC SRS – YAST2 firstboot, Esrs Web Administrator




40. The system will now start the services.

Figure 123 EMC SRS – Console after boot




41. Open a web browser and navigate to https://<<var_emcsrs_hostname>>:9443.

42. Click Login at the top right corner of the screen.

**Figure 124 EMC SRS – Home Screen**

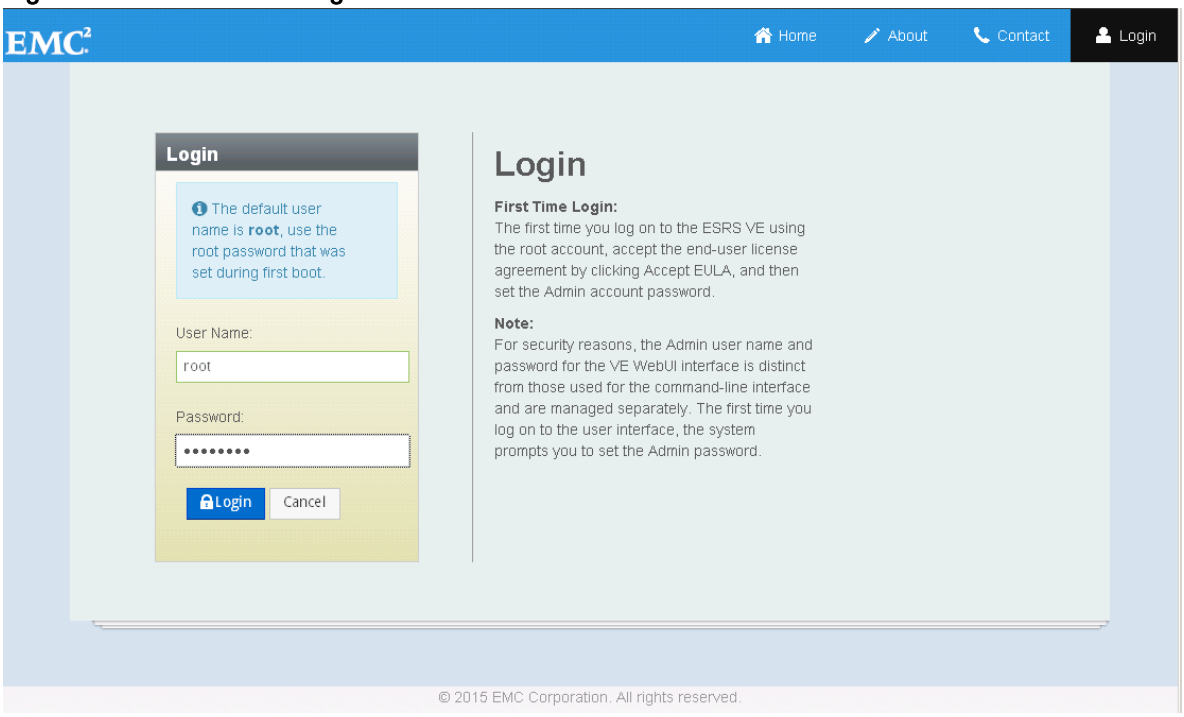



43. Use root as the user.

44. Enter <<var_mgmt_passwd>> as the Password.

45. Click Login.

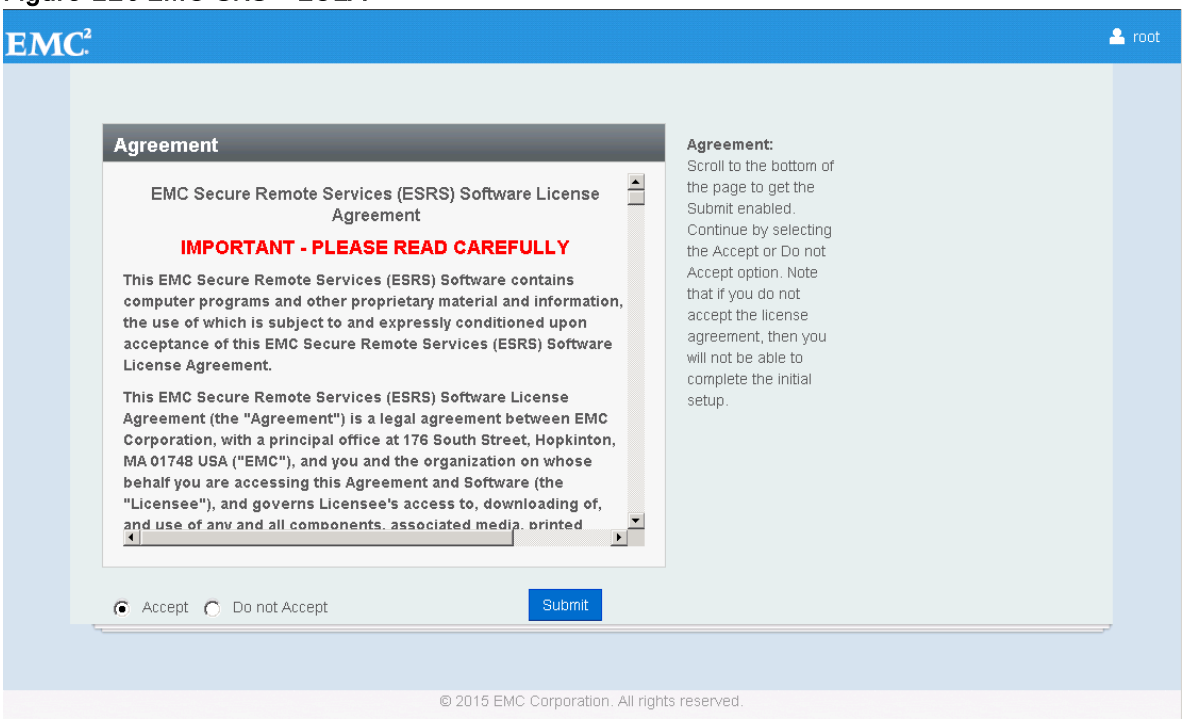
Figure 125 EMC SRS – Login Screen




46. Click the Radio button to Accept the EULA.

47. Click Submit.

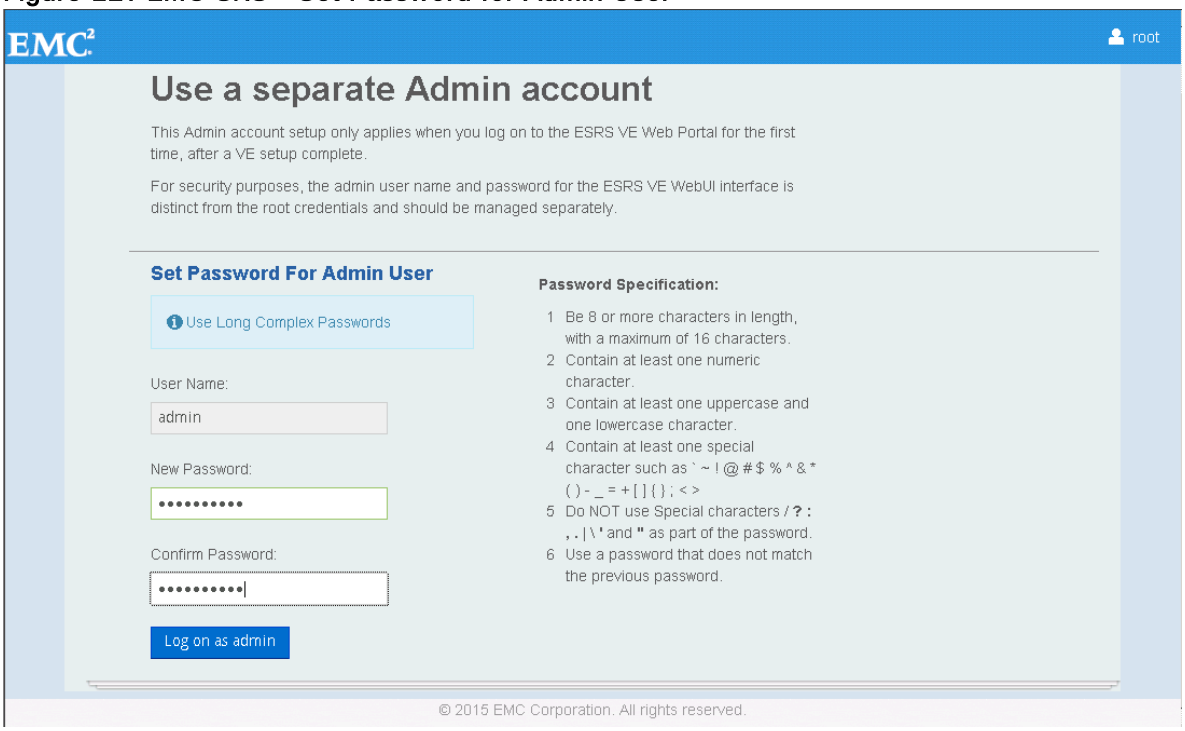
Figure 126 EMC SRS – EULA



48. Enter <<var_emcsrs_admin_passwd>> as the password for user admin.

49. Click Log on as admin.

**Figure 127 EMC SRS – Set Password for Admin User**




50. Complete the Primary Contact Registration form.

51. Click Submit & Go to Technical Registration.

52. Complete the Technical Contact Registration.

53. Click Submit & Go to Provisioning.

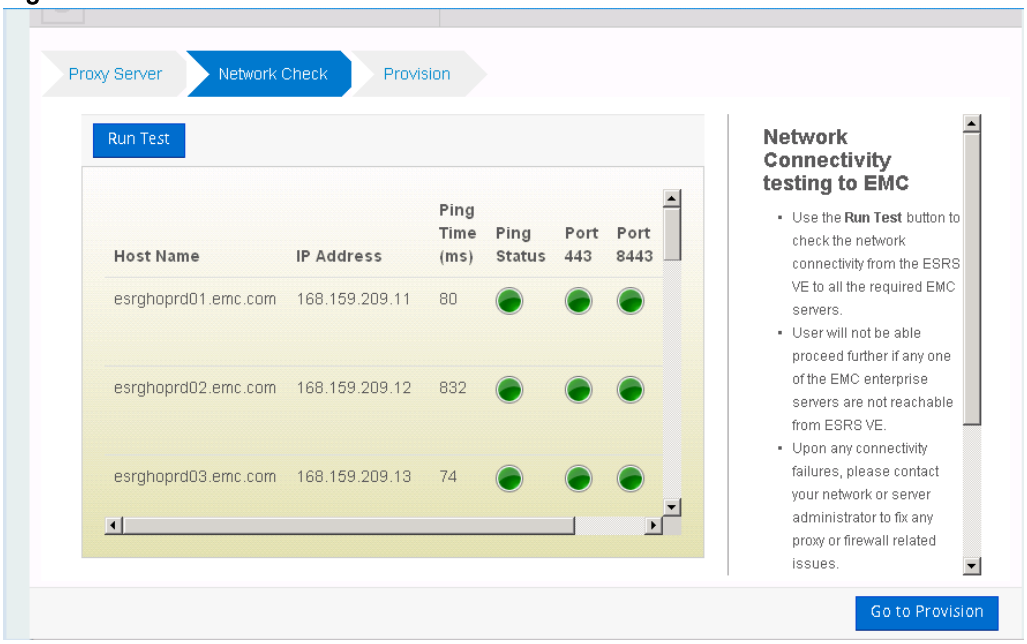
54. Configure the Proxy Server configuration.

55. Click Submit & Go to Network Check.

56. Click Run Test.

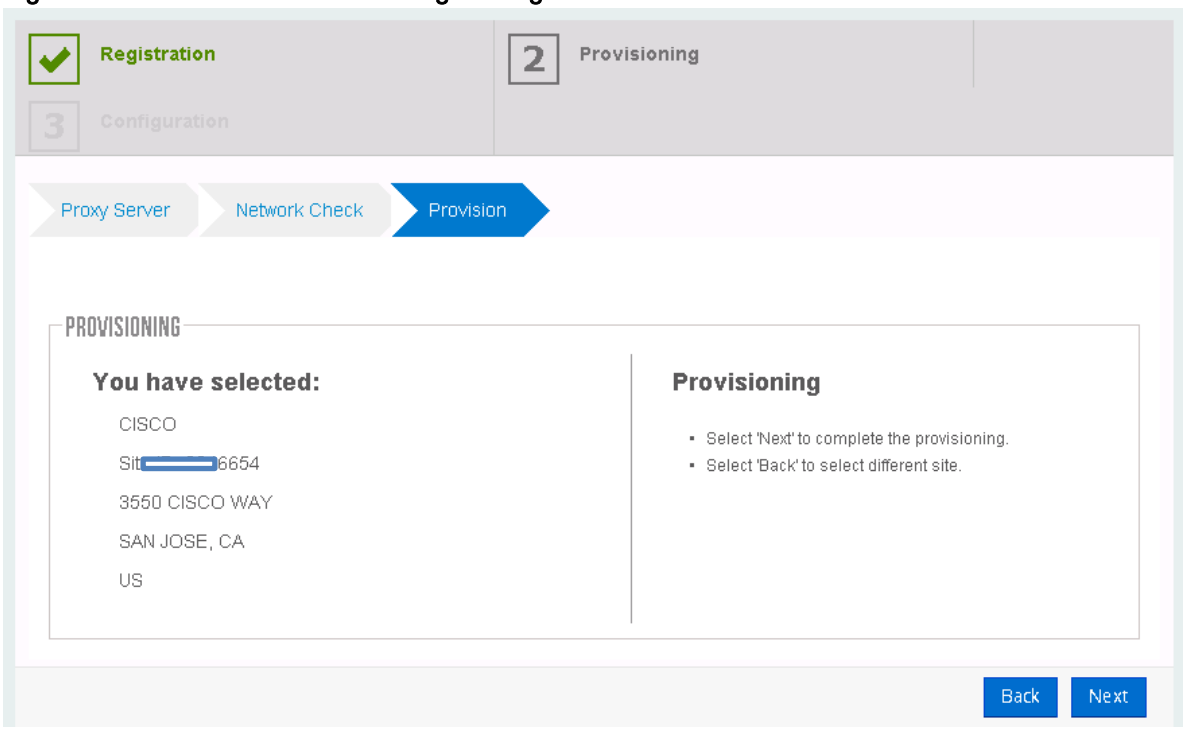
57. Click Go to Provision.

Figure 128 EMC SRS – Network Test results




58. Enter your User name and Password you use at http://www.emc.com/.
59. Click Next.
60. Enter the Side ID where the storage is located – If you do not know the side ID please contact EMC support.
61. Click Next.

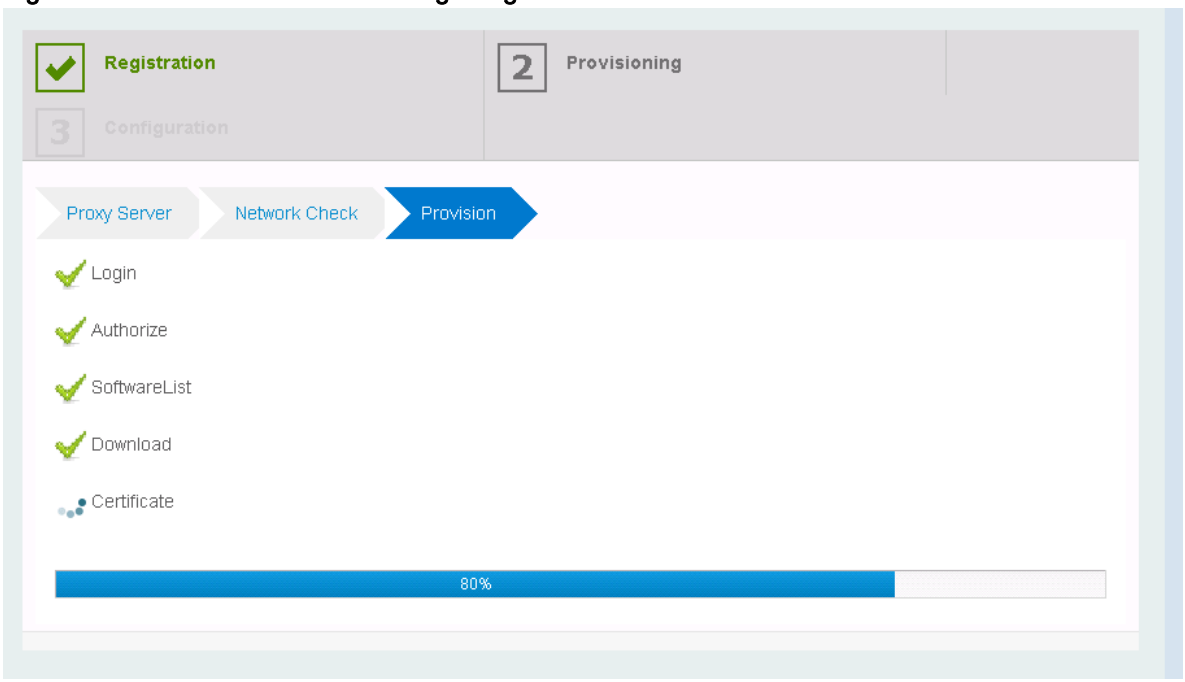
Figure 129 EMC SRS – Provisioning settings




62. Check the information.

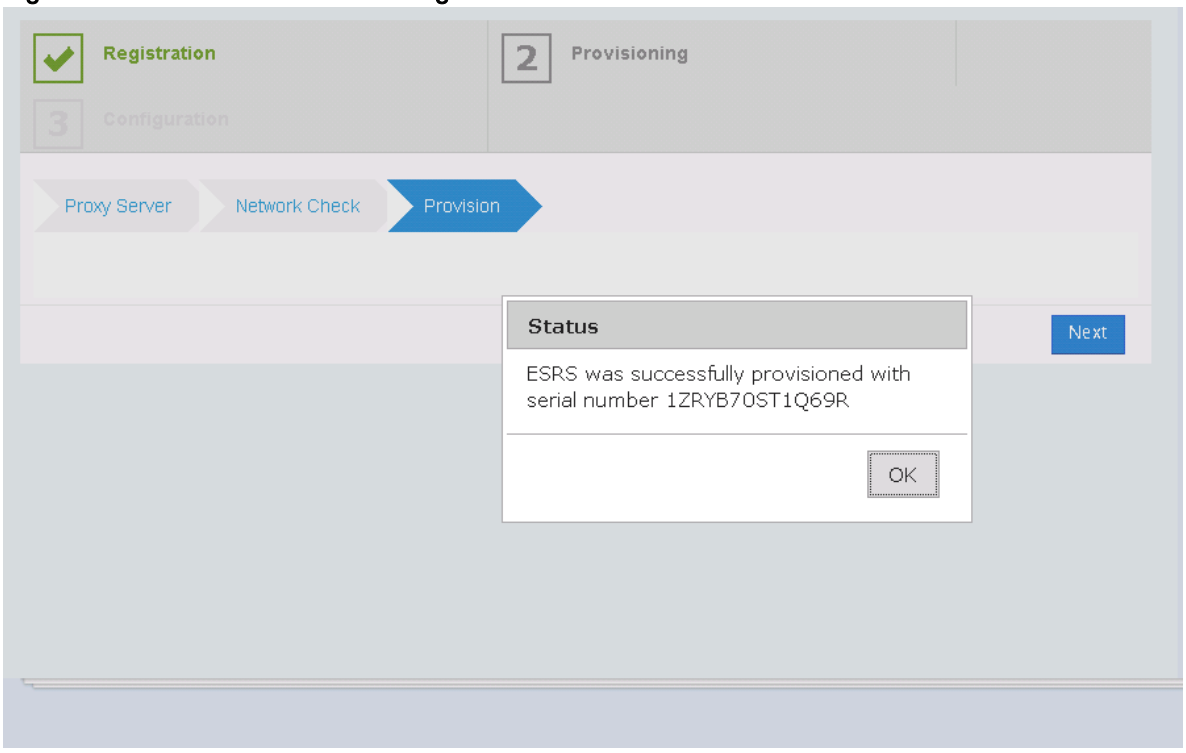
63. Click Next.

Figure 130 EMC SRS – Provisioning Progress



After the provisioning process is finished, a pop-up window displays with the Serial Number for this EMC SRS system.

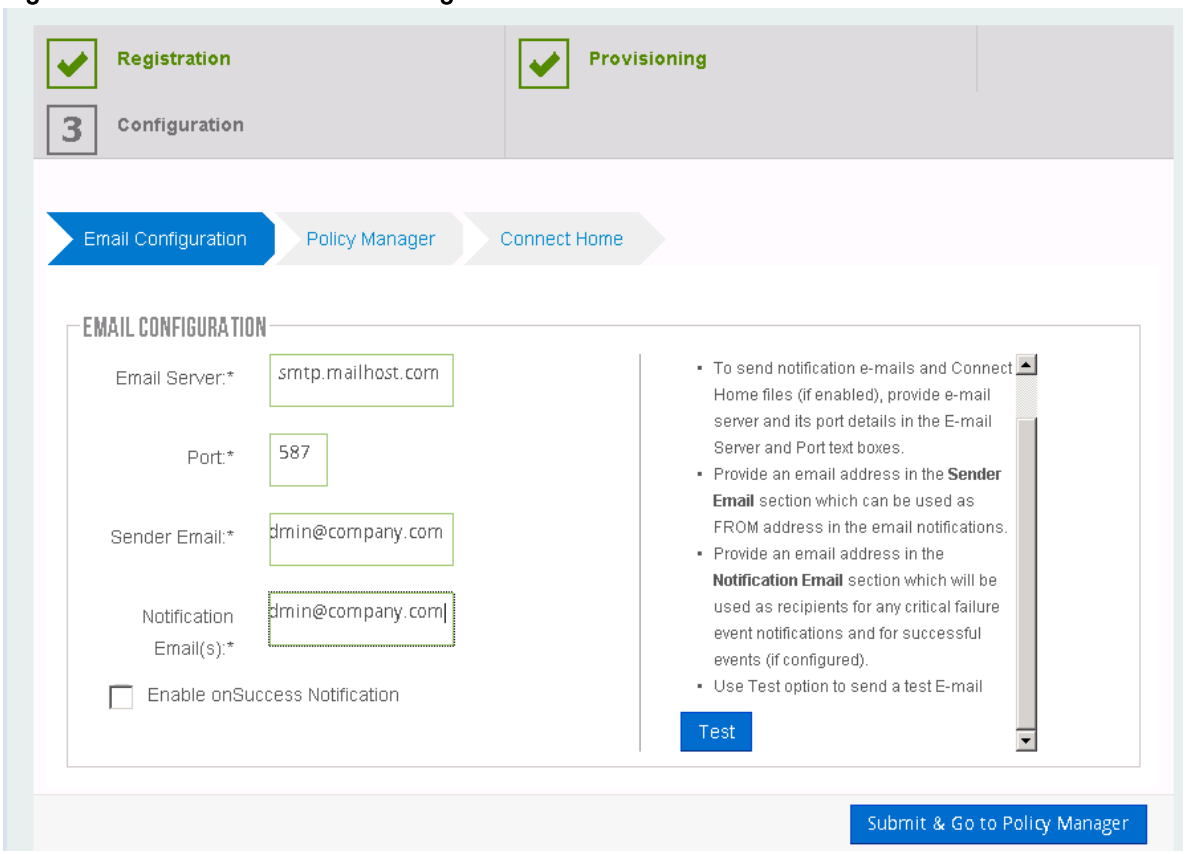
**Figure 131 EMC SRS – Provisioning finished**




64. Enter the information for the Email Configuration. Make sure the SMTP server does NOT require authentication.

65. Click Submit & Go To Policy Manager.

**Figure 132 EMC SRS – Email Configuration**

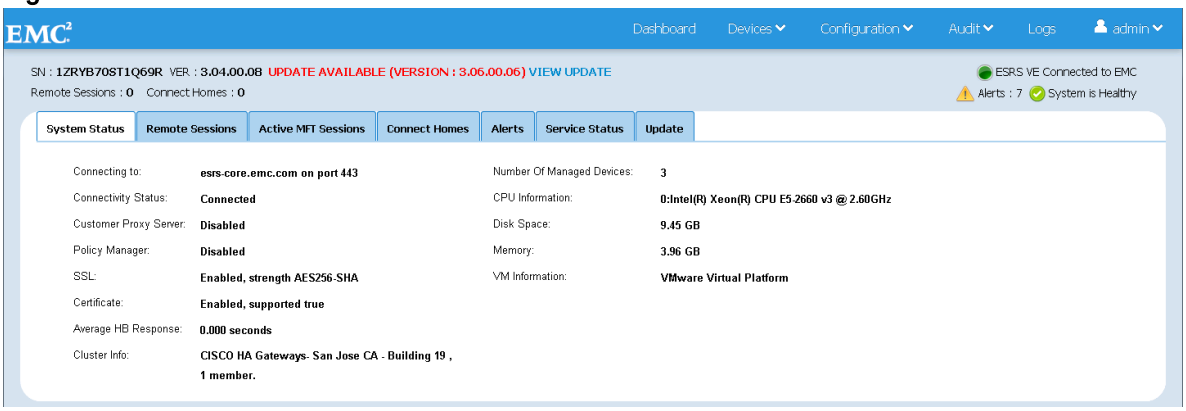



66. Configure the Policy Manager.

67. Configure Connect Home.

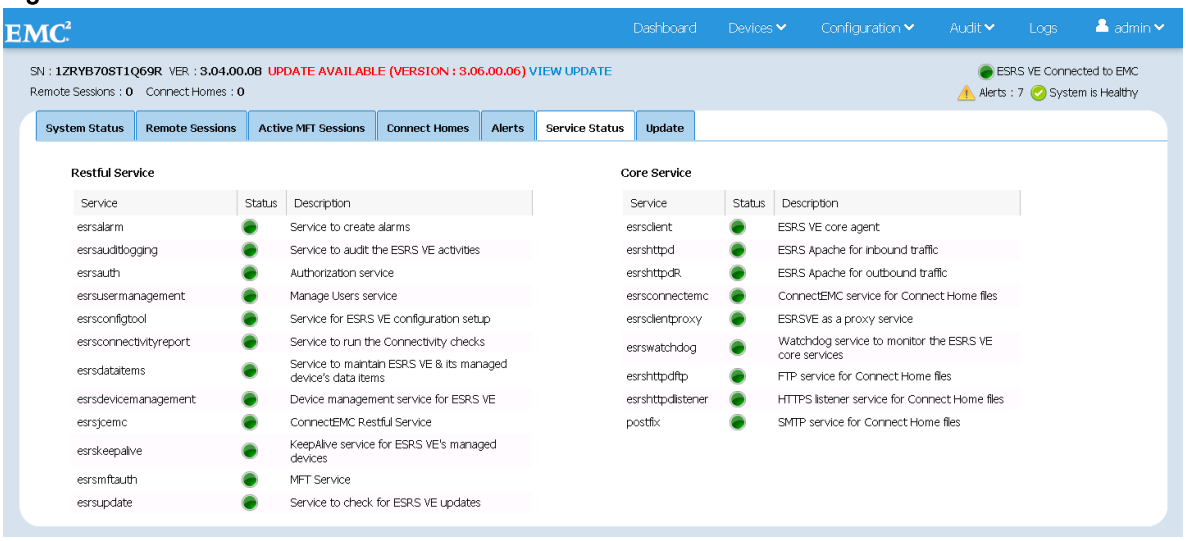
The Dashboard displays.

**Figure 133 EMC SRS – Dashboard**




68. Click the Service Status Tab, all Services should be green.

**Figure 134 EMC SRS – Services Status**



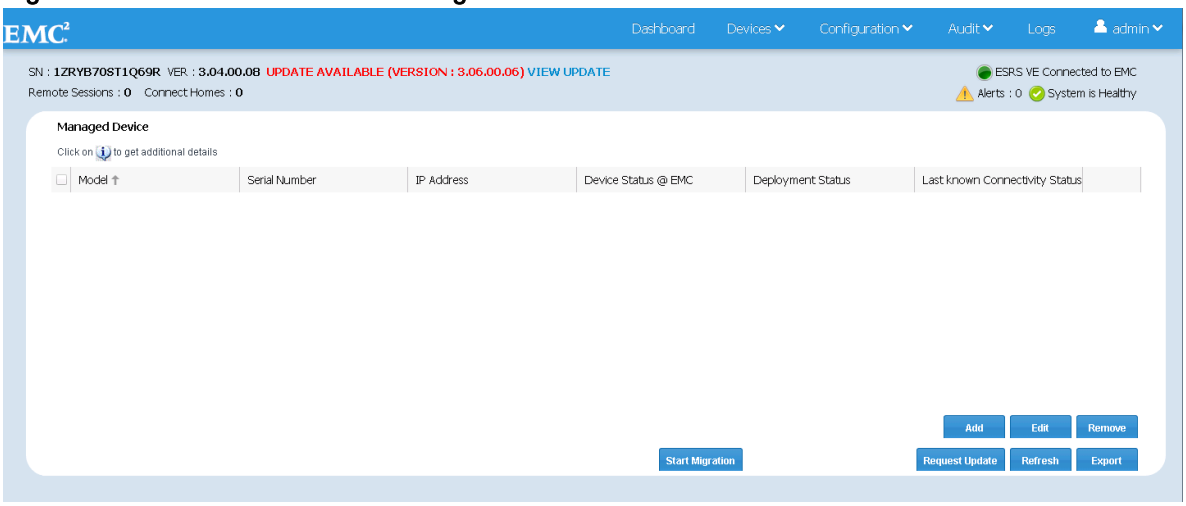

69. Click Devices > Managed Devices.

**Figure 135 EMC SRS – Devices Menu**




70. Manage devices should not be listed at this stage. Click Add.

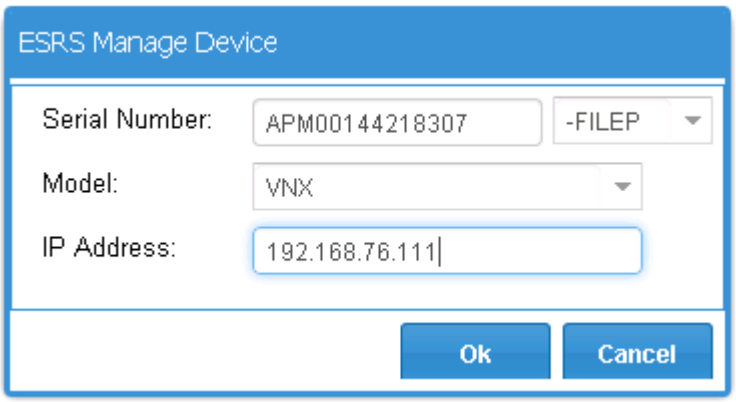
**Figure 136 EMC SRS – List of Managed Devices**




71. Enter the Serial Number of the VNX in the Management POD.

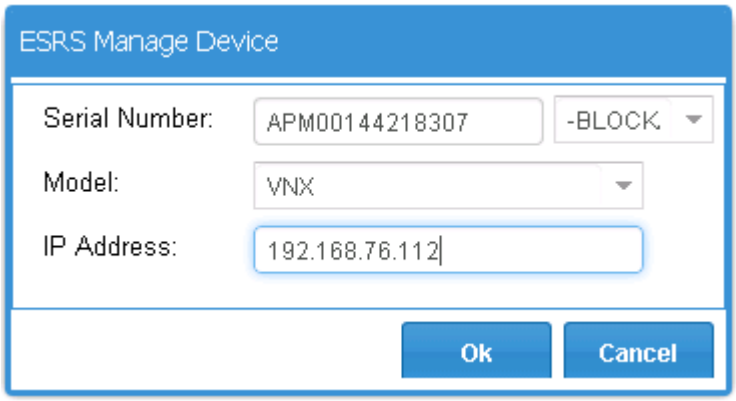
72. Select VNX from the Model drop-down list.
73. Select –FILEP from the drop-down menu right of the serial number.
74. Enter <<var_mgmt_vnx_cs1_ip>> as the IP Address.
75. Click OK.

**Figure 137 EMC SRS – Add Device, Control Station for File**




76. Click Add.
77. Enter the Serial Number of the VNX in the Management POD.
78. Select VNX from the Model drop-down list.
79. Select –BLOCK-A from the drop-down menu right of the serial number.
80. Enter <<var_mgmt_vnx_spa_ip>> as the IP Address.
81. Click OK.

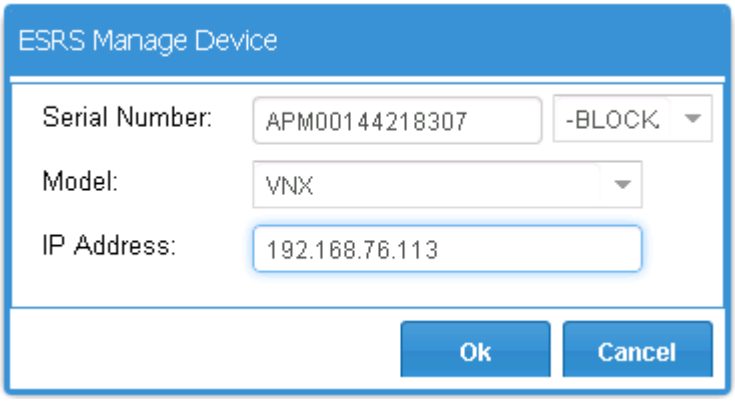
**Figure 138 EMC SRS – Add Device – SPA for Block**




82. Click Add.

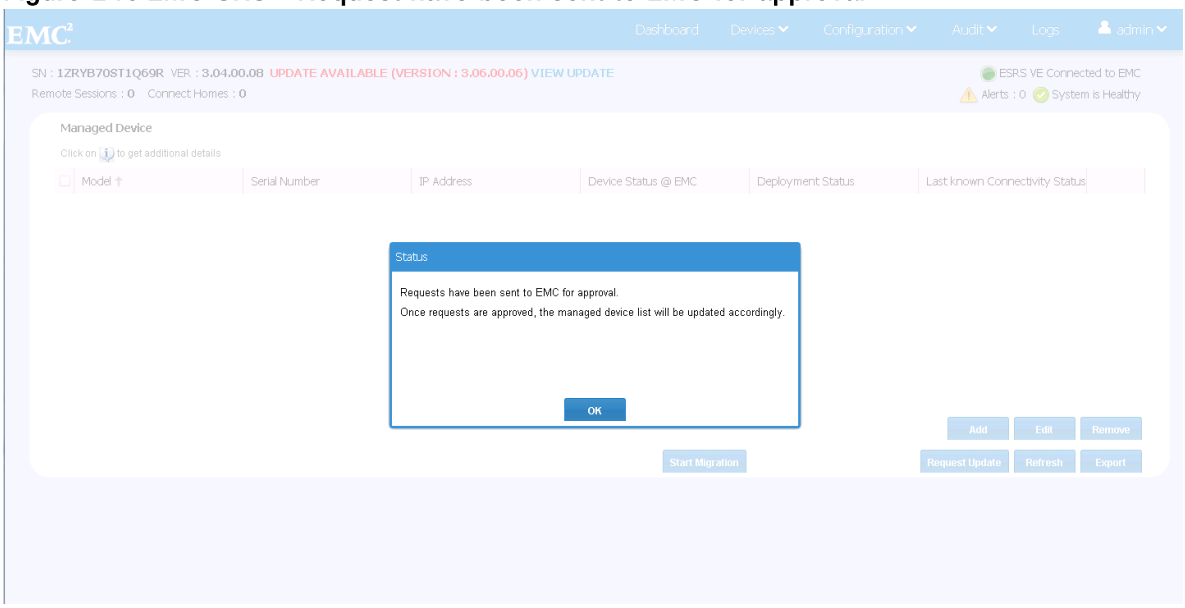
83. Enter the Serial Number of the VNX in the Management POD.
84. Select VNX from the Model drop-down list.
85. Select –BLOCK-A from the drop-down menu right of the serial number.
86. Enter <<var_mgmt_vnx_spb_ip>> as the IP Address.
87. Click OK.

**Figure 139 EMC SRS – Add Device, SPB for BLOCK**



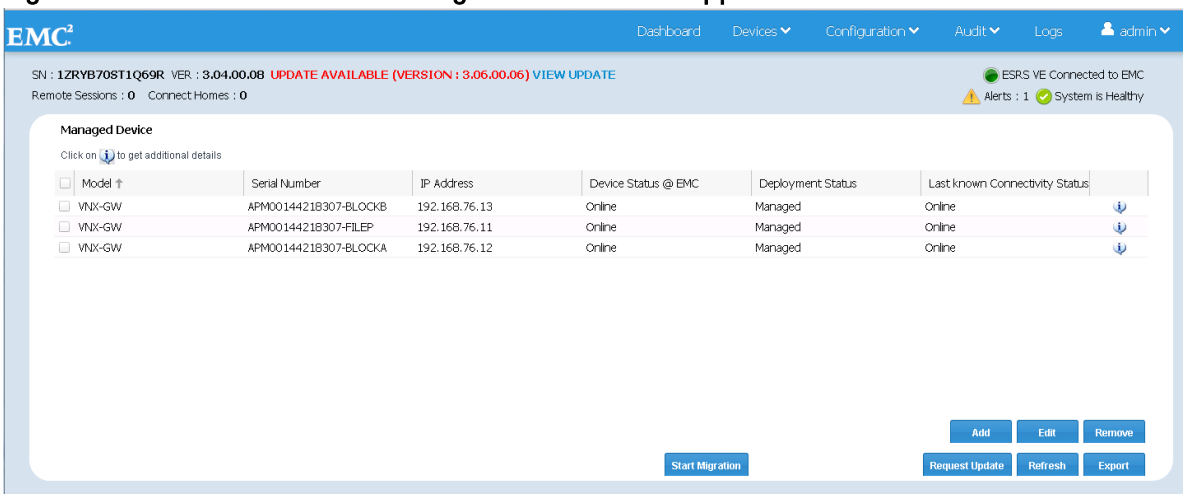

88. Click Request Update – The request to add this VNX to the configured Side is send to EMC for approval.
89. Click OK.

**Figure 140 EMC SRS – Request have been sent to EMC for approval**




90. Click Refresh to see if the request is approved from EMC.

**Figure 141 EMC SRS – List of Managed Devices after Approval**




The second part of the ESRS configuration is the RemotleyAnywhere section on the EMC VNX storage.

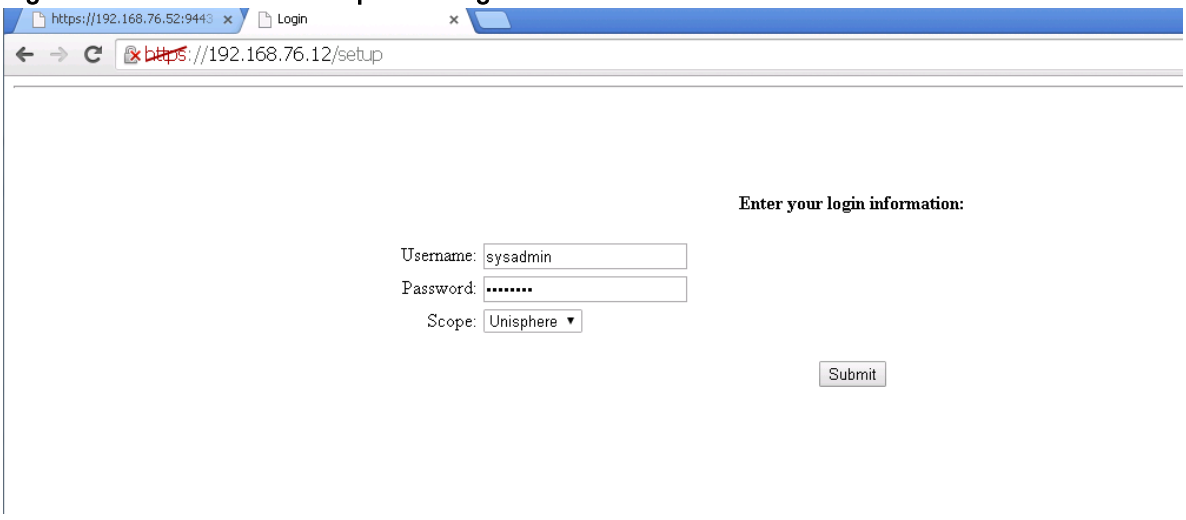
91. Open the page http://<<var_mgmt_vnx_spa_ip>>/setup in a web browser.

92. Enter <<var_mgmt_vnx_user>> as the Username.

93. Enter <<var_mgmt_vnx_passwd>> as the Password.

94. Click Submit.

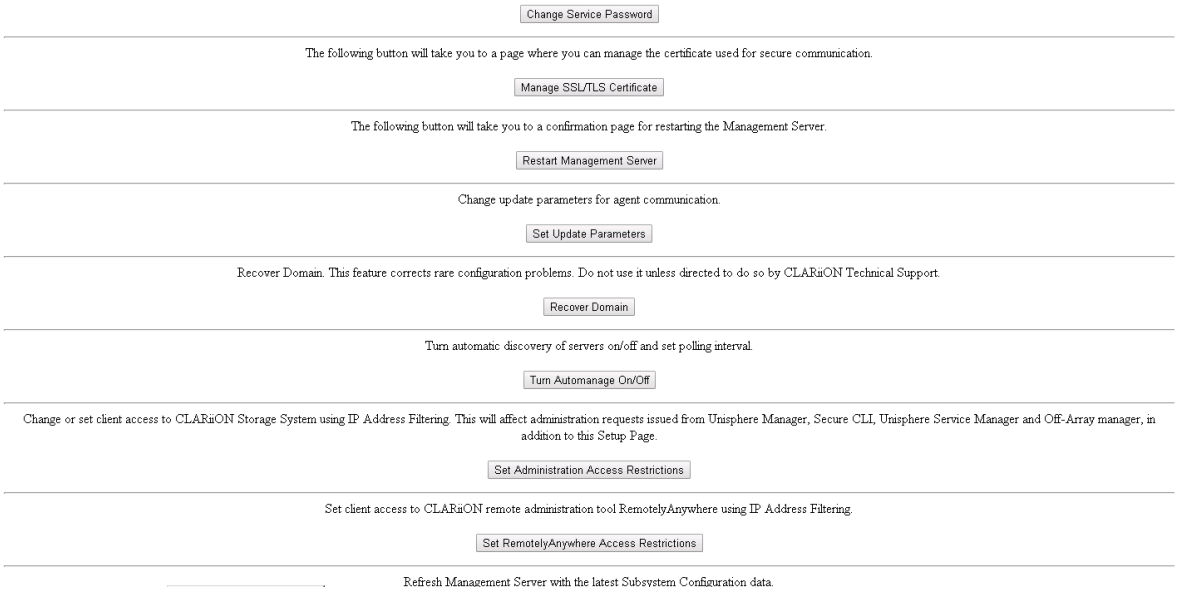
**Figure 142 EMC VNX – Setup Tool Login**




95. Scroll down to the end of the page.

96. Click Set RemotelyAnywhere Access Restrictions.

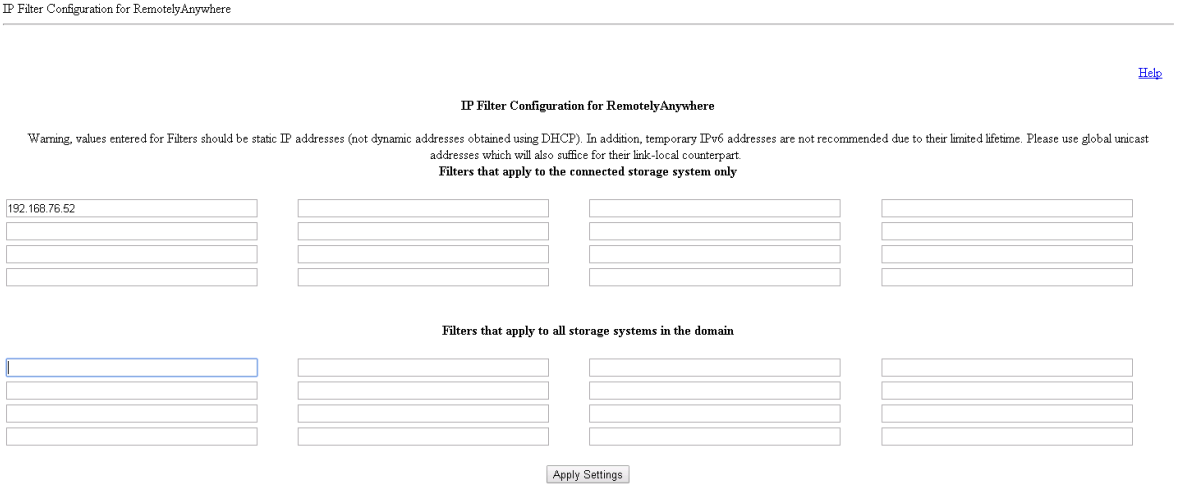
**Figure 143 EMC VNX – Setup Tool Home Screen**




97. Enter <<var_emcsrs_ip>> into an empty field in the Filters that apply to the connected storage system only section.

98. Click Apply Settings.

**Figure 144 EMC VNX – Setup Tool, RemotlyAnyway Access Restrictions**




99. Click Apply Settings.

Figure 145 EMC VNX – Setup Tool, Apply Settings




100. Click Logout.

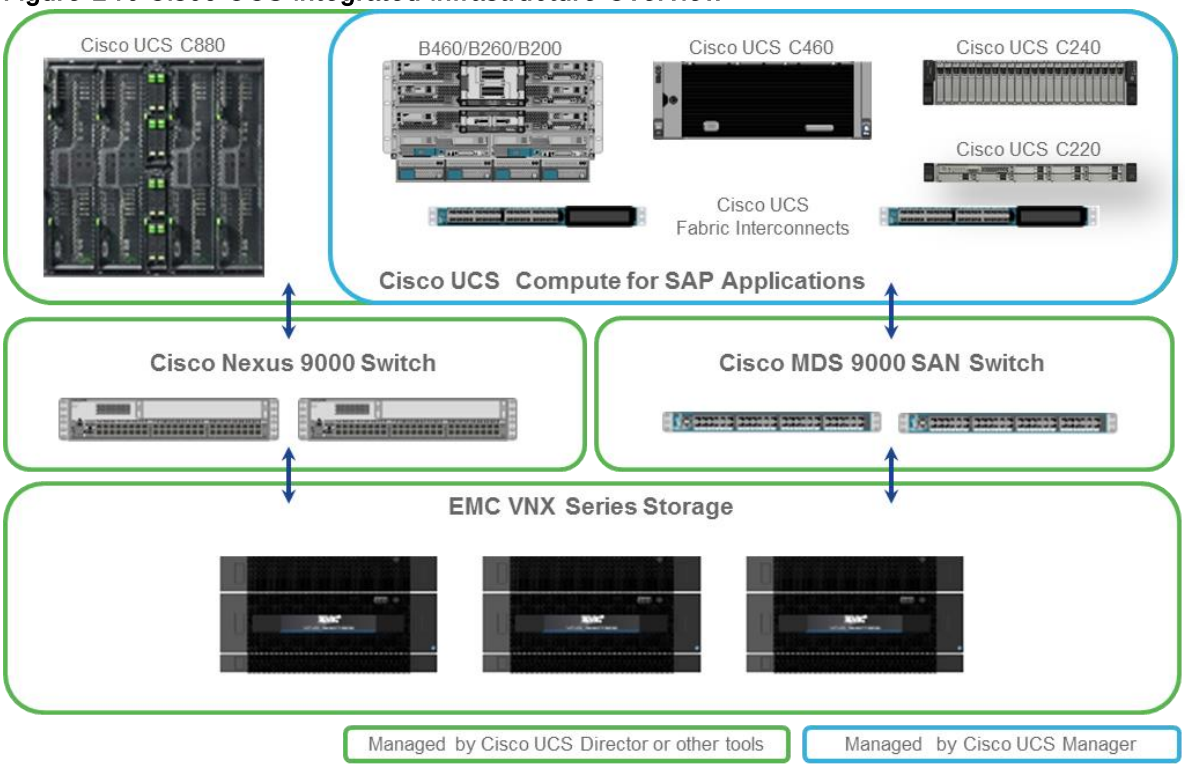
The configuration will be replicated to the SPB.

Verify with EMC service that the storage systems are listed and accessible.

# Install and Configure the Cisco UCS Integrated Infrastructure

The SAP HANA TDI option enables organizations to run multiple SAP HANA production and non-production systems on the same infrastructure. In this configuration, the existing servers used by different SAP HANA systems share the same network infrastructure and storage systems. In addition, SAP application server can share the same infrastructure with the SAP HANA database. With this configuration, the solution controls the communication between the application server and the database. This approach quarantines the bandwidth and latency for best performance and includes the application server and the SAP HANA database in the disaster-tolerance / disaster recovery solution.

**Figure 146 Cisco UCS Integrated Infrastructure Overview**




With the features available in Cisco Unified Computing System, it is possible to separate the network traffic between two different use cases by creating separate network uplink port channels. You can implement the VLAN groups' available in the Cisco UCS to map one or more VLANs to specific uplink port channels on the Fabric Interconnects.

For example, Create 2 port channels on each Cisco UCS Fabric-Interconnect:

- Port channel 11 and 13 are created on Fabric Interconnect A.
- Port channel 12 and 14 are created on Fabric Interconnect B.

In this example, you create a VLAN-Group for Administrative networks and add all the VLANs carrying traffic for Management and Administration in that VLAN-Group. You then force the VLAN group to use Port channel 11 on Fabric Interconnect A and Port channel 12 on Fabric Interconnect B.

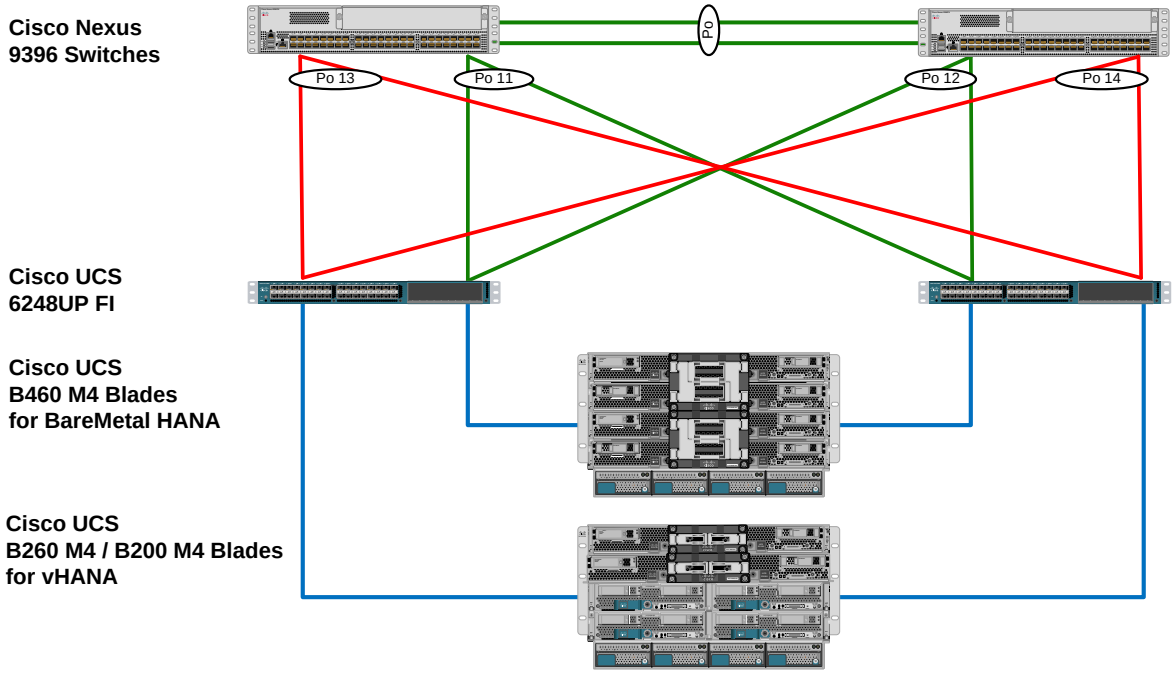
Similarly, you can create VLAN-Group for Application traffic and add all the VLANs carrying traffic for Applications in that VLAN-Group. Then force the VLAN group to use Port channel 13 on Fabric Interconnect A and Port channel 14 on Fabric Interconnect B.

With this approach no bandwidth is shared between Administrators and Applications. The bandwidth for the applications can be increased or decreased using the number of ports in the Port channel 13 and 14.



If the VLAN Groups are used to separate network traffic, it is important to know that only the VLANs from one VLAN Group are allowed per vNIC. It is recommended to use VLAN groups only where required, since this methodology can also be used in case the network traffic for tenant A must be separated from all other tenants.

**Figure 147 Network Separation of Multiple Systems using Port Channel and VLGroups**




The following sections detail the baseline configuration of all the involved components of one or two pieces per type, for example switch, server or storage. Detailed steps to add more components to the architecture are described later.

## Device Cabling

Table 20 lists the device cabling used in this example. This may differ in your setup as other combinations of server types and storages can be used.

## Cisco Nexus 9000 A

**Table 20 Cisco Nexus 9000 A Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco Nexus 9000 A | Eth1/1 | 10GbE | | |
| | Eth1/2 | 10GbE | | |
| | Eth1/3 | 10GbE | Cisco UCS 6248 A | 1/13 |
| | Eth1/4 | 10GbE | Cisco UCS 6248 B | 1/13 |
| | Eth1/5 | 10GbE | Cisco UCS 6248 A | 1/1 |
| | Eth1/6 | 10GbE | Cisco UCS 6248 A | 1/2 |
| | Eth1/9 | 10GbE | Cisco Nexus 9000 B | 1/9 |
| | Eth1/10 | 10GbE | Cisco Nexus 9000 B | 1/10 |
| | Eth1/11 | 10GbE | Cisco Nexus 9000 M1 | 1/5 |
| | Eth1/12 | 10GbE | Cisco Nexus 9000 M2 | 1/5 |
| | Eth1/13 | 10GbE | EMC VNX8000-1 DM2 | 0/0 |
| | Eth1/14 | 10GbE | EMC VNX8000-1 DM3 | 0/0 |
| | Eth1/15 | 10GbE | Cisco UCS 6248 B | 1/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/16 | 10GbE | Cisco UCS 6248 B | 1/2 |
| | Eth1/29 | 10GbE | Backup Destination | |
| | Eth1/30 | 10GbE | | |
| | Eth1/31 | 10GbE | Cisco C880-1 | 0/0 |
| | Eth1/32 | 10GbE | Cisco C880-1 | 1/0 |
| | MGMT0 | 1GbE | Cisco Nexus 9000 M1 | 1/21 |
| | CONS | Serial | Cisco 2911 ISR | 0/0/0 |

## Cisco Nexus 9000 B

**Table 21 Cisco Nexus 9000 B Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco Nexus 9000 B | Eth1/1 | 10GbE | | |
| | Eth1/2 | 10GbE | | |
| | Eth1/3 | 10GbE | Cisco UCS 6248 A | 1/15 |
| | Eth1/4 | 10GbE | Cisco UCS 6248 B | 1/15 |
| | Eth1/5 | 10GbE | Cisco UCS 6248 A | 1/5 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/6 | 10GbE | Cisco UCS 6248 A | 1/6 |
| | Eth1/9 | 10GbE | Cisco Nexus 9000 A | 1/9 |
| | Eth1/10 | 10GbE | Cisco Nexus 9000 B | 1/10 |
| | Eth1/11 | 10GbE | Cisco Nexus 9000 M1 | 1/6 |
| | Eth1/12 | 10GbE | Cisco Nexus 9000 M2 | 1/6 |
| | Eth1/13 | 10GbE | EMC VNX8000-1 DM2 | 0/1 |
| | Eth1/14 | 10GbE | EMC VNX8000-1 DM3 | 0/1 |
| | Eth1/15 | 10GbE | Cisco UCS 6248 B | 1/5 |
| | Eth1/16 | 10GbE | Cisco UCS 6248 B | 1/6 |
| | Eth1/29 | 10GbE | Backup Destination | |
| | Eth1/30 | 10GbE | | |
| | Eth1/31 | 10GbE | Cisco C880-1 | 0/1 |
| | Eth1/32 | 10GbE | Cisco C880-1 | 1/1 |
| | MGMT0 | 1GbE | Cisco Nexus 9000 M2 | 1/21 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | CONS | Serial | Cisco 2911 ISR | 0/0/1 |

## Cisco MDS 9148 A

**Table 22 Cisco MDS 9148 A Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco MDS 9148 A | FC1/1 | 8 Gbps | Cisco UCS 6248 A | FC1/25 |
| | FC 1/2 | 8 Gbps | Cisco UCS 6248 A | FC1/26 |
| | FC 1/3 | 8 Gbps | Cisco UCS 6248 A | FC1/27 |
| | FC 1/4 | 8 Gbps | Cisco UCS 6248 A | FC1/28 |
| | FC 1/5 | 8 Gbps | Cisco UCS 6248 A | FC1/29 |
| | FC 1/6 | 8 Gbps | Cisco UCS 6248 A | FC1/30 |
| | FC 1/7 | 8 Gbps | Cisco UCS 6248 A | FC1/31 |
| | FC 1/8 | 8 Gbps | Cisco UCS 6248 A | FC1/32 |
| | FC 1/25 | 8 Gbps | EMC VNX8000-A SPA | 0/0 |
| | FC 1/26 | 8 Gbps | EMC VNX8000-A SPB | 0/0 |
| | FC 1/27 | 8 Gbps | EMC VNX8000-A SPA | 0/1 |
| | FC | 8 Gbps | EMC VNX8000-A SPB | 0/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | 1/28 | | | |
| | FC 1/29 | 8 Gbps | EMC VNX8000-A SPA | 0/2 |
| | FC 1/30 | 8 Gbps | EMC VNX8000-A SPB | 0/2 |
| | FC 1/31 | 8 Gbps | EMC VNX8000-A SPA | 0/3 |
| | FC 1/32 | 8 Gbps | EMC VNX8000-A SPB | 0/3 |
| | FC 1/47 | 8 Gbps | Cisco C880-1 | 0/0 |
| | FC 1/48 | 8 Gbps | Cisco C880-1 | 1/0 |
| | MGMT0 | 1GbE | Cisco Nexus 9000 M1 | 1/22 |
| | CONS | Serial | Cisco 2911 ISR | 0/0/4 |

## Cisco MDS 9148 B

**Table 23 Cisco MDS 9148 B Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco MDS 9148 B | FC1/1 | 8 Gbps | Cisco UCS 6248 B | FC1/25 |
| | FC 1/2 | 8 Gbps | Cisco UCS 6248 B | FC1/26 |
| | FC 1/3 | 8 Gbps | Cisco UCS 6248 B | FC1/27 |
| | FC 1/4 | 8 Gbps | Cisco UCS 6248 B | FC1/28 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | FC 1/5 | 8 Gbps | Cisco UCS 6248 B | FC1/29 |
| | FC 1/6 | 8 Gbps | Cisco UCS 6248 B | FC1/30 |
| | FC 1/7 | 8 Gbps | Cisco UCS 6248 B | FC1/31 |
| | FC 1/8 | 8 Gbps | Cisco UCS 6248 B | FC1/32 |
| | FC 1/25 | 8 Gbps | EMC VNX8000-A SP A | 2/0 |
| | FC 1/26 | 8 Gbps | EMC VNX8000-A SP B | 2/0 |
| | FC 1/27 | 8 Gbps | EMC VNX8000-A SP A | 2/1 |
| | FC 1/28 | 8 Gbps | EMC VNX8000-A SP B | 2/1 |
| | FC 1/29 | 8 Gbps | EMC VNX8000-A SP A | 2/2 |
| | FC 1/30 | 8 Gbps | EMC VNX8000-A SP B | 2/2 |
| | FC 1/31 | 8 Gbps | EMC VNX8000-A SP A | 2/3 |
| | FC 1/32 | 8 Gbps | EMC VNX8000-A SP B | 2/3 |
| | FC 1/47 | 8 Gbps | Cisco C880-1 | 0/1 |
| | FC 1/48 | 8 Gbps | Cisco C880-1 | 1/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | MGMT0 | 1GbE | Cisco Nexus 9000 M2 | 1/22 |
| | CONS | Serial | Cisco 2911 ISR | 0/0/5 |

## Cisco UCS 6248 A

**Table 24 Cisco UCS 6248 A Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco UCS 6248 A | Eth1/1 | 10GbE | Cisco Nexus 9000 A | 1/5 |
| | Eth1/2 | 10GbE | Cisco Nexus 9000 A | 1/6 |
| | Eth1/5 | 10GbE | Cisco Nexus 9000 B | 1/5 |
| | Eth1/6 | 10GbE | Cisco Nexus 9000 B | 1/6 |
| | Eth1/9 | 10GbE | Cisco UCS C240M4-1 | 2/1 |
| | Eth1/10 | 10GbE | Cisco UCS C220M4-1 | MLOM1 |
| | Eth1/11 | 10GbE | Cisco UCS C460M4-1 | 4/1 |
| | Eth1/12 | 10GbE | Cisco UCS C460M4-1 | 9/1 |
| | Eth1/13 | 10GbE | Cisco Nexus 9000 A | 1/13 |
| | Eth1/15 | 10GbE | Cisco Nexus 9000 B | 1/13 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/17 | 10GbE | Cisco UCS 5108-1 | A0 |
| | Eth1/18 | 10GbE | Cisco UCS 5108-1 | A1 |
| | Eth1/19 | 10GbE | Cisco UCS 5108-1 | A2 |
| | Eth1/20 | 10GbE | Cisco UCS 5108-1 | A3 |
| | Eth1/21 | 10GbE | Cisco UCS 5108-2 | A0 |
| | Eth1/22 | 10GbE | Cisco UCS 5108-2 | A1 |
| | Eth1/23 | 10GbE | Cisco UCS 5108-2 | A2 |
| | Eth1/24 | 10GbE | Cisco UCS 5108-2 | A3 |
| | FC1/25 | 8 Gbps | MDS 9148S A | FC1/1 |
| | FC1/26 | 8 Gbps | MDS 9148S A | FC1/2 |
| | FC1/27 | 8 Gbps | MDS 9148S A | FC1/3 |
| | FC1/28 | 8 Gbps | MDS 9148S A | FC1/4 |
| | FC1/29 | 8 Gbps | MDS 9148S A | FC1/5 |
| | FC1/30 | 8 Gbps | MDS 9148S A | FC1/6 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | FC1/31 | 8 Gbps | MDS 9148S A | FC1/7 |
| | FC1/32 | 8 Gbps | MDS 9148S A | FC1/8 |
| | MGMT0 | 1GbE | Cisco Nexus 9000 M1 | 1/20 |
| | CONS | Serial | Cisco 2911 ISR | 0/0/2 |

## Cisco UCS 6248 B

**Table 25 Cisco UCS 6248 B Cabling**

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco UCS 6248 B | Eth1/1 | 10GbE | Cisco Nexus 9000 A | 1/15 |
| | Eth1/2 | 10GbE | Cisco Nexus 9000 A | 1/16 |
| | Eth1/5 | 10GbE | Cisco Nexus 9000 B | 1/15 |
| | Eth1/6 | 10GbE | Cisco Nexus 9000 B | 1/16 |
| | Eth1/9 | 10GbE | Cisco UCS C240M4-1 | 2/2 |
| | Eth1/10 | 10GbE | Cisco UCS C220M4-1 | MLOM2 |
| | Eth1/11 | 10GbE | Cisco UCS C460M4-1 | 4/2 |
| | Eth1/12 | 10GbE | Cisco UCS C460M4-1 | 9/2 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | Eth1/13 | 10GbE | Cisco Nexus 9000 A | 1/4 |
| | Eth1/15 | 10GbE | Cisco Nexus 9000 B | 1/4 |
| | Eth1/17 | 10GbE | Cisco UCS 5108-1 | B0 |
| | Eth1/18 | 10GbE | Cisco UCS 5108-1 | B1 |
| | Eth1/19 | 10GbE | Cisco UCS 5108-1 | B2 |
| | Eth1/20 | 10GbE | Cisco UCS 5108-1 | B3 |
| | Eth1/21 | 10GbE | Cisco UCS 5108-2 | B0 |
| | Eth1/22 | 10GbE | Cisco UCS 5108-2 | B1 |
| | Eth1/23 | 10GbE | Cisco UCS 5108-2 | B2 |
| | Eth1/24 | 10GbE | Cisco UCS 5108-2 | B3 |
| | FC1/25 | 8 Gbps | MDS 9148S B | FC1/1 |
| | FC1/26 | 8 Gbps | MDS 9148S B | FC1/2 |
| | FC1/27 | 8 Gbps | MDS 9148S B | FC1/3 |
| | FC1/28 | 8 Gbps | MDS 9148S B | FC1/4 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| | FC1/29 | 8 Gbps | MDS 9148S B | FC1/5 |
| | FC1/30 | 8 Gbps | MDS 9148S B | FC1/6 |
| | FC1/31 | 8 Gbps | MDS 9148S B | FC1/7 |
| | FC1/32 | 8 Gbps | MDS 9148S B | FC1/8 |
| | MGMT0 | 1GbE | Cisco Nexus 9000 M2 | 1/20 |
| | CONS | Serial | Cisco 2911 ISR | 0/0/3 |

## Cisco Nexus 9000 Configuration

Table 26 lists the required information to set up the Cisco Nexus 9000 switches in this Cisco UCS Integrated Infrastructure for SAP HANA.

**Table 26 Information to Setup Cisco Nexus Switches in the Reference Architecture**

| Name | Variable |
|---|---|
| Global default administrative password | <<var_mgmt_passwd>> |
| SNMP Community String for Read Only access | <<var_snmp_ro_string>> |
| Nexus 9000 A hostname | <<var_nexus_A_hostname>> |
| Nexus 9000 A Management IP Address | <<var_nexus_A_mgmt0_ip>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| Nexus 9000 B hostname | <<var_nexus_B_hostname>> |
| Nexus 9000 B Management IP Address | <<var_nexus_B_mgmt0_ip>> |
| Infrastructure Management Network VLAN ID | <<var_management_vlan_id>> |

| Name | Variable |
|---|---|
| Global Administration Network VLAN ID | <<var_admin_vlan_id>> |
| Global Backup Network | <<var_backup_vlan_id>> |
| VMware Vmotion Network VLAN ID | <<var_vmotion_vlan_id>> |
| VMware ESX Storage access Network VLAN ID | <<var_esx_nfs_vlan_id>> |
| Virtual Port Channel Domain ID for N9K A and B | <<var_nexus_vpc_domain_id>> |
| | <<var_ucs_clustername>> |
| | <<var_backup_node01>> |
| | |

## Initial Cisco Nexus 9000 Configuration

These steps provide details for the initial Cisco Nexus 9000 Switch setup.

### Cisco Nexus A

To set up the initial configuration for the first Cisco Nexus switch complete the following steps:



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes


         ---- System Admin Account Setup ----


Do you want to enforce secure password standard (yes/no) [y]: yes

  Enter the password for "admin": <<var_mgmt_passwd>>
  Confirm the password for "admin": <<var_mgmt_passwd>>

         ---- Basic System Configuration Dialog VDC: 1 ----
```

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes



  Create another login account (yes/no) [n]:

  Configure read-only SNMP community string (yes/no) [n]: y

    SNMP community string : <<var_snmp_ro_string>>

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : <<var_nexus_A_hostname>>

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address : <<var_nexus_A_mgmt0_ip>>
```

```
    Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>

  Configure the default gateway? (yes/no) [y]:

    IPv4 address of the default gateway : <<var_mgmt_gw>>

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]:

  Enable the ssh service? (yes/no) [y]:

    Type of ssh key you would like to generate (dsa/rsa) [rsa]:

    Number of rsa key bits <1024-2048> [2048]:

  Configure the ntp server? (yes/no) [n]: y

    NTP server IPv4 address : <<var_global_ntp_server_ip>>

  Configure default interface layer (L3/L2) [L2]:

  Configure default switchport interface state (shut/noshut) [noshut]:

  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:


The following configuration will be applied:
  password strength-check
  snmp-server community monitor ro
  switchname <<var_nexus_A_hostname>>
```

```
vrf context management
ip route 0.0.0.0/0 <<var_mgmt_gw>>
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server <<var_global_ntp_server_ip>>
  system default switchport
  no system default switchport shutdown
  copp profile strict
interface mgmt0
ip address <<var_nexus_A_mgmt0_ip>> <<var_mgmt_netmask>>
no shutdown

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

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

[########################################] 100%
Copy complete.
```

### Cisco Nexus B

To set up the initial configuration for the second Cisco Nexus switch complete the following steps:



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes


         ---- System Admin Account Setup ----
```

```
Do you want to enforce secure password standard (yes/no) [y]: yes

  Enter the password for "admin": <<var_mgmt_passwd>>
  Confirm the password for "admin": <<var_mgmt_passwd>>

         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes



  Create another login account (yes/no) [n]:

  Configure read-only SNMP community string (yes/no) [n]: y

    SNMP community string : <<var_snmp_ro_string>>

  Configure read-write SNMP community string (yes/no) [n]:
```

```
Enter the switch name : <<var_nexus_B_hostname>>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

  Mgmt0 IPv4 address : <<var_nexus_B_mgmt0_ip>>

  Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>

Configure the default gateway? (yes/no) [y]:

  IPv4 address of the default gateway : <<var_mgmt_gw>>

Configure advanced IP options? (yes/no) [n]:

Enable the telnet service? (yes/no) [n]:

Enable the ssh service? (yes/no) [y]:

  Type of ssh key you would like to generate (dsa/rsa) [rsa]:

  Number of rsa key bits <1024-2048> [2048]:

Configure the ntp server? (yes/no) [n]:   y

  NTP server IPv4 address : <<var_global_ntp_server_ip>>

Configure default interface layer (L3/L2) [L3]: L2

Configure default switchport interface state (shut/noshut) [shut]:   Enter
```

```
  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:
The following configuration will be applied:
  password strength-check
  switchname <<var_nexus_B_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_mgmt_gw>>
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server <<var_global_ntp_server_ip>>
  system default switchport
  no system default switchport shutdown
  copp profile strict
interface mgmt0
ip address <<var_nexus_B_mgmt0_ip>> <<var_mgmt_netmask>>
no shutdown

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

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

[########################################] 100%
Copy complete.
```

Verify the configuration with the following commands. The ping destination in this example is the management port of Nexus 9000 B:

```
CRA-N9K-A# show int bri

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
```

```
--------------------------------------------------------------------------------
mgmt0  --            up     192.168.76.1                              1000     1500


CRA-N9K-A# ping 192.168.76.2 vrf management
PING 192.168.76.2 (192.168.76.2): 56 data bytes
64 bytes from 192.168.76.2: icmp_seq=0 ttl=254 time=0.375 ms
64 bytes from 192.168.76.2: icmp_seq=1 ttl=254 time=0.245 ms
64 bytes from 192.168.76.2: icmp_seq=2 ttl=254 time=0.236 ms
64 bytes from 192.168.76.2: icmp_seq=3 ttl=254 time=0.212 ms
64 bytes from 192.168.76.2: icmp_seq=4 ttl=254 time=0.218 ms

--- 192.168.76.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.212/0.257/0.375 ms
CRA-N9K-A#
```

## Enable the Appropriate Cisco Nexus 9000 Features and Settings

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

The following commands enable the IP switching feature and set the default spanning tree behaviors.

On each Nexus 9000, enter the configuration mode:

```
config terminal
```

Use the following commands to enable the necessary features:

```
feature udld

feature lacp

feature vpc
feature interface-vlan
feature lldp
```

## Configure the Spanning Tree Defaults

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

The following commands set the default spanning tree behaviors.

On each Cisco Nexus 9000, enter configuration mode:

```
config terminal

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
```

Save the running configuration to start-up:

```
copy run start
```

## Create VLANs for Management and ESX Traffic

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following step on both switches.

From the configuration mode, run the following commands:

```
vlan <<var_management_vlan_id>>
name Infrastructure-Management


vlan <<var_temp_vlan_id>>
name Temporary-VLAN



vlan <<var_admin_vlan_id>>

name Global-Admin-Network


vlan <<var_backup_vlan_id>>

name Global-Backup-Network


vlan <<var_vmotion_vlan_id>>

name vMotion-Network


vlan <<var_esx_nfs_vlan_id>>

name ESX-NFS_Datastore-Network
```

Save the running configuration to start-up:

```
copy run start
```

Validate the VLAN configuration:

```
show vlan bri
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Eth1/1, Eth1/2, Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                 Eth1/9, Eth1/10, Eth1/11
                                                 Eth1/12, Eth1/13, Eth1/14
                                                 Eth1/15, Eth1/16, Eth1/17
                                                 Eth1/18, Eth1/19, Eth1/20
                                                 Eth1/21, Eth1/22, Eth1/23
                                                 Eth1/24, Eth1/25, Eth1/26
                                                 Eth1/27, Eth1/28, Eth1/29
                                                 Eth1/30, Eth1/31, Eth1/32
                                                 Eth1/33, Eth1/34, Eth1/35
                                                 Eth1/36, Eth1/37, Eth1/38
                                                 Eth1/39, Eth1/40, Eth1/41
                                                 Eth1/42, Eth1/43, Eth1/44
                                                 Eth1/45, Eth1/46, Eth1/47
                                                 Eth1/48, Eth2/1, Eth2/2, Eth2/3
                                                 Eth2/4, Eth2/5, Eth2/6, Eth2/7
                                                 Eth2/8, Eth2/9, Eth2/10, Eth2/11
                                                 Eth2/12
2    Temorary-VLAN                     active
76   Infrastructure-Management         active
177  Global-Admin-Network              active
199  Global-Backup-Network             active
2031 vMotion-Network                   active
2034 ESX-NFS_Datastore-Network         active
```

## Configure Virtual Port Channel Domain

The 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.

### Cisco Nexus 9000 A

To configure virtual port channels (vPCs) for switch A, complete the following steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make Nexus 9000A the primary vPC peer by defining a low priority value:

```
role priority 10
```

3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_B_mgmt0_ip>>  source
<<var_nexus_A_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
peer-switch

delay restore 150

peer-gateway

auto-recovery
```

5. Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

To configure vPCs for switch B, complete the following step:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make Cisco Nexus 9000 B the secondary vPC peer by defining a higher priority value than that of the Nexus 9000 A:

```
role priority 20
```

3. Use the management interfaces on the supervisors of the Cisco Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_A_mgmt0_ip>>  source
<<var_nexus_B_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
peer-switch

delay restore 150
```

```
peer-gateway

auto-recovery
```

5. Save the running configuration to start-up:

```
copy run start
```

## Configure Network Interfaces for the VPC Peer Links

### Cisco Nexus 9000 A

1. Define a port description for the interfaces connecting to VPC Peer <<var_nexus_B_hostname>>.

```
interface Eth1/9

description VPC Peer <<var_nexus_B_hostname>>:1/9


interface Eth1/10

description VPC Peer <<var_nexus_B_hostname>>:1/10
```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```
interface Eth1/9-10

channel-group 1 mode active

no shutdown
```

3. Define a description for the port channel connecting to <<var_nexus_B_hostname>>.

```
interface Po1

description vPC peer-link
```

4. Make the port channel a switchport, and configure a trunk to allow multiple VLANs.

```
switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

5. Make this port channel the VPC peer link and bring it up.

```
spanning-tree port type network

vpc peer-link

no shutdown
```

6. Save the running configuration to start-up.

```
copy run start
```

### Cisco Nexus 9000 B

1. Define a port description for the interfaces connecting to VPC peer <<var_nexus_A_hostname>>.

```
interface Eth1/9
description VPC Peer <<var_nexus_A_hostname>>:1/9

interface Eth1/10
description VPC Peer <<var_nexus_A_hostname>>:1/10
```

2. Apply a port channel to both VPC peer links and bring up the interfaces.

```
interface Eth1/9-10
channel-group 1 mode active
no shutdown
```

3. Define a description for the port channel connecting to <<var_nexus_A_hostname>>.

```
interface Po1
description vPC peer-link
```

4. Make the port channel a switchport and configure a trunk to allow multiple VLANs.

```
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_management_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

5. Make this port channel the VPC peer link and bring it up.

```
spanning-tree port type network
vpc peer-link
no shutdown
```

6. Save the running configuration to start-up.

```
copy run start
```

7. To Verify the VPC configuration, in this example vPC ID 63, you can run the following commands:

```
CRA-N9K-A# show vpc
Legend:
```

```
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 63
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 1
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,2031,2034

CRA-N9K-A#



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

vPC domain id                     : 63
Peer status                       : peer adjacency formed ok
```

```
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 1
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)


vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,2031,2034


CRA-N9K-B#
```

## Configure Network Interfaces to Connect the EMC VNX Storage

From each N9K switch 2 link connects to each Data Mover on the VNX storage array. A virtual port channel is created for the two links connected to a single Data Mover, but connected to two different switches. In this example configuration, links connected to Data mover-2 of VNX storage array are connected to Ethernet port 1/13 on each switch and links connected to Data mover-3 are connected to Ethernet port 1/14 on each switch. A virtual port channel (id 33) is created for port Ethernet 1/13 on each switch and a different virtual port channel (id 34) is created for port Ethernet 1/14 on each switch. Note that only a storage VLAN is required on this port, therefore the port is in access mode. This section details the configuration on the port channels and interfaces.

### Cisco Nexus 9000 A

1. Define a port description for the interface connecting to EMC-VNX5400-M1:

```
interface Eth1/13
description EMC-VNX-A-DM2:0/0
```

```
interface Eth1/14
description EMC-VNX-A-DM3:0/0

Define the port channel
interface Po33
description EMC-VNX-A-DM2-vPC

interface Po34
description EMC-VNX-A-DM3-vPC
```

2. Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/13
channel-group 33 mode active
no shutdown

interface eth1/14
channel-group 34 mode active
no shutdown
```

3. Make the port channel a switchport, and configure a trunk to allow NFS VLANs:

```
interface Po33
switchport
switchport mode trunk
switchport trun allowed vlan <<var_esx_nfs_vlan_id>>,<<var_management_vlan_id>>

interface Po34
switchport
switchport mode trunk
switchport trun allowed vlan <<var_esx_nfs_vlan_id>>,<<var_management_vlan_id>>
```

4. Set the MTU to be 9216 to support jumbo frames:

```
interface Po33
mtu 9216

interface Po34
mtu 9216
```

5. Make this port channel a VPC and bring it up:

```
interface Po33
spanning-tree port type edge trunk
vpc 33
no shutdown

interface Po34
spanning-tree port type edge trunk
vpc 34
no shutdown
```

6. Save the running configuration to start-up:

```
copy run start
Cisco Nexus 9000 B
Define a port description for the interface connecting to EMC-VNX5400-M1
interface Eth1/13
description EMC-VNX-A-DM2:0/0

interface Eth1/14
description EMC-VNX-A-DM3:0/0
```

7. Define the port channel:

```
interface Po33
description EMC-VNX-A-DM2-vPC
```

```
interface Po34
description EMC-VNX-A-DM3-vPC
```

8. Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/13
channel-group 33 mode active
no shutdown

interface eth1/14
channel-group 34 mode active
no shutdown
```

9. Make the port channel a switchport, and configure a trunk to allow NFS VLANs:

```
interface Po33
switchport
switchport mode trunk
switchport trun allowed vlan <<var_esx_nfs_vlan_id>>,<<var_management_vlan_id>>

interface Po34
switchport
switchport mode trunk
switchport trun allowed vlan <<var_esx_ nfs_vlan_id>>,<<var_management_vlan_id>>
```

10. Set the MTU to be 9216 to support jumbo frames:

```
interface Po33
mtu 9216

interface Po34
mtu 9216
```

11. Make this port channel a VPC and bring it up:

```
interface Po33
spanning-tree port type edge trunk
vpc 33
```

```
no shutdown

interface Po34
spanning-tree port type edge trunk
vpc 34
no shutdown
```

12. Save the running configuration to start-up:

```
copy run start
```

13. To Verify the VPC configuration, in this example VPC 33 and 34, run the following commands:

```
cra-n9k-a# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 25
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 inconsistency reason       : Consistency Check Not Performed
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
```

```
1    Po1    up     -


vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
33   Po33   down*  success     success                    -


34   Po34   down*  success     success                    -


cra-n9k-a#
```

## Configure Network Interfaces for Access to the Management Landscape

The port connected to the management network needs to be in trunk mode and it requires the infrastructure VLAN as part of the allowed VLANs list. Depending on your requirements, you may need to enable more VLANs for your applications For example, a Windows virtual machine may need to access the active directory / DNS servers deployed in the management network. You may also want to enable the port channels and virtual port channels for the high availability of the infrastructure network.

The following is an example of configuration for the Network Ports connected to the Nexus 9000 switches of the management infrastructure.

### Cisco Nexus 9000 A

To enable access to the management infrastructure, complete the following steps:

1. Define a port description for the interface connecting to the management switch:

```
interface eth1/11
description Aceess-POD1-N9000-M1:Eth1/5

interface eth1/12
description Aceess-POD1-N9000-M2:Eth1/5
```

2. Define a description for the port channel:

```
interface Po44
description Management-POD-vPC
```

3. Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/11-12

channel-group 44 mode active

no shutdown
```

4. Make the port channel a switchport and configure a trunk to allow management VLANs:

```
interface Po44

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_backup_vlan_id>>
```

5. Set the MTU to be 9216 to support jumbo frames:

```
interface Po44

mtu 9216
```

6. Make this port channel a VPC and bring it up:

```
interface Po44

spanning-tree port type network

vpc 44

no shutdown
```

7. Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

To enable access to the management infrastructure, complete the following steps:

1. Define a port description for the interface connecting to the management switch:

```
interface eth1/11

description Aceess-POD1-N9000-M1:Eth1/6


interface eth1/12

description Aceess-POD1-N9000-M2:Eth1/6
```

2. Define a description for the port channel:

```
interface Po44

description Management-POD-vPC
```

3. Apply a port channel to both VPC peer links and bring up the interfaces:

```
interface eth1/11-12

channel-group 44 mode active

no shutdown
```

4. Make the port channel a switchport, and configure a trunk to allow management VLANs:

```
interface Po44

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_backup_vlan_id>>
```

5. Set the MTU to be 9216 to support jumbo frames:

```
interface Po44

mtu 9216
```

6. Make this port channel a VPC and bring it up:

```
interface Po44

spanning-tree port type network

vpc 44

no shutdown
```

7. Save the running configuration to start-up:

```
copy run start
```

8. To Verify the VPC configuration, in this example vPC 44, run the following commands:

```
CRA-N9K-A# show vpc 44



vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
44   Po44   up     success     success                    76,177,199
CRA-N9K-A# show int bri
```

```
--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     192.168.76.1                            1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Por
t
Interface                                                                    Ch
#
--------------------------------------------------------------------------------
…
…
Eth1/11       1       eth  trunk  up      none                       10G(D) 44
Eth1/12       1       eth  trunk  up      none                       10G(D) 44
…
…
CRA-N9K-A#

CRA-N9K-B# show vpc 44


vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                Active vlans
--   ----   ------ ----------- ------                ------------
44   Po44   up     success     success               76,177,199
CRA-N9K-B# show int bri

--------------------------------------------------------------------------------
```

```
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     192.168.76.2                            1000     1500


--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Por
t
Interface                                                                    Ch
#
--------------------------------------------------------------------------------
…
…
Eth1/11       1       eth  trunk  up      none                       10G(D) 44
Eth1/12       1       eth  trunk  up      none                       10G(D) 44
…
…


CRA-N9K-B#
```

## Configure Administration Port Channels to Cisco UCS Fabric Interconnect

For management traffic, a separate port channel is used within the Cisco UCS domain. This option enables a dedicated bandwidth for administration tasks and application traffic.

### Cisco Nexus 9000 A

Define a description for the port channel connecting to <<var_ucs_clustername>>-A:

```
interface Po11
description <<var_ucs_clustername>>-A
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-A:

```
interface Eth1/3
description <<var_ucs_clustername>>-A:1/13
```

Apply it to a port channel and bring up the interface:

```
interface eth1/3
channel-group 11 mode active
```

```
no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po11

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 11

no shutdown
```

Define a description for the port channel connecting to <<var_ucs_clustername>>-B:

```
interface Po12

description <<var_ucs_clustername>>-B
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-B:

```
interface Eth1/4

description <<var_ucs_clustername>>-B:1/13
```

Apply it to a port channel and bring up the interface:

```
interface Eth1/4

channel-group 12 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po12

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 12

no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

Define a description for the port channel connecting to <<var_ucs_clustername>>-A:

```
interface Po11

description <<var_ucs_clustername>>-A
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-A:

```
interface Eth1/3

description <<var_ucs_clustername>>-A:1/15
```

Apply it to a port channel and bring up the interface:

```
interface eth1/3
channel-group 11 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po11

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up

```
vpc 11

no shutdown
```

Define a description for the port channel connecting to <<var_ucs_clustername>>-B:

```
interface Po12

description <<var_ucs_clustername>>-B
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-B:

```
interface Eth1/4

description <<var_ucs_clustername>>-B:1/15
```

Apply it to a port channel and bring up the interface:

```
interface Eth1/4

channel-group 12 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po12

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 12

no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

To Verify the VPC configuration, in this example vPC 11 and 12, run the following commands:

```
CRA-N9K-A# show vpc 11



vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
11   Po11   down*  success     success                    -

CRA-N9K-A# show vpc 12



vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
12   Po12   down*  success     success                    -


CRA-N9K-B# show vpc 11



vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
11   Po11   down*  Not         Consistency Check Not      -
                   Applicable  Performed

CRA-N9K-B# show vpc 12
```

```
vPC status
----------------------------------------------------------------------------
id    Port    Status Consistency Reason                     Active vlans
--    ----    ------ ----------- ------                     ------------
12    Po12    down*  Not         Consistency Check Not      -
                     Applicable  Performed
```



Since the ports on the Cisco UCS Fabric Interconnects are not configured yet, the Status is shown as "down" and there are no active VLANs.

## Configure Port Channels Connected to Cisco UCS Fabric Interconnects

The interfaces connected to the fabric interconnects need to be in the trunk mode; storage, vMotion, infra, and application VLANs are allowed on this port. On the switch side, interfaces connected to FI-A and FI-B are in a vPC, and from the FI side the links connected to Nexus 9396 A and B switches are in regular LACP port channels. It is a good practice to use a specific description for each port and port channel on the switch for a better diagnosis, if any problems arise later. Refer to section Cisco Nexus 9000 A for the exact configuration commands for Nexus 9K switch A and B.

### Cisco Nexus 9000 A

Define a description for the port channel connecting to <<var_ucs_clustername>>-A:

```
interface Po13

description <<var_ucs_clustername>>-A-Appl
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-A:

```
interface Eth1/5

description <<var_ucs_clustername>>-A:1/1

interface Eth1/6

description <<var_ucs_clustername>>-A:1/2
```

Apply it to a port channel and bring up the interface:

```
interface eth1/5-6
channel-group 13 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po13

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_temp_vlan_id>>

switchport trunk native vlan <<var_temp_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 13

no shutdown
```

Define a description for the port channel connecting to <<var_ucs_clustername>>-B:

```
interface Po14

description <<var_ucs_clustername>>-B-Appl
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-B:

```
interface Eth1/15

description <<var_ucs_clustername>>-B:1/1


interface Eth1/16

description <<var_ucs_clustername>>-B:1/2
```

Apply it to a port channel and bring up the interface:

```
interface Eth1/15-16

channel-group 14 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

interface Po14

```
switchport
switchport mode trunk
```

```
switchport trunk allowed vlan <<var_temp_vlan_id>>

switchport trunk native vlan <<var_temp_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 14

no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

Define a description for the port channel connecting to <<var_ucs_clustername>>-A:

```
interface Po13

description <<var_ucs_clustername>>-A-Appl
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-A:

```
interface Eth1/5

description <<var_ucs_clustername>>-A:1/5

interface Eth1/6

description <<var_ucs_clustername>>-A:1/6
```

Apply it to a port channel and bring up the interface:

```
interface eth1/5-6
channel-group 13 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po13

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_temp_vlan_id>>

switchport trunk native vlan <<var_temp_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 13
no shutdown
```

Define a description for the port channel connecting to <<var_ucs_clustername>>-B:

```
interface Po14
description <<var_ucs_clustername>>-B-Appl
```

Define a port description for the interface connecting to <<var_ucs_clustername>>-B:

```
interface Eth1/15
description <<var_ucs_clustername>>-B:1/5

interface Eth1/16
description <<var_ucs_clustername>>-B:1/6
```

Apply it to a port channel and bring up the interface:

```
interface Eth1/15-16
channel-group 14 mode active
no shutdown
```

Make the port channel a switchport, and configure a trunk to allow multiple VLANs:

```
interface Po14
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_temp_vlan_id>>
switchport trunk native vlan <<var_temp_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 14
no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

To Verify the VPC configuration, in this example vPC 13 and 14, you can run the following commands:

```
CRA-N9K-A# show vpc 13

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
13   Po13   down*  success     success                    2

CRA-N9K-A# show vpc 14

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
14   Po14   down*  success     success                    2


CRA-N9K-B# show vpc 13

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
13   Po13   down*  Not         Consistency Check Not      2
```

```
                    Applicable  Performed

CRA-N9K-B# show vpc 14

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
14   Po14   down*  Not         Consistency Check Not      2
                    Applicable  Performed
```



Since the ports on the Cisco UCS Fabric Interconnects are not configured yet, the Status is shown as “down” and there are no active VLANs.

## Configure Network Interfaces to the Backup Destination

Port channels can be defined to have a dedicated bandwidth for each type of Network. Below is an example of how to create a port channel for a backup Network; the cables are connected to storage for backup. This example uses port Ethernet 1/29 on each Nexus 9000 connected to EMC DataDomain that is used as the backup destination.

### Cisco Nexus 9000 A

Define a description for the port channel connecting to the backup destination:

```
interface Po21

description Backup-Destination-1
```

Define a port description for the interface connecting to the backup destination:

```
interface Eth1/29

description <<var_backup_node01>>
```

Apply it to a port channel and bring up the interface:

```
interface eth1/29
channel-group 21 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow NFS VLAN for Backup:

```
interface Po21
```

```
switchport
switchport mode trunk

switchport trunk allowed vlan <<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 21

no shutdown
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

Define a description for the port channel connecting to the backup destination:

```
interface Po21

description Backup-Destination-1
```

Define a port description for the interface connecting to the backup destination:

```
interface Eth1/29

description <<var_backup_node01>>
```

Apply it to a port channel and bring up the interface:

```
interface eth1/29
channel-group 21 mode active

no shutdown
```

Make the port channel a switchport, and configure a trunk to allow NFS VLAN for Backup:

```
interface Po21

switchport
switchport mode trunk

switchport trunk allowed vlan <<var_backup_vlan_id>>
```

Make the port channel and associated interfaces spanning tree edge ports:

```
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames:

```
mtu 9216
```

Make this a VPC port channel and bring it up:

```
vpc 21
no shutdown
```

Save the running configuration to start-up:

copy run start

To Verify the VPC configuration, in this example vPC 13 and 14, run the following commands:

```
CRA-N9K-A# show vpc 21

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
21   Po21   down*  success     success                    -

CRA-N9K-B# show vpc 21


vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
21   Po21   down*  Not         Consistency Check Not      -
                   Applicable  Performed
```



The ports on the Backup destination are not configured yet. The Status is shown as down and there are no active vlans

## Configure Ports connected to Cisco C880 M4 for VMware ESX

Each N9K switch 2 link connects to each Cisco C880 M4 server. In this use case, two Ethernet interfaces are mapped to vSwitch0 for VMkernel and NFS traffic, and two Ethernet Interfaces are mapped to vSwitch1 for Application traffic. The network ports are configured as trunk ports without port channel or vPC. In this

example configuration, links connected to C880 are connected to Ethernet port 1/31 and 1/32 on each switch.

To configure  the interfaces for administrative traffic, complete the following steps:.

### Cisco Nexus 9000 A

Define a port description for the interface connecting to C880M4-1:

```
interface Eth1/31

description C880m4-1

switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>

no shutdown
```

Set the MTU to be 9216 to support jumbo frames if required:

```
interface Eth1/31

mtu 9216
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

Define a port description for the interface connecting to C880M4-1:

```
interface Eth1/31

description C880m4-1

switchport
switchport mode trunk

switchport trunk allowed vlan
<<var_management_vlan_id>>,<<var_admin_vlan_id>>,<<var_vmotion_vlan_id>>,<<var_es
x_nfs_vlan_id>>,<<var_backup_vlan_id>>

no shutdown
```

Set the MTU to be 9216 to support jumbo frames if required:

```
interface Eth1/31

mtu 9216
```

Save the running configuration to start-up:

```
copy run start
```

To configure the interfaces for application traffic, complete the following steps:

### Cisco Nexus 9000 A

Define a port description for the interface connecting to C880M4-1:

```
interface Eth1/32

description C880m4-1-Application

switchport
switchport mode trunk

no shutdown
```

Set the MTU to be 9216 to support jumbo frames if required:

```
interface Eth1/32

mtu 9216
```

Save the running configuration to start-up:

```
copy run start
```

### Cisco Nexus 9000 B

Define a port description for the interface connecting to C880M4-1:

```
interface Eth1/32

description C880m4-1-Application

switchport
switchport mode trunk

no shutdown
```

Set the MTU to be 9216 to support jumbo frames if required:

```
interface Eth1/32

mtu 9216
```

Save the running configuration to start-up:

```
copy run start
```

## Cisco MDS Configuration

This section explains the fabric switch configuration required for the Cisco Integrated Infrastructure for SAP HANA with EMC VNX Storage. The details about configuring the password, management connectivity and strengthening the device are not covered in this document; for more information, refer to the Cisco MDS 9148S Switch Configuration Guide.

This example uses the Fibre Channel Port Channel between the Cisco MDS switches and the Cisco UCS Fabric Interconnects.



Since the Cisco UCS is not configured at this time the FC ports connected to the Cisco UCS Fabric Interconnects will not come up.

Table 27 the setup for the Cisco MDS 9000 switches in this Cisco UCS Integrated Infrastructure for SAP HANA.

**Table 27 Information to Setup Cisco MDS Switches in the Reference Architecture**

| Name | Variable |
|---|---|
| Global default administrative password | <<var_mgmt_passwd>> |
| SNMP Community String for Read Only access | <<var_snmp_ro_string>> |
| MDS 9000 A hostname | <<var_mds-a_name>> |
| MDS 9000 A Management IP Address | <<var_mds-a_ip>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| Time Zone in a format required by the MDS switches | <<var_mds_timezone>> |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| MDS 9000 B hostname | <<var_mds-b_name>> |
| MDS 9000 B Management IP Address | <<var_mds-b_ip>> |
| Fibre Channel - Port Channel ID for MDS A | <<var_fc-pc_a_id>> |
| Fibre Channel - Port Channel ID for MDS B | <<var_fc-pc_b_id>> |
| VSAN ID for MDS A | <<var_san_a_id>> |
| VSAN ID for MDS B | <<var_san_b_id>> |
| Name of Zone Template with multiple paths | <<var_zone_temp_name>> |
| Name of Zone Template with a single paths | <<var_zone_temp_1path_name>> |
| Name of the Zone Set | <<var_zoneset_name> |

## Cisco MDS Initial Configuration

### Cisco MDS 9148 A

Connect to the console port of MDS9148S-A.

```
         ---- System Admin Account Setup ----


Do you want to enforce secure password standard (yes/no) [y]: yes

  Enter the password for "admin": <<var_mgmt_passwd>>
  Confirm the password for "admin": <<var_mgmt_passwd>>

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco MDS 9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.

Press Enter at any time to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes


  Create another login account (yes/no) [n]:
```

```
 Configure read-only SNMP community string (yes/no) [n]: yes

 SNMP community string : <<var_snmp_ro_string>>

 Enter the switch name : <<var_mds-a_name>>

 Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

 Mgmt0 IPv4 address : <<var_mds-a_ip>>

Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>

Configure the default gateway? (yes/no) [y]:

IPv4 address of the default gateway : <<var_mgmt_gw>>

Configure advanced IP options? (yes/no) [n]:

Enable the ssh service? (yes/no) [y]:

Type of ssh key you would like to generate (dsa/rsa) [rsa]:

Number of rsa key bits <768-2048> [1024]: 2048

Enable the telnet service? (yes/no) [n]:

Enable the http-server? (yes/no) [y]:

Configure clock? (yes/no) [n]:
```

```
 Configure timezone? (yes/no) [n]: y

Enter timezone config : <<var_mds_timezone>>

 Configure summertime? (yes/no) [n]: y

Please note, this is not a wizard. It is just to get you into the system with
minimal config.
Sample config: PDT 2 sunday march 02:00 1 sunday november 02:00 59
You can configure the switch most accurately after logging in.

summer-time config :PDT 2 sunday march 02:00 1 sunday november 02:00 59

 Configure the ntp server? (yes/no) [n]: y

 NTP server IPv4 address : <<var_global_ntp_server_ip>>

 Configure default switchport interface state (shut/noshut) [shut]: noshut

 Configure default switchport trunk mode (on/off/auto) [on]: auto

 Configure default switchport port mode F (yes/no) [n]: y

 Configure default zone policy (permit/deny) [deny]:

 Enable full zoneset distribution? (yes/no) [n]:

 Configure default zone mode (basic/enhanced) [basic]:

The following configuration will be applied:
  password strength-check
```

```
  snmp-server community <<var_snmp_ro_string>>  ro
  switchname <<var_mds-a_name>>
  interface mgmt0
    ip address <<var_mds-a_ip>> <<var_mgmt_netmask>>
    no shutdown
  ip default-gateway <<var_mgmt_gw>>
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  feature http-server
  clock timezone <<var_mgmt_timezone>>
  clock summer-time PDT 2 sunday march 02:00 1 sunday november 02:00 59
  ntp server <<var_global_ntp_server_ip>>
  no system default switchport shutdown
  system default switchport trunk mode auto
  system default switchport mode F
  no system default zone default-zone permit
  no system default zone distribute full
  no system default zone mode enhanced

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

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

[########################################] 100%



User Access Verification
<<var_mds-a_name>> login:
```

Log in to the MDS 9148S-A as admin and enter configuration mode:

```
config terminal
```

Use the following commands to enable the necessary features:

```
feature npiv
```

### Cisco MDS 9148 B

Connect to the console port of MDS9148S-B.

```
         ---- System Admin Account Setup ----


Do you want to enforce secure password standard (yes/no) [y]: yes

  Enter the password for "admin": <<var_mgmt_passwd>>
  Confirm the password for "admin": <<var_mgmt_passwd>>

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco MDS 9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.

Press Enter at any time to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

```
Create another login account (yes/no) [n]:

Configure read-only SNMP community string (yes/no) [n]: yes

SNMP community string : <<var_snmp_ro_string>>

Enter the switch name : <<var_mds-b_name>>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

Mgmt0 IPv4 address : <<var_mds-b_ip>>

Mgmt0 IPv4 netmask : <<var_mgmt_netmask>>

Configure the default gateway? (yes/no) [y]:

IPv4 address of the default gateway : <<var_mgmt_gw>>

Configure advanced IP options? (yes/no) [n]:

Enable the ssh service? (yes/no) [y]:

Type of ssh key you would like to generate (dsa/rsa) [rsa]:

Number of rsa key bits <768-2048> [1024]: 2048

Enable the telnet service? (yes/no) [n]:

Enable the http-server? (yes/no) [y]:

Configure clock? (yes/no) [n]:
```

```
 Configure timezone? (yes/no) [n]: y

 Enter timezone config : <<var_mds_timezone>>

 Configure summertime? (yes/no) [n]: y

Please note, this is not a wizard. It is just to get you into the system with
minimal config.

Sample config: PDT 2 sunday march 02:00 1 sunday november 02:00 59

You can configure the switch most accurately after logging in.

summer-time config :PDT 2 sunday march 02:00 1 sunday november 02:00 59

 Configure the ntp server? (yes/no) [n]: y

 NTP server IPv4 address : <<var_global_ntp_server_ip>>

 Configure default switchport interface state (shut/noshut) [shut]: noshut

 Configure default switchport trunk mode (on/off/auto) [on]: auto

 Configure default switchport port mode F (yes/no) [n]: y

 Configure default zone policy (permit/deny) [deny]:

 Enable full zoneset distribution? (yes/no) [n]:

 Configure default zone mode (basic/enhanced) [basic]:

The following configuration will be applied:
```

```
  password strength-check
  snmp-server community <<var_snmp_ro_string>>  ro
  switchname <<var_mds-b_name>>
  interface mgmt0
  ip address <<var_mds-b_ip>> <<var_mgmt_netmask>>
  no shutdown
  ip default-gateway <<var_mgmt_gw>>
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  feature http-server
  clock timezone <<var_mgmt_timezone>>
  clock summer-time PDT 2 sunday march 02:00 1 sunday november 02:00 59
  ntp server <<var_global_ntp_server_ip>>
  no system default switchport shutdown
  system default switchport trunk mode auto
  system default switchport mode F
  no system default zone default-zone permit
  no system default zone distribute full
  no system default zone mode enhanced

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

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

[########################################] 100%



User Access Verification
<<var_mds-b_name>> login:
```

## Configure the Management Port

### Cisco MDS 9148 A

On MDS 9148 A enter configuration mode:

```
config terminal
```

Use the following commands to configure the management port mgmt0:

```
interface mgmt 0
switchport speed 1000
no shut
```

Save the running configuration to start-up.

```
copy run start
```

### Cisco MDS 9148 B

On MDS 9148 B enter configuration mode:

```
config terminal
```

Use the following commands to configure the management port mgmt0:

```
interface mgmt 0
switchport speed 1000
no shut
```

Save the running configuration to start-up:

```
copy run start
```

Verify the configuration with the following commands. The ping destination in this example is the management port of MDS 9148S B:

```
CRA-EMC-A# show int bri

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                         Mode  Speed  Channel
                        Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1/1      10     auto   auto    notConnected     swl    --           110
fc1/2      10     auto   auto    notConnected     swl    --           110
```

```
…
…
…
--------------------------------------------------------------------------------
Interface               Status     IP Address          Speed     MTU
--------------------------------------------------------------------------------
mgmt0                    up         192.168.76.3/24    1 Gbps    1500
…
…
…

CRA-EMC-A# ping 192.168.76.4 count 5
PING 192.168.76.4 (192.168.76.4) 56(84) bytes of data.
64 bytes from 192.168.76.4: icmp_seq=1 ttl=64 time=0.122 ms
64 bytes from 192.168.76.4: icmp_seq=2 ttl=64 time=0.115 ms
64 bytes from 192.168.76.4: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 192.168.76.4: icmp_seq=4 ttl=64 time=0.116 ms
64 bytes from 192.168.76.4: icmp_seq=5 ttl=64 time=0.105 ms

--- 192.168.76.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.105/0.114/0.122/0.012 ms
CRA-EMC-A#
```

## Configure Fibre Channel Ports and Port Channels

### Cisco MDS 9148 A

On MDS 9148 A enter configuration mode:

```
config terminal
```

Enable required Features:

```
feature fport-channel-trunk
feature npiv
```

Use the following commands to configure the FC Port channel and add all FC ports connected to Cisco UCS Fabric Interconnect A:

```
int port-channel <<var_fc-pc_a_id>>
channel mode active



int fc1/1-8
channel-group <<var_fc-pc_a_id>> force

int port-channel <<var_fc-pc_a_id>>
switchport mode F
switchport trunk mode off
no shut
```

Save the running configuration to start-up:

```
copy run start
```

To verify the FC Port channel configuration, in this example FC-PC 110, run the following commands:

```
CRA-EMC-A(config-if)# show port channel database
port channel 110
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update succeeded
    8 ports in total, 0 ports up
    Ports:   fc1/1    [down]
             fc1/2    [down]
             fc1/3    [down]
             fc1/4    [down]
             fc1/5    [down]
             fc1/6    [down]
             fc1/7    [down]
             fc1/8    [down]
```

```
CRA-EMC-A(config-if)# show int bri

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1/1      1      auto   auto    notConnected    swl    --           110
fc1/2      1      auto   auto    notConnected    swl    --           110
fc1/3      1      auto   auto    notConnected    swl    --           110
fc1/4      1      auto   auto    notConnected    swl    --           110
fc1/5      1      auto   auto    notConnected    swl    --           110
fc1/6      1      auto   auto    notConnected    swl    --           110
fc1/7      1      auto   auto    notConnected    swl    --           110
fc1/8      1      auto   auto    notConnected    swl    --           110
fc1/9      1      F      auto    sfpAbsent       --     --           --
fc1/10     1      F      auto    sfpAbsent       --     --           --
fc1/11     1      F      auto    sfpAbsent       --     --           --
fc1/12     1      F      auto    sfpAbsent       --     --           --
fc1/13     1      F      auto    sfpAbsent       --     --           --
…
CRA-EMC-A(config-if)#
```

### Cisco MDS 9148 B

On MDS 9148 B enter configuration mode:

```
config terminal
```

Enable required features:

```
feature fport-channel-trunk
feature npiv
```

Use the following commands to configure the FC Port channel and add all FC ports connected to Cisco UCS Fabric Interconnect B:

```
int port channel <<var_fc-pc_b_id>>
```

```
channel mode active

int fc1/1-8
channel-group <<var_fc-pc_b_id>> force

int port channel <<var_fc-pc_b_id>>
switchport mode F
switchport trunk mode off
no shut
```

Save the running configuration to start-up:

```
copy run start
```

To verify the FC Port channel configuration, in this example FC-PC 120, run the following commands:

```
CRA-EMC-B# show port channel database
port channel 120
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update succeeded
    8 ports in total, 0 ports up
    Ports:   fc1/1    [down]
             fc1/2    [down]
             fc1/3    [down]
             fc1/4    [down]
             fc1/5    [down]
             fc1/6    [down]
             fc1/7    [down]
             fc1/8    [down]

CRA-EMC-B# show int bri

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
```

```
                    Mode   Trunk                          Mode  Speed  Channel
                           Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1/1       1      auto   auto    notConnected     swl    --           120
fc1/2       1      auto   auto    notConnected     swl    --           120
fc1/3       1      auto   auto    notConnected     swl    --           120
fc1/4       1      auto   auto    notConnected     swl    --           120
fc1/5       1      auto   auto    notConnected     swl    --           120
fc1/6       1      auto   auto    notConnected     swl    --           120
fc1/7       1      auto   auto    notConnected     swl    --           120
fc1/8       1      auto   auto    notConnected     swl    --           120
fc1/9       1      F      auto    sfpAbsent        --     --           --
fc1/10      1      F      auto    sfpAbsent        --     --           --
fc1/11      1      F      auto    sfpAbsent        --     --           --
fc1/12      1      F      auto    sfpAbsent        --     --           --
fc1/13      1      F      auto    sfpAbsent        --     --           --
…
CRA-EMC-B#
```

## Configure VSANs

Before configuring the global VSAN on MDS 9148 switches, it is crucial to enable the NPIV feature on the Cisco MDS 9148S switches. To enable the NPIV feature on MDS 9148S switch, complete the following steps:

### Cisco MDS 9148 A

On MDS 9148 A enter configuration mode:

```
config terminal
```

Use the following commands to enable the necessary features:

```
feature npiv
```

Use the following commands to configure the VSAN:

```
vsan database
vsan <<var_san_a_id>>
vsan <<var_san_a_id>> interface port channel <<var_fc-pc_a_id>>
```

```
vsan <<var_san_a_id>> interface fc 1/25
vsan <<var_san_a_id>> interface fc 1/26
vsan <<var_san_a_id>> interface fc 1/27
vsan <<var_san_a_id>> interface fc 1/28
vsan <<var_san_a_id>> interface fc 1/29
vsan <<var_san_a_id>> interface fc 1/30
vsan <<var_san_a_id>> interface fc 1/31
vsan <<var_san_a_id>> interface fc 1/32
end
```



For ports with “Status Up” you will see a notification that traffic may be impacted. Type y and press Enter to commit the change.

Save the running configuration to start-up:

```
copy run start
```

To verify the VSAN configuration, in this example VSAN 10, run the following commands:

```
CRA-EMC-A# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 10 information
         name:VSAN0010  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan
```

```
vsan 4094:isolated_vsan
Show the interfaces that are members of a VSAN:
CRA-EMC-A# show vsan membership
vsan 1 interfaces:
    fc1/9             fc1/10            fc1/11            fc1/12
    fc1/13            fc1/14            fc1/15            fc1/16
    fc1/17            fc1/18            fc1/19            fc1/20
    fc1/21            fc1/22            fc1/23            fc1/24
    fc1/33            fc1/34            fc1/35            fc1/36
    fc1/37            fc1/38            fc1/39            fc1/40
    fc1/41            fc1/42            fc1/43            fc1/44
    fc1/45            fc1/46            fc1/47            fc1/48

vsan 10 interfaces:
    fc1/1             fc1/2             fc1/3             fc1/4
    fc1/5             fc1/6             fc1/7             fc1/8
    fc1/25            fc1/26            fc1/27            fc1/28
    fc1/29            fc1/30            fc1/31            fc1/32
    port channel 110

vsan 4079(evfp_isolated_vsan) interfaces:


vsan 4094(isolated_vsan) interfaces:
```

Show the connection status for all Fibre Channel ports on the Cisco Nexus switch:

```
CRA-EMC-A(config)# show int bri

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                         Mode  Speed  Channel
                        Mode                                (Gbps)
```

```
--------------------------------------------------------------------------------
fc1/1       10    auto   auto    notConnected     swl    --            110
fc1/2       10    auto   auto    notConnected     swl    --            110
fc1/3       10    auto   auto    notConnected     swl    --            110
fc1/4       10    auto   auto    notConnected     swl    --            110
fc1/5       10    auto   auto    notConnected     swl    --            110
fc1/6       10    auto   auto    notConnected     swl    --            110
fc1/7       10    auto   auto    notConnected     swl    --            110
fc1/8       10    auto   auto    notConnected     swl    --            110
…
…
fc1/25      10     F      auto    up               swl    F       8     --
fc1/26      10     F      auto    up               swl    F       8     --
fc1/27      10     F      auto    up               swl    F       8     --
fc1/28      10     F      auto    up               swl    F       8     --
fc1/29      10     F      auto    up               swl    F       8     --
fc1/30      10     F      auto    up               swl    F       8     --
fc1/31      10     F      auto    up               swl    F       8     --
fc1/32      10     F      auto    up               swl    F       8     --
…
…
--------------------------------------------------------------------------------
Interface               Status                            Speed
                                                          (Gbps)
--------------------------------------------------------------------------------
sup-fc0                 up                                1


--------------------------------------------------------------------------------
Interface               Status     IP Address          Speed     MTU
--------------------------------------------------------------------------------
mgmt0                    up         192.168.76.3/24    1 Gbps    1500
```

```
--------------------------------------------------------------------------------
Interface              Vsan   Admin  Status         Oper   Oper     IP
                              Trunk           Mode   Speed    Address
                              Mode                  (Gbps)
--------------------------------------------------------------------------------
port channel 110       10     auto   noOperMembers  --             --
```

### Cisco MDS 9148 B

On MDS 9148 B enter configuration mode:

```
config terminal
```

Use the following commands to configure the VSAN:

```
vsan database
vsan <<var_san_b_id>>
vsan <<var_san_b_id>> interface port channel <<var_fc-pc_b_id>>
vsan <<var_san_b_id>> interface fc 1/25
vsan <<var_san_b_id>> interface fc 1/26
vsan <<var_san_b_id>> interface fc 1/27
vsan <<var_san_b_id>> interface fc 1/28
vsan <<var_san_b_id>> interface fc 1/29
vsan <<var_san_b_id>> interface fc 1/30
vsan <<var_san_b_id>> interface fc 1/31
vsan <<var_san_b_id>> interface fc 1/32
end
```



For ports with “Status Up” you will see a notification that traffic may be impacted. Type y and press Enter to commit the change.

Save the running configuration to start-up:

```
copy run start
```

To verify the VSAN configuration, in this example VSAN 20, run the following commands:

```
CRA-EMC-B# show vsan
vsan 1 information
```

```
            name:VSAN0001  state:active
            interoperability mode:default
            loadbalancing:src-id/dst-id/oxid
            operational state:down

vsan 20 information
            name:VSAN0020  state:active
            interoperability mode:default
            loadbalancing:src-id/dst-id/oxid
            operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan
```

Show the interfaces that are members of a VSAN:

```
CRA-EMC-A# show vsan membership
vsan 1 interfaces:
    fc1/9           fc1/10          fc1/11          fc1/12
    fc1/13          fc1/14          fc1/15          fc1/16
    fc1/17          fc1/18          fc1/19          fc1/20
    fc1/21          fc1/22          fc1/23          fc1/24
    fc1/33          fc1/34          fc1/35          fc1/36
    fc1/37          fc1/38          fc1/39          fc1/40
    fc1/41          fc1/42          fc1/43          fc1/44
    fc1/45          fc1/46          fc1/47          fc1/48

vsan 20 interfaces:
    fc1/1           fc1/2           fc1/3           fc1/4
    fc1/5           fc1/6           fc1/7           fc1/8
    fc1/25          fc1/26          fc1/27          fc1/28
    fc1/29          fc1/30          fc1/31          fc1/32
    port channel 120

vsan 4079(evfp_isolated_vsan) interfaces:


vsan 4094(isolated_vsan) interfaces:
```

Show the connection status for all Fibre Channel ports on the Cisco Nexus switch:

```
CRA-EMC-A(config)# show int bri

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                          Mode  Speed  Channel
                        Mode                                 (Gbps)
--------------------------------------------------------------------------------
```

```
fc1/1       20     auto   auto    notConnected     swl    --           120
fc1/2       20     auto   auto    notConnected     swl    --           120
fc1/3       20     auto   auto    notConnected     swl    --           120
fc1/4       20     auto   auto    notConnected     swl    --           120
fc1/5       20     auto   auto    notConnected     swl    --           120
fc1/6       20     auto   auto    notConnected     swl    --           120
fc1/7       20     auto   auto    notConnected     swl    --           120
fc1/8       20     auto   auto    notConnected     swl    --           120
…
…
fc1/25      20     F      auto    up               swl    F       8    --
fc1/26      20     F      auto    up               swl    F       8    --
fc1/27      20     F      auto    up               swl    F       8    --
fc1/28      20     F      auto    up               swl    F       8    --
fc1/29      20     F      auto    up               swl    F       8    --
fc1/30      20     F      auto    up               swl    F       8    --
fc1/31      20     F      auto    up               swl    F       8    --
fc1/32      20     F      auto    up               swl    F       8    --
…
…
--------------------------------------------------------------------------------
Interface               Status                            Speed
                                                          (Gbps)
--------------------------------------------------------------------------------
sup-fc0                 up                                1


--------------------------------------------------------------------------------
Interface              Status     IP Address          Speed     MTU
--------------------------------------------------------------------------------
mgmt0                   up         192.168.76.4/24    1 Gbps   1500
```

```
--------------------------------------------------------------------------------
Interface              Vsan   Admin   Status         Oper   Oper     IP
                              Trunk          Mode   Speed    Address
                              Mode                (Gbps)
--------------------------------------------------------------------------------
port channel 120       20     auto    noOperMembers  --             --
```

## Configure the Fibre Channel Zoning

To use the EMC VNX storages in a SAN configuration, you need to define single initiator zones. In each zone, there is only one server-based HBA, but multiple storage ports are allowed.



You can only define the global zoneset without any zones.

### Cisco MDS 9148 A

On MDS 9148 A enter configuration mode:

```
config terminal
```

Use the following commands to create the zone template with all storage ports:

```
zone name <<var_zone_temp_name>> vsan <<var_san_a_id>>
member interface fc1/25
member interface fc1/26
member interface fc1/27
member interface fc1/28
member interface fc1/29
member interface fc1/30
member interface fc1/31
member interface fc1/32
exit

zone name <<var_zone_temp_1path_name>> vsan <<var_san_a_id>>
member interface fc1/25
exit
```

Use the following commands to create the zoneset:

```
zoneset name <<var_zoneset_name>> vsan <<var_san_a_id>>
```

Save the running configuration to start-up:

```
copy run start
```

Use the following commands to verify the configuration:

```
CRA-EMC-A(config)# show zone
zone name zone_temp vsan 10
   interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
   interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

CRA-EMC-A(config)# show zoneset
zoneset name CRA-EMC-A vsan 10
```

### Cisco MDS 9148 B

On MDS 9148 B enter configuration mode:

```
config terminal
```

Use the following commands to create the zone template with all storage ports:

```
zone name <<var_zone_temp_name>> vsan <<var_san_b_id>>
member interface fc1/25
member interface fc1/26
member interface fc1/27
member interface fc1/28
member interface fc1/29
member interface fc1/30
```

```
member interface fc1/31
member interface fc1/32

zone name <<var_zone_temp_1path_name>> vsan <<var_san_b_id>>
member interface fc1/26
exit
```

Use the following commands to create the zoneset:

```
zoneset name <<var_zoneset_name>> vsan <<var_san_b_id>>
```

Save the running configuration to start-up:

```
copy run start
```

## Cisco UCS Configuration

This section details how to configure the Cisco UCS Fabric Interconnects and Cisco UCS. This task can be subdivided in to the following segments:

- Initial configuration of Cisco UCS Fabric Interconnects
- Configuration of Global Policies
- Configuration of VLANs, Port Channels and vNIC Templates
- Configuration of VSANs, Port Channels and vHBA Templates
- Configuration of Service Profile Templates for the different Use-Cases
- Configuration of LAN and SAN Uplink Ports
- Configuration of Server Ports and Server Discovery

### Configure the Cisco UCS Fabric Interconnects

The Cisco UCS Fabric Interconnects, blade server chassis and C-Series server must be mounted in the rack and the appropriate cables must be connected. Two CAT5 ethernet cables must be connected between the two Cisco UCS Fabric Interconnects for management pairing on ports L1 and L2. Two redundant power supplies are provided per Cisco UCS Fabric Interconnect, it is highly recommended that both are plugged in, ideally drawing power from two different power strips. Connect mgmt0 interfaces of each Cisco UCS Fabric Interconnect to the management network, and set the switch port connected to Cisco UCS Fabric Interconnect in access mode with access VLAN as management VLAN.

Table 28 the required information for the initial configuration of Cisco UCS in this Cisco UCS Integrated Infrastructure for SAP HANA.

**Table 28 Information to Setup Cisco UCS in the Reference Architecture**

| Name | Variable |
|---|---|
| Global default administrative password | <<var_mgmt_passwd>> |
| UCS Domain Cluster Name | <<var_ucs_clustername>> |
| UCS Fabric Interconnect A Management IP Address | <<var_ucsa_mgmt_ip>> |
| Management network Netmask | <<var_mgmt_mask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| UCS Manager Cluster IP Address | <<var_ucs_cluster_ip>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| DNS domain name | <<var_mgmt_dns_domain_name>> |
| UCS Fabric Interconnect B Management IP Address | <<var_ucsb_mgmt_ip>> |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| Name for the UCS Sub-Organization used for ESXi hosts | <<var_esx_sub-org-name>> |

To perform the initial configuration of the Cisco UCS Fabric Interconnects, complete the following steps:



If the Cisco 2911 ISR is used, you can connect to the console through telnet <<var_isr_ip>> 2005. If the Cisco 2911 ISR is not used, attach the RJ-45 serial console cable to the first fabric interconnect and connect the other end to the serial port of your laptop. Configure the password for the admin account, fabric ID "A", UCS system name, management IP address, subnet mask and default gateway and cluster IP address (or UCSM Virtual IP address), as the initial configuration script takes you through the configuration process.

### Cisco UCS Fabric Interconnect A

Connect to the console port on the first Cisco UCS 6200 fabric interconnect:

```
Enter the configuration method: 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 passwords? (y/n) [y]: y

Enter the password for "admin": <<var_mgmt_passwd>>
```

```
Enter the same password for "admin": <<var_mgmt_passwd>>

Is this fabric interconnect part of a cluster (select 'no' for standalone)?
(yes/no) [n]: y

Which switch fabric (A|B): A

Enter the system name: <<var_ucs_clustername>>

Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>>

Physical switch Mgmt0 IPv4 netmask: <<var_mgmt_mask>>

IPv4 address of the default gateway: <<var_mgmt_gw>>

Cluster IPv4 address: <<var_ucs_cluster_ip>>

Configure DNS Server IPv4 address? (yes/no) [no]: y

DNS IPv4 address: <<var_nameserver_ip>>

Configure the default domain name? y

Default domain name: <<var_mgmt_dns_domain_name>>

Join centralized management environment (UCS Central)? (yes/no) [n]: Enter
```

Review the settings printed to the console. If they are correct, answer yes to apply and save the configuration.

Wait for the log in prompt to make sure that the configuration has been saved.

### Cisco UCS Fabric Interconnect B

To configure Cisco UCS Fabric Interconnect B, complete the following steps:

Disconnect the RJ-45 serial console from the Fabric Interconnect A that you just configured and attach it to the Fabric Interconnect B, or in case the Cisco 2911 ISR is used use telnet <<var_isr_ip>> 2006. The second fabric interconnect detects that its peer has been configured and prompt you to join the cluster. The only information you need to provide is the fabric interconnect specific management IP address, subnet mask and default gateway, as shown below:

```
Enter the configuration method: console
Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster.  Do you want to continue {y|n}? y
Enter the admin password for the peer fabric interconnect: <<var_mgmt_passwd>>

Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>>

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

Wait for the login prompt to make sure that the configuration has been saved.

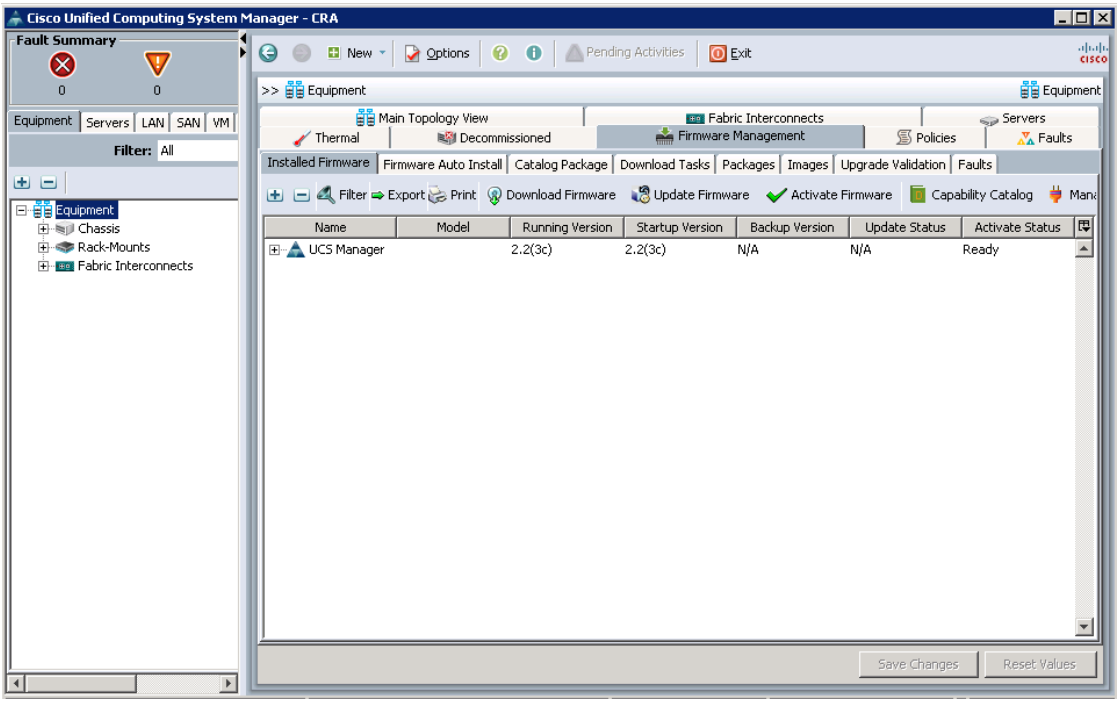
When the initial configurations on both Cisco UCS Fabric Interconnects are completed, you can disconnect the serial console cable or close the telnet sessions to the Cisco 2911 ISR. The Cisco UCS Manager is accessible through the Cisco UCS Manager GUI (https://<<ucs_cluster_ip>>/) and through SSH.

## Log in to Cisco UCS Manager

To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS cluster address.
2. Click the Launch UCS Manager link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.
5. Click Login.

**Figure 148 UCS Manager – Firmware Management**




## Upgrade Cisco UCS Manager Software

This CVD assumes the use of Cisco UCS Manager Software version 2.2(3c) or higher. To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 2.2(3c), refer to Cisco UCS Manager Install and Upgrade Guides.

## Configure Unified Ports

Cisco UCS Fabric Interconnects do have Universal Ports capable for 1/10Gigabit Ethernet or 2/4/8 Gigabit Fibre Channel. The ports are configured as Ethernet ports by default, and can be converted in to Fibre Channel ports if needed. To connect the EMC VNX storage array, FC ports are needed. Ports located on the expansion module must be converted into FC ports.

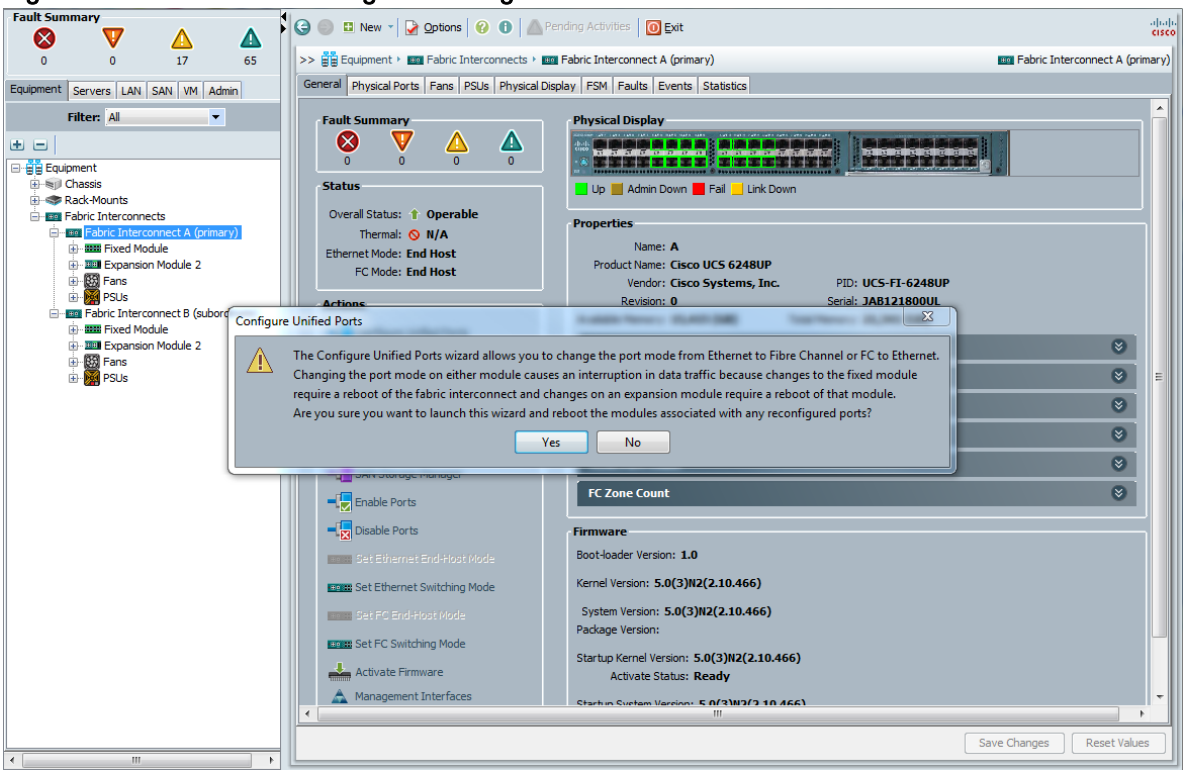
1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.

2. Select Fabric Interconnects > Fabric Interconnect A.

3. Click the Global tab in the Properties pane and click Configure Unified Ports.

4. Click Yes.

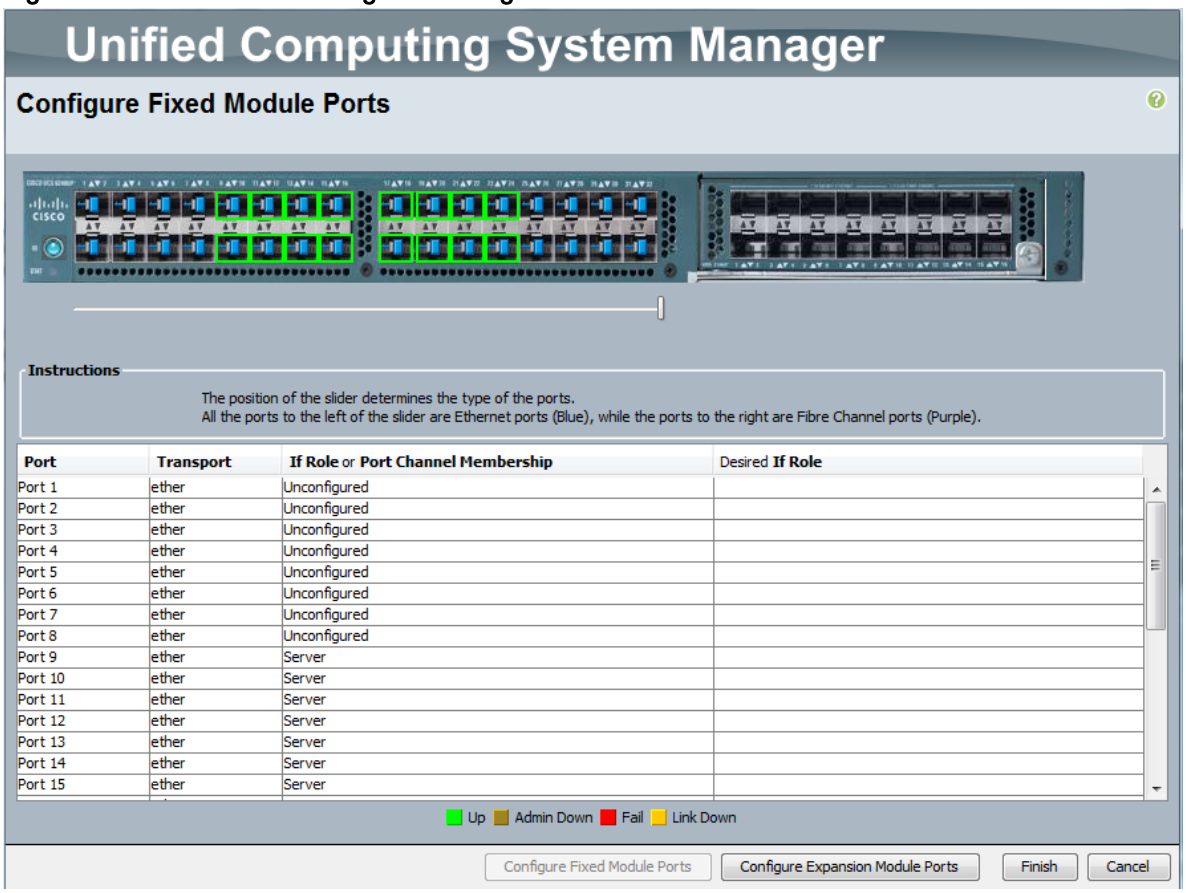
**Figure 149 Cisco UCS Manager – Configure Unified Ports**




5. In the new Window leave the slider on the right position (all ports on the Fixed Module are used for Ethernet).

6. Click Configure Expansion Module Ports.

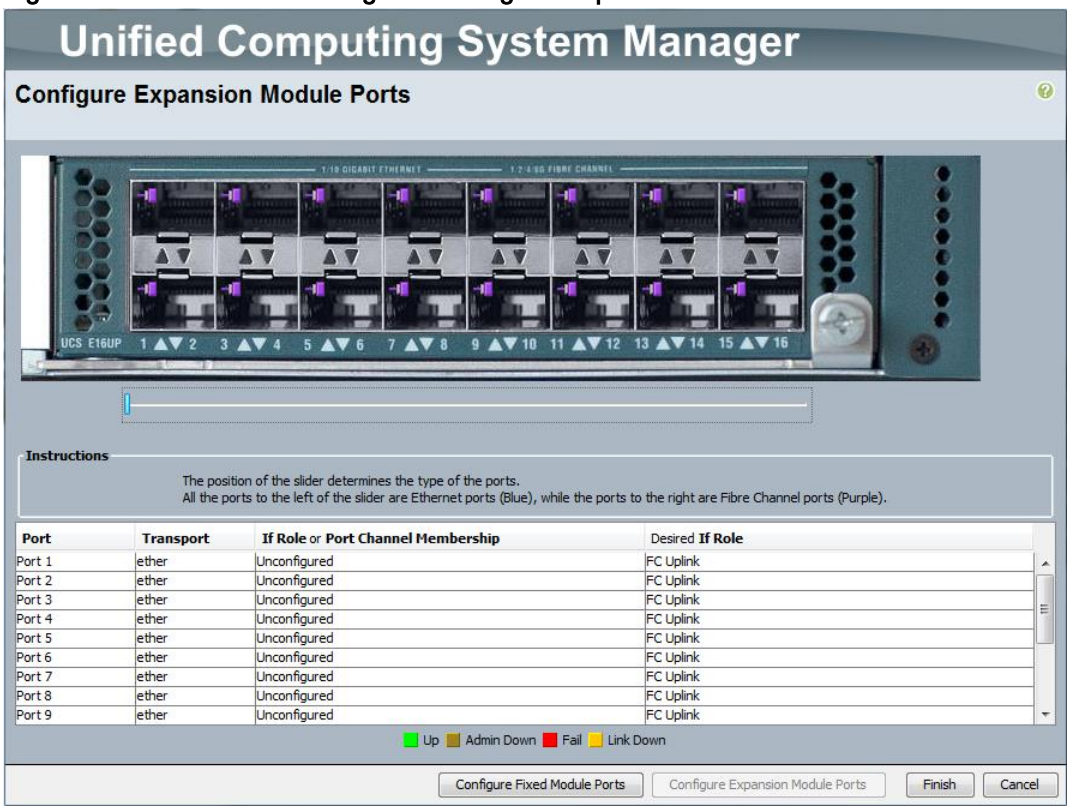
Figure 150 Cisco UCS Manager – Configure Fixed Module Ports




7. Select the slider bar at the top to set to the left. Make sure that ports 2/1 to 2/15 display FC Uplink.

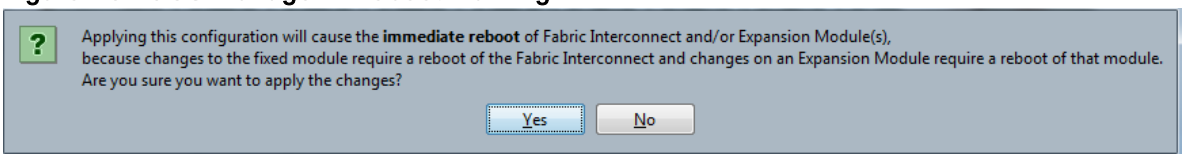
8. Click Finish.

Figure 151 Cisco UCS Manager – Configure Expansion Module Ports




9. In the pop-up click OK to reboot the Expansion Module.

Figure 152 UCS Manager – Reboot warning

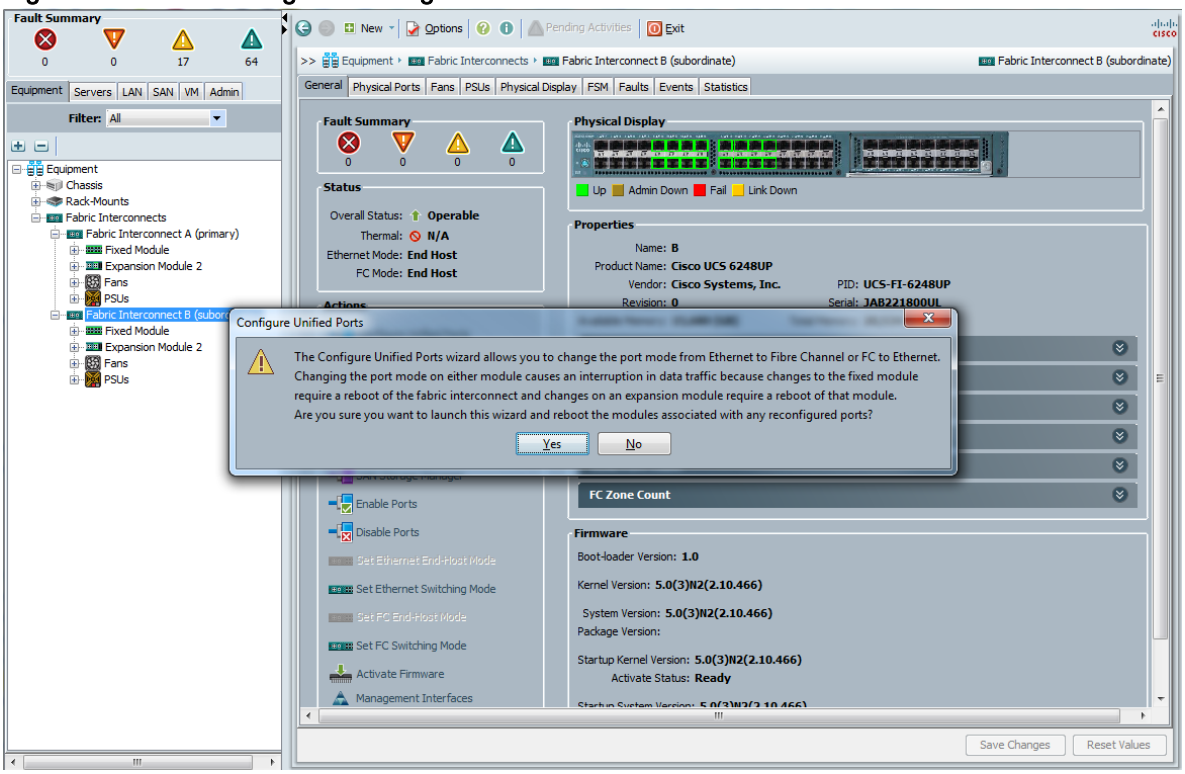



10. Select Fabric Interconnects > Fabric Interconnect B.

11. Click the Global tab in the Properties pane and click Configure Unified Ports.

12. Click Yes.

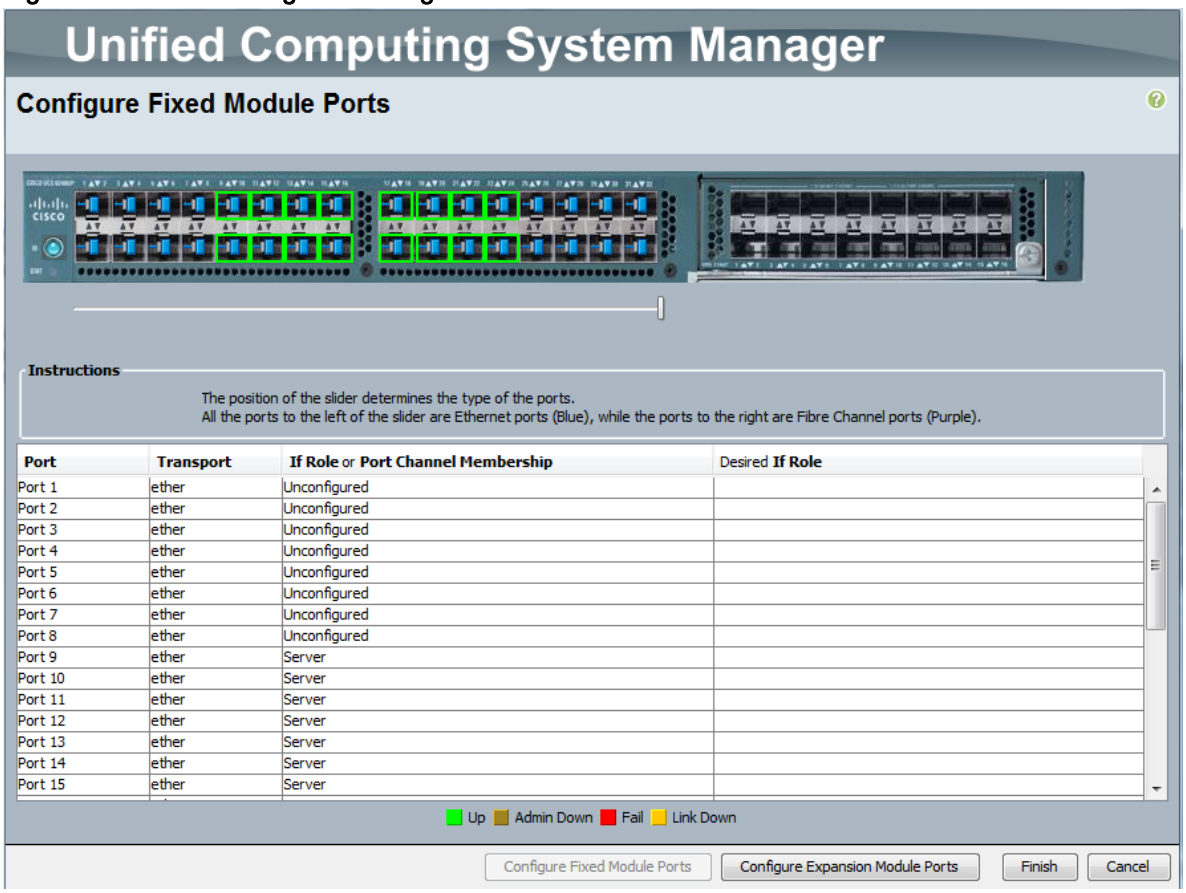
**Figure 153 UCS Manager – Configure Unified Ports**




13. In the new Window leave the slider on the right position (all ports on the Fixed Module are used for Ethernet).

14. Click Configure Expansion Module Ports.

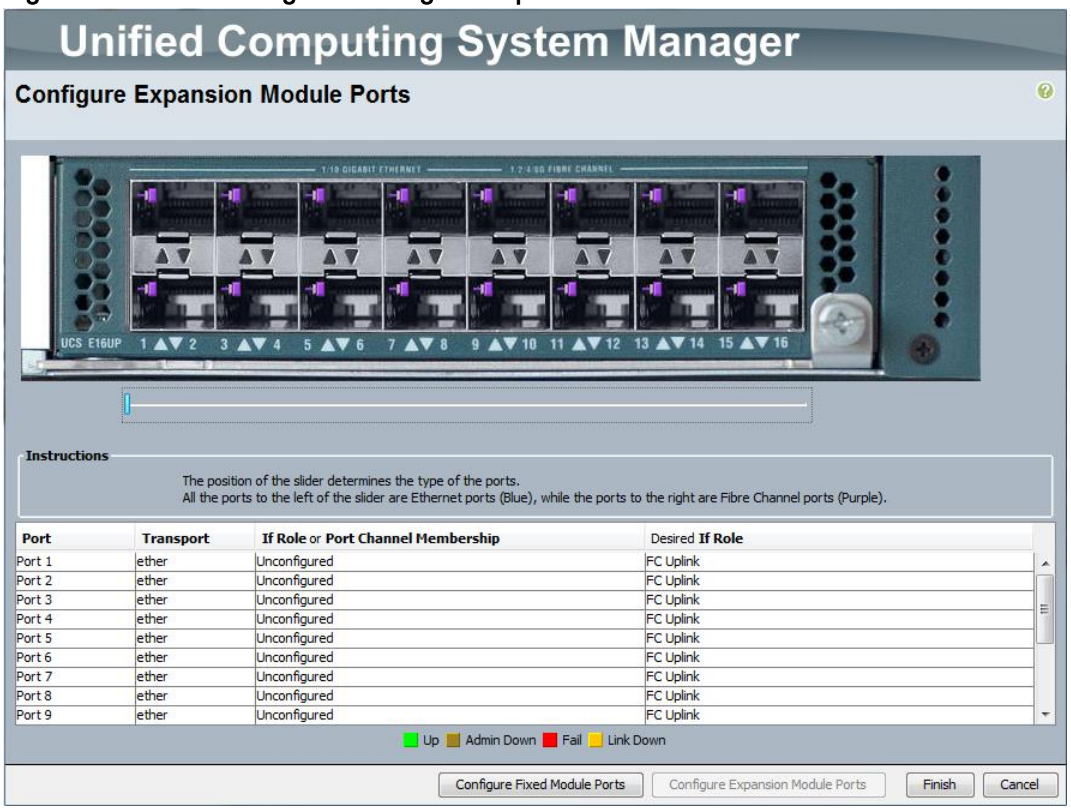
Figure 154 UCS Manager – Configure Fixed Module Ports




15. Select the slider bar at the top to set to the left. Make sure that ports 2/1 to 2/15 are showing FC Uplink.

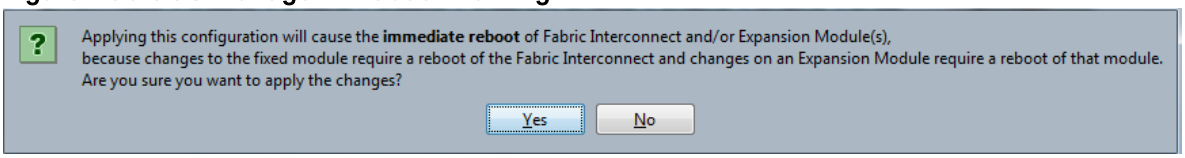
16. Click Finish.

Figure 155 UCS Manager – Configure Expansion Module Ports




17. In the pop-up window click OK to reboot the Expansion Module.

Figure 156 UCS Manager – Reboot warning




## Add Block of IP Addresses for KVM Access

To create a block of IP addresses for server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:



This block of IP addresses must be in the same subnet as the management IP addresses for the Cisco UCS Manager.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.
3. In the Actions pane, select Create Block of IP Addresses.

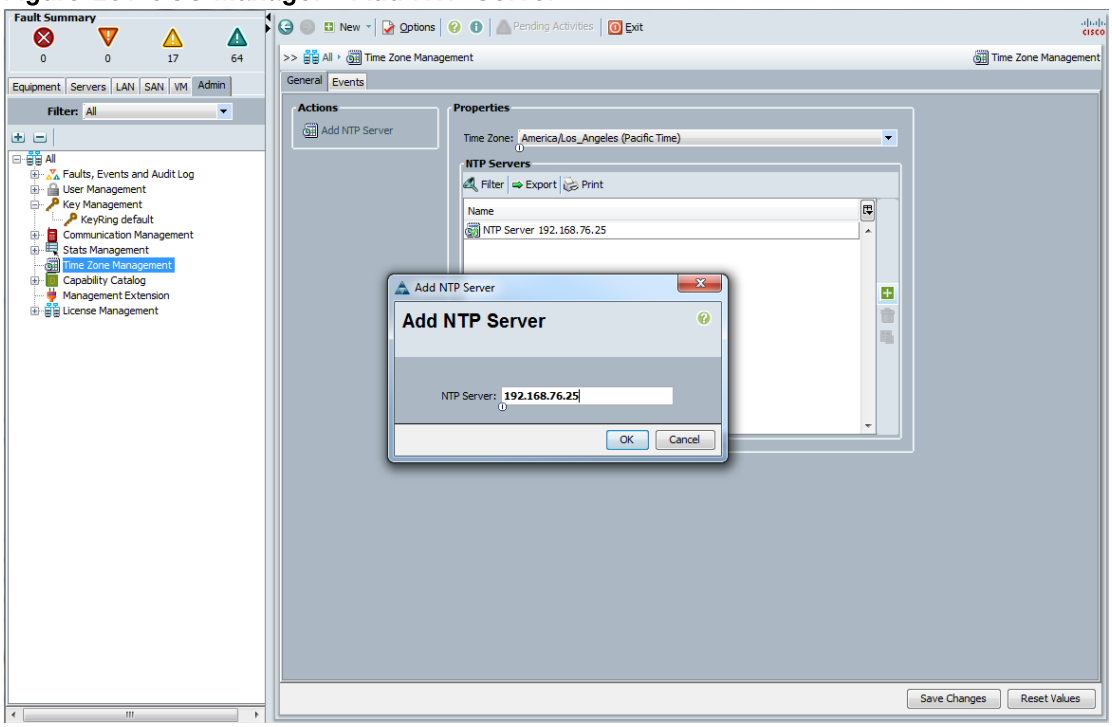
4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
5. Click OK to create the IP block.
6. Click OK in the confirmation message.

## Configure Timezone and NTP

To synchronize the Cisco UCS environment to the NTP server, complete the following steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes, and then click OK.
5. Click Add NTP Server.
6. Enter <<var_global_ntp_server_ip>> and click OK.
7. Click OK.

**Figure 157 UCS Manager – Add NTP Server**



### Chassis Connection Options

For the Cisco UCS 2200 Series Fabric Extenders, two configuration options are available: Pinning and Port Channel.

The Port Channel option provides better features for a shared infrastructure and should be the default. However, there are also use cases in which only a few large I/O streams are used, and for these the pinning option can provide a more stable performance. To pass the hwcct test from SAP for SAP HANA Scale-Out solutions, the Pinning mode is preferred. Use the Cisco UCS Performance Manager to monitor the usage of the connections and reconfigure the option on a global or per chassis basis.

### Chassis Connection in Pinning Mode

In the pinning mode, every VIC in a Cisco UCS B-Series server is pinned to an uplink cable from the fabric extender (or I/O module [IOM]) to the fabric interconnect based on the available number of uplinks. In most cases, the chassis are connected with four 10 Gigabit Ethernet cables per IOM to the fabric interconnect. The chassis backplane provides eight internal connections; a half-width blade can use one connection, and a full-width blade can use two connections and a full-width double-high blade can use 4 connections. Every connector is mapped to a VIC on the blade, and every VIC is represented by a virtual network interface connection (vCON) in Cisco UCS Manager.

To run SAP HANA on an infrastructure with four uplinks per IOM, use Figure 158 to Figure 160 to understand the pinning of IOM uplink ports (Port1 to Port4) and vCON. This pinning information is used when the virtual network interface card (vNIC) and virtual host bus adapter (vHBA) placement policy is defined.

**Figure 158 Cisco UCS 5108 Chassis with Eight Half-Width Blades (Cisco UCS B230 or B200)**

| | |
|---|---|
| Port1 - vCON1 | Port2 - vCON1 |
| Port3 - vCON1 | Port4 - vCON1 |
| Port1 - vCON1 | Port2 - vCON1 |
| Port3 - vCON1 | Port4 - vCON1 |

**Figure 159 Cisco UCS 5108 Chassis with Four Full-Width Blades (Cisco UCS B440 or B260)**

| | |
|---|---|
| Port1 - vCON1 | Port2 - vCON2 |
| Port3 - vCON1 | Port4 - vCON2 |
| Port1 - vCON1 | Port2 - vCON2 |
| Port3 - vCON1 | Port4 - vCON2 |

**Figure 160 Cisco UCS 5108 Chassis with Two Full-Width Double-High Blades (Cisco UCS B460)**

| | |
|---|---|
| Port1 – vCON3 | Port2 – vCON4 |
| Port3 – vCON1 | Port4 - vCON2 |

| | |
|---|---|
| Port1 – vCON3 | Port2 – vCON4 |
| Port3 - vCON1 | Port4 - vCON2 |

### Configure Server Discovery Policy

The Discovery Policy for the rack server is different than the discovery policy for blade chassis. For the rack server, the options define whether or not the system will discover the servers immediately or wait for user acknowledge. The blade chassis policy specifies the number of network links between the IO-Module and fabric interconnect and if those links are configured as independent links or as port channels.

### Edit Chassis Discovery Policy

Setting the discovery policy simplifies the process of adding Cisco UCS B-Series Chassis and additional fabric extenders for Cisco UCS C-Series connectivity.

To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Set the Link Grouping Preference to none for pinning mode.
5. Click Save Changes.
6. Click OK.

**Figure 161 UCS Manager – Chassis Discovery Policy**

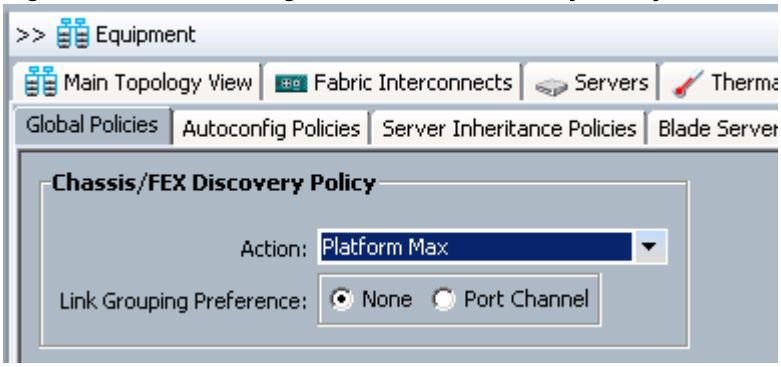
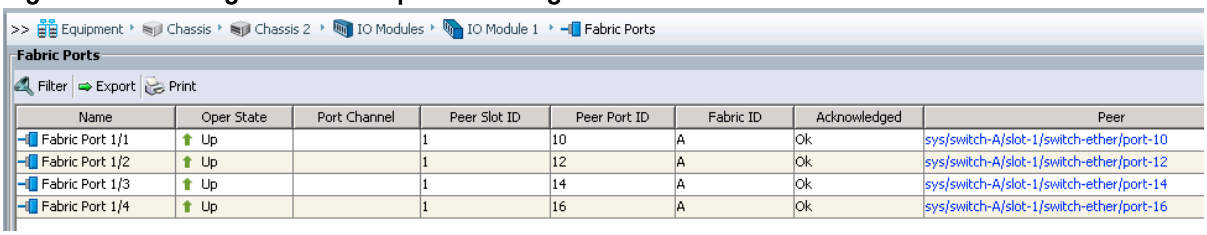
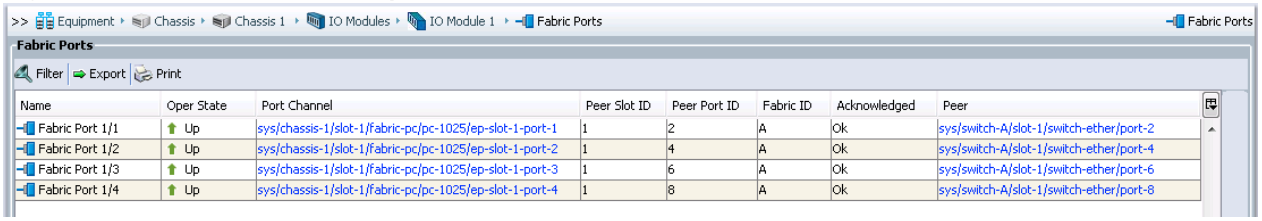


**Figure 162 Pinning Mode Example – Nothing Listed in the Port Channel Column**




| Name | Oper State | Port Channel | Peer Slot ID | Peer Port ID | Fabric ID | Acknowledged | Peer |
|---|---|---|---|---|---|---|---|
| Fabric Port 1/1 | Up | | 1 | 10 | A | Ok | sys/switch-A/slot-1/switch-ether/port-10 |
| Fabric Port 1/2 | Up | | 1 | 12 | A | Ok | sys/switch-A/slot-1/switch-ether/port-12 |
| Fabric Port 1/3 | Up | | 1 | 14 | A | Ok | sys/switch-A/slot-1/switch-ether/port-14 |
| Fabric Port 1/4 | Up | | 1 | 16 | A | Ok | sys/switch-A/slot-1/switch-ether/port-16 |

**Figure 163 Port Channel Example – The used Port Channel is Listed in the Column**



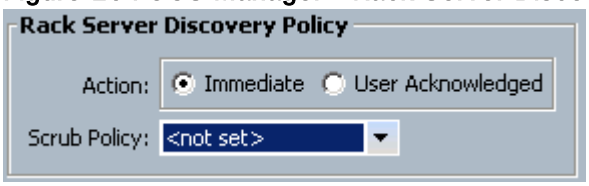

| Name | Oper State | Port Channel | Peer Slot ID | Peer Port ID | Fabric ID | Acknowledged | Peer |
|---|---|---|---|---|---|---|---|
| Fabric Port 1/1 | Up | sys/chassis-1/slot-1/fabric-pc/pc-1025/ep-slot-1-port-1 | 1 | 2 | A | Ok | sys/switch-A/slot-1/switch-ether/port-2 |
| Fabric Port 1/2 | Up | sys/chassis-1/slot-1/fabric-pc/pc-1025/ep-slot-1-port-2 | 1 | 4 | A | Ok | sys/switch-A/slot-1/switch-ether/port-4 |
| Fabric Port 1/3 | Up | sys/chassis-1/slot-1/fabric-pc/pc-1025/ep-slot-1-port-3 | 1 | 6 | A | Ok | sys/switch-A/slot-1/switch-ether/port-6 |
| Fabric Port 1/4 | Up | sys/chassis-1/slot-1/fabric-pc/pc-1025/ep-slot-1-port-4 | 1 | 8 | A | Ok | sys/switch-A/slot-1/switch-ether/port-8 |

## Edit the Cisco UCS Rack-Mount Server Discovery Policy

To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Rack Server Discovery Policy to Immediate.
4. Click Save Changes.
5. Click OK.

**Figure 164 UCS Manager – Rack Server Discovery Policy**




## Power Policy

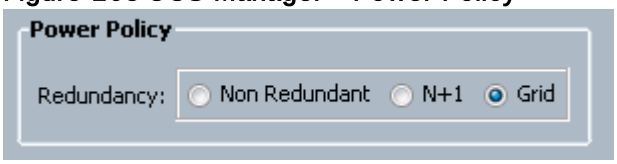
To run Cisco UCS with two independent power distribution units, the redundancy must be configured as a Grid. To configure the Power Policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Power Policy to Grid

4. Click Save Changes.

5. Click OK.

**Figure 165 UCS Manager – Power Policy**



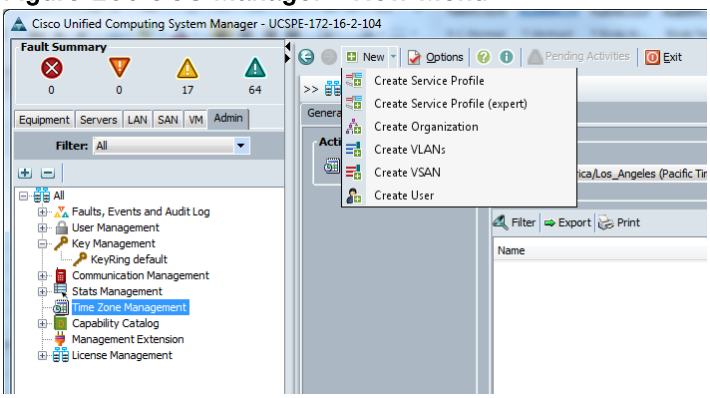

## Create a New Organization

To create an organization unite for ESX hosts, complete the following steps:

1. In Cisco UCS Manager, on the Tool bar click New.

2. From the drop-down menu select Create Organization.

**Figure 166 UCS Manager – New Menu**

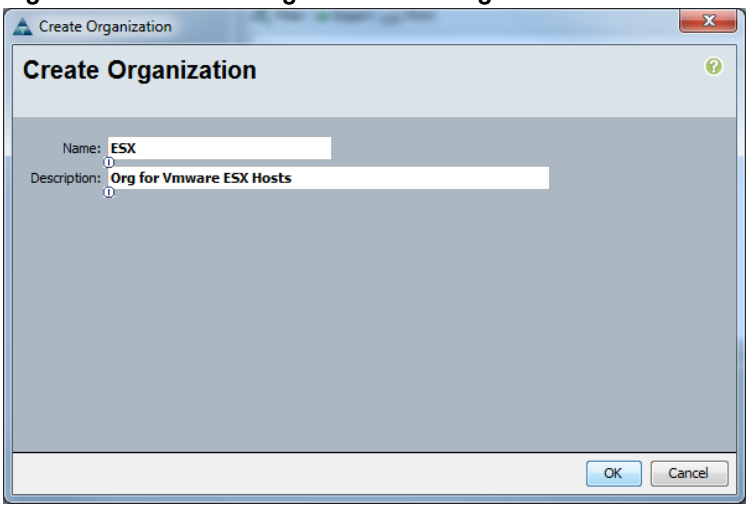



3. Enter the Name as <<var_esx_sub-org-name>>.

4. Optional Enter the Description as Org for VMware ESX Hosts.

5. Click OK to create the Organization.

Figure 167 UCS Manager – Create Organization




## Configure LAN Settings

This section details the LAN specific configuration of Cisco UCS.

Table 29 the required information to setup the LAN of the Cisco UCS in this Cisco UCS Integrated Infrastructure.

Table 29 Information to Setup Cisco UCS in the Reference Architecture

| Name | Variable |
|---|---|
| Name of the Eth Adapter Policy for SAP HANA Scale-Out | <<var_eth_adapter_policy_name>> |
| Name of the Global MAC Address Pool | <<var_global_mac_pool_name>> |
| Name of the MAC Address Pool for the Access/Client Network Group | <<var_access_mac_pool_name>> |
| Name of the BestEffort Network Policy | <<var_ucs_besteffort_policy_name>> |
| Name of the Platinum Network Policy | <<var_ucs_platinum_policy_name>> |
| Name of the Gold Network Policy | <<var_ucs_gold_policy_name>> |
| Name of the Silver Network Policy | <<var_ucs_silver_policy_name>> |
| Name of the Bronze Network Policy | <<var_ucs_bronze_policy_name>> |
| Name of the Global Admin VLAN | <<var_ucs_admin_vlan_name>> |
| Global Administration Network VLAN ID | <<var_admin_vlan_id>> |
| Name of the Temporary VLAN | <<var_ucs_temp_vlan_name>> |

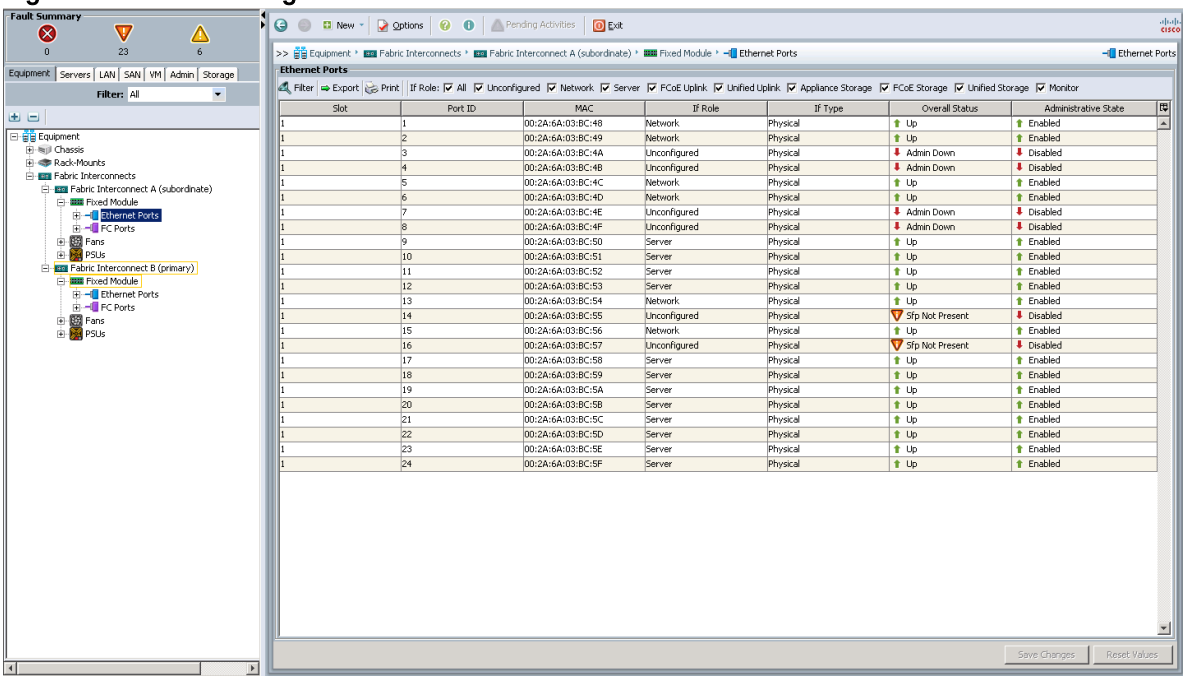
| Name | Variable |
|---|---|
| Temporary used VLAN ID | <<var_temp_vlan_id>> |
| Name of the NFS VLAN for ESX and other use cases | <<var_ucs_esx_nfs_vlan_name>> |
| VMware ESX Storage access Network VLAN ID | <<var_esx_nfs_vlan_id>> |
| Name of the Vmotion VLAN | <<var_ucs_vmotion_vlan_name>> |
| VMware Vmotion Network VLAN ID | <<var_vmotion_vlan_id>> |
| Name of the Global Backup VLAN | <<var_ucs_backup_vlan_name>> |
| Global Backup Network | <<var_backup_vlan_id>> |
| Name of the Nexus1000V Control VLAN | <<var_ucs_n1k_control_vlan_name>> |
| Cisco Nexus1000V Control Network VLAN ID | <<var_n1k_control_vlan_id>> |
| Name of the Network Group for Admin tasks | <<var_ucs_admin_zone>> |
| Name of the Network Group for Backup tasks | <<var_ucs_backup_zone>> |
| Name of the Network Group for Client Access | <<var_ucs_client_zone>> |
| Name of the Network Group for HANA internal traffic | <<var_ucs_internal_zone>> |
| Name of the Network Group for HANA replication traffic | <<var_ucs_replication_zone>> |
| Name of the vNIC on Fabric A for ESXi Admin traffic | <<var_ucs_esx_a_vnic_name>> |
| Name of the vNIC on Fabric B for ESXi Admin traffic | <<var_ucs_esx_b_vnic_name>> |
| Name of the vNIC on Fabric A for ESXi Application/VM traffic | <<var_ucs_esx_a_appl_vnic_name>> |
| Name of the vNIC on Fabric B for ESXi Application/VM traffic | <<var_ucs_esx_b_appl_vnic_name>> |
| Name of the LAN Connection Policy for ESX server | <<var_ucs_esx_lan_connect_policy_name>> |

### Configure LAN Uplink Ports

To enable uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port (Ports 1,2,5,6,13,15)
5. Click Yes to confirm uplink ports and click OK.
6. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
7. Expand Ethernet Ports.
8. Select ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
9. Click Yes to confirm the uplink ports and click OK.

**Figure 168 UCS Manager – List of Ethernet Ports on Fabric Interconnect A**



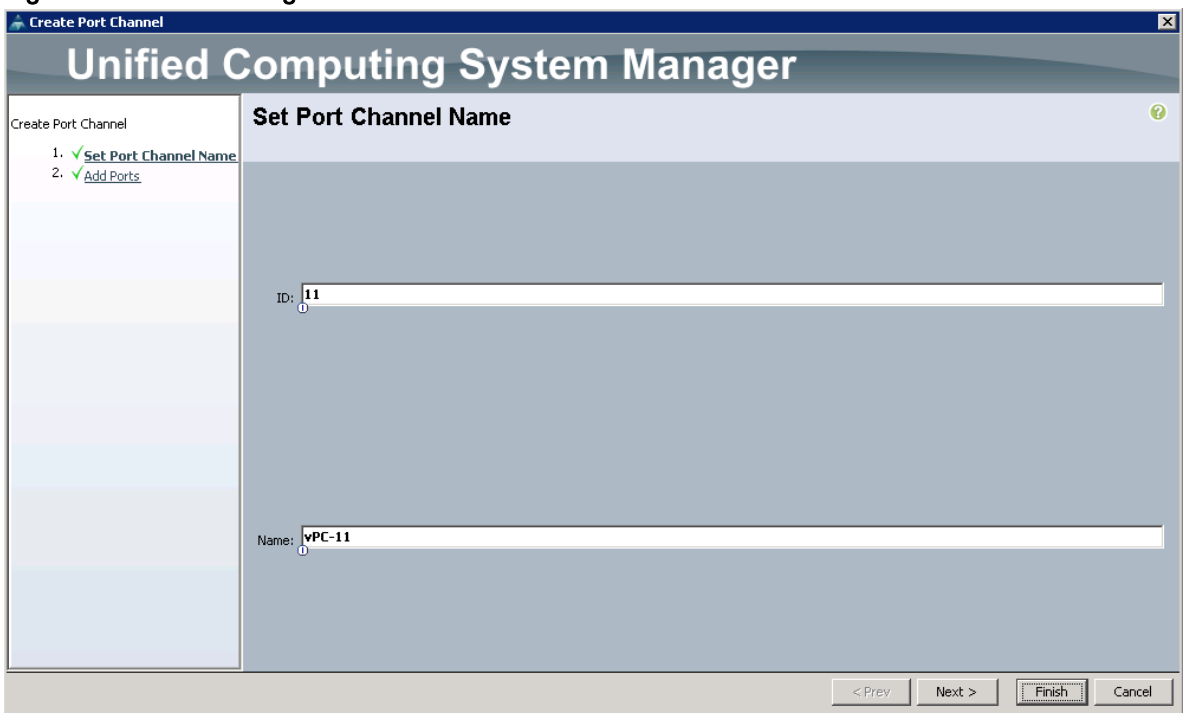

## Create Uplink Port Channels to Cisco Nexus Switches

A separate Uplink Port Channel is required to move admin traffic and application traffic out of the Cisco UCS environment. For example, create Port channel 11 on Fabric Interconnect A and Port channel 12 on Fabric Interconnect B for infrastructure admin networks. Create additional Port channel 13 on Fabric Interconnect A and Port channel 14 on Fabric Interconnect B for all application networks.

To configure the port channels for admin traffic out of the Cisco UCS environment, complete the following steps:

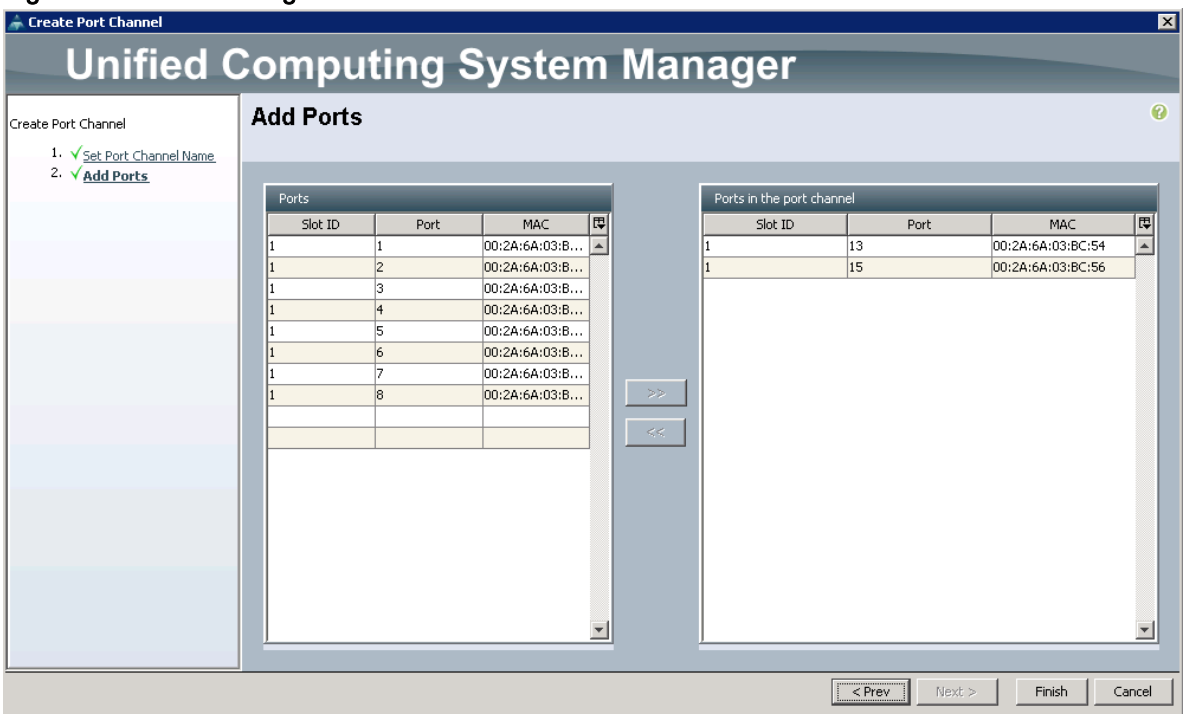
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter 11 as the unique ID of the port channel.
6. Enter vPC-11 as the name of the port channel.
7. Click Next.

**Figure 169 UCS Manager – Set Port Channel Name**



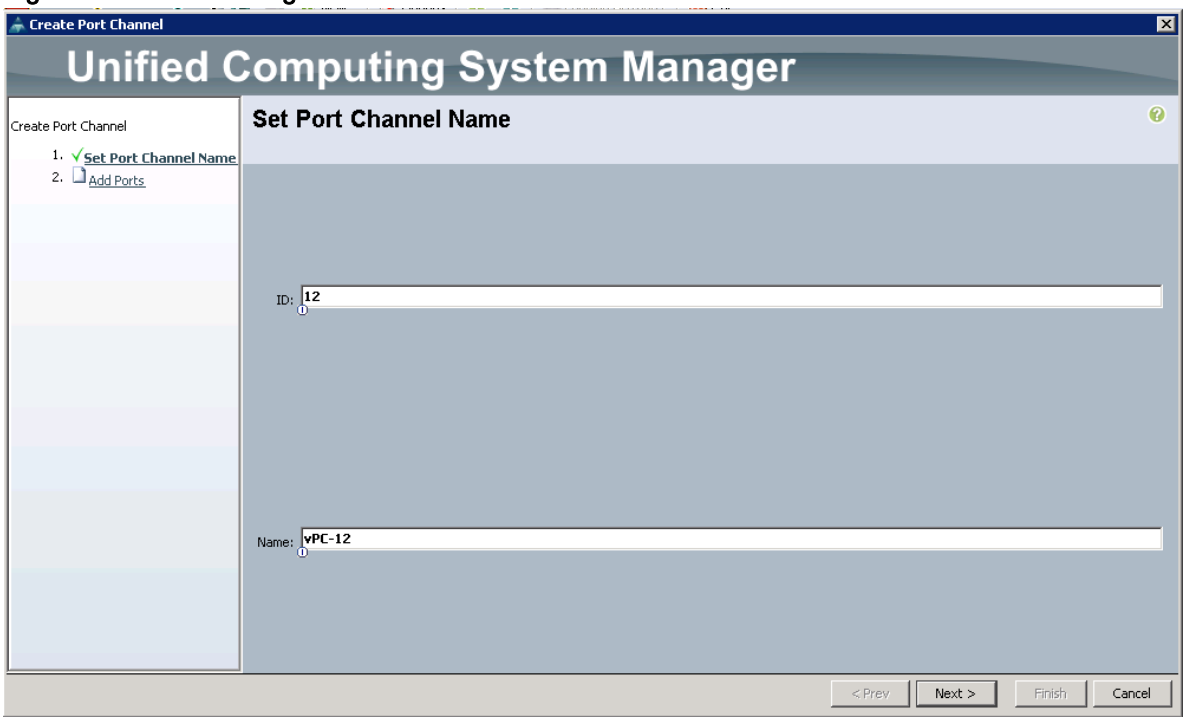

8. Select the following ports to add to the port channel:
   - Slot ID 1 and port 13
   - Slot ID 1 and port 15
9. Click >> to add the ports to the port channel.

Figure 170 UCS Manager – Add Ports to the Port Channel




10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 12 as the unique ID of the port channel.
16. Enter vPC-12 as the name of the port channel.
17. Click Next.

Figure 171 UCS Manager – Set Port Channel Name



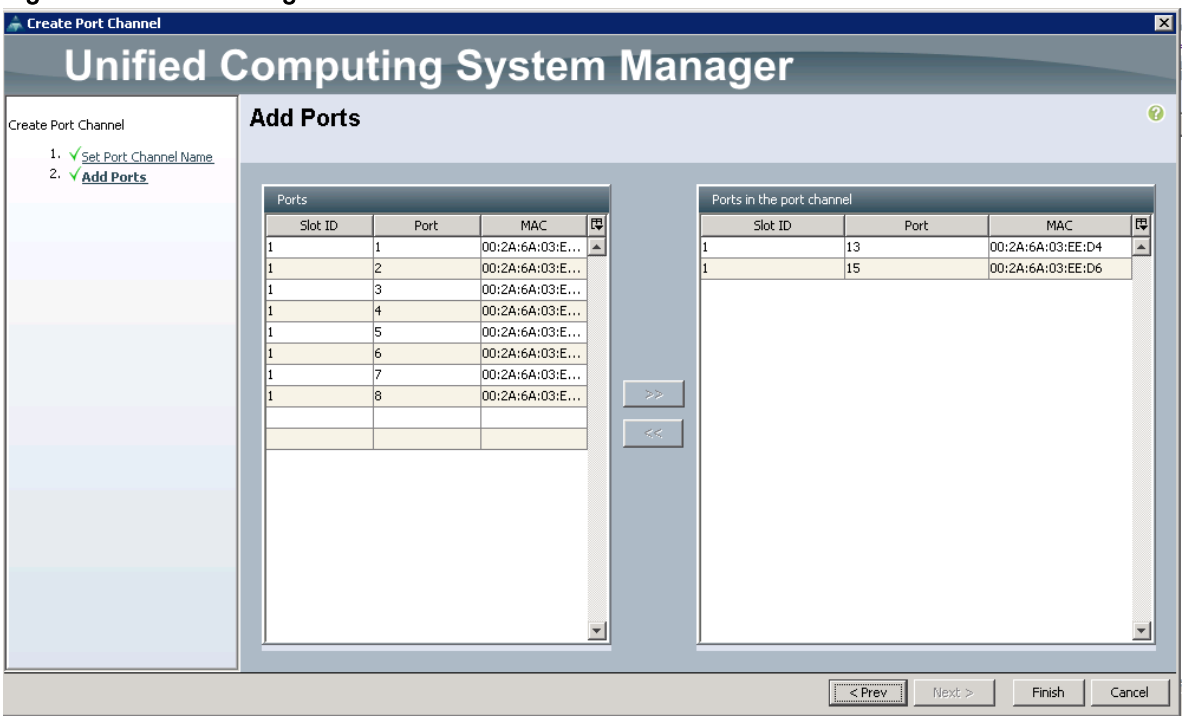

18. Select the following ports to add to the port channel:

— Slot ID 1 and port 13

— Slot ID 1 and port 15

19. Click >> to add the ports to the port channel.

Figure 172 UCS Manager – Add Ports to the Port Channel

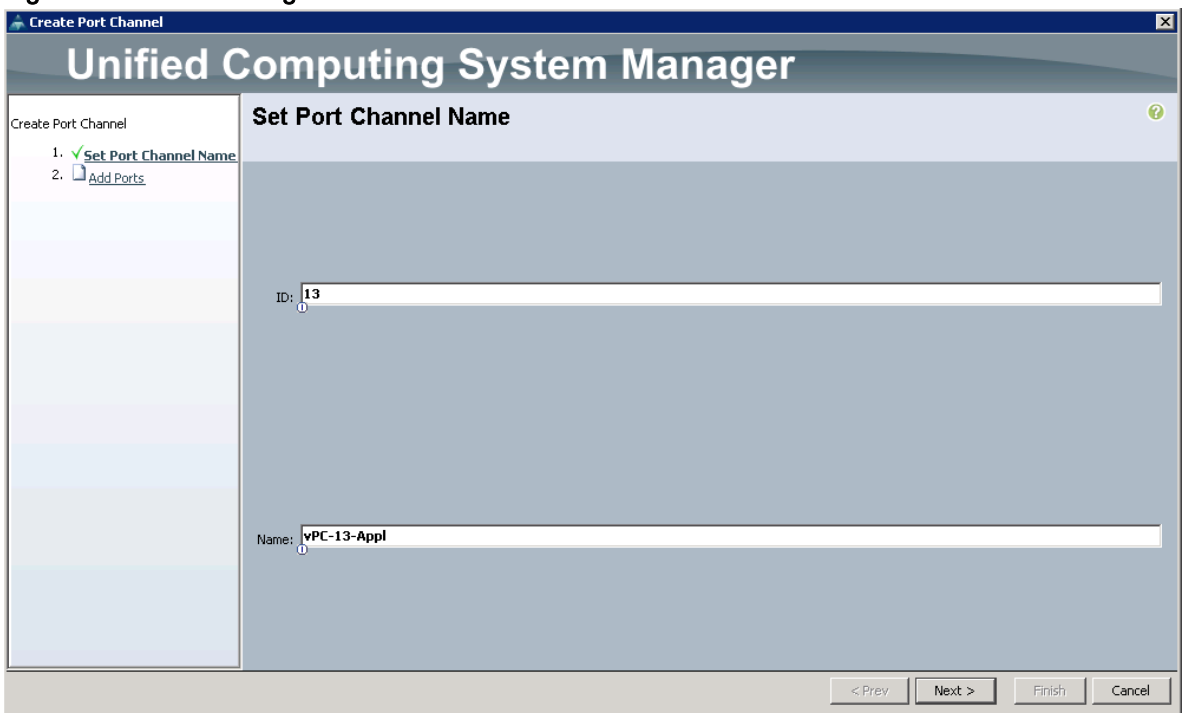



20. Click Finish to create the port channel.
21. Click OK.

To create a port channel for application traffic, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter 13 as the unique ID of the port channel.
6. Enter vPC-13-Appl as the name of the port channel.
7. Click Next.

Figure 173 UCS Manager – Set Port Channel Name




8. Select the following ports to add to the port channel:

— Slot ID 1 and port 1

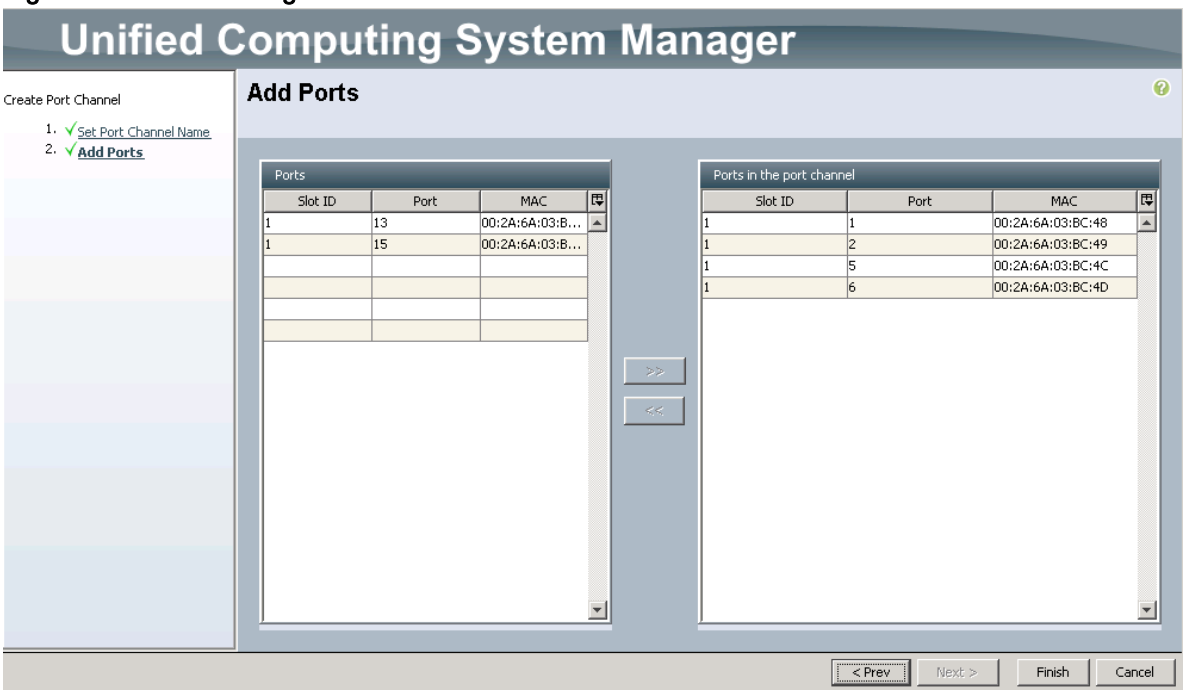
— Slot ID 1 and port 2

— Slot ID 1 and port 5

— Slot ID 1 and port 6

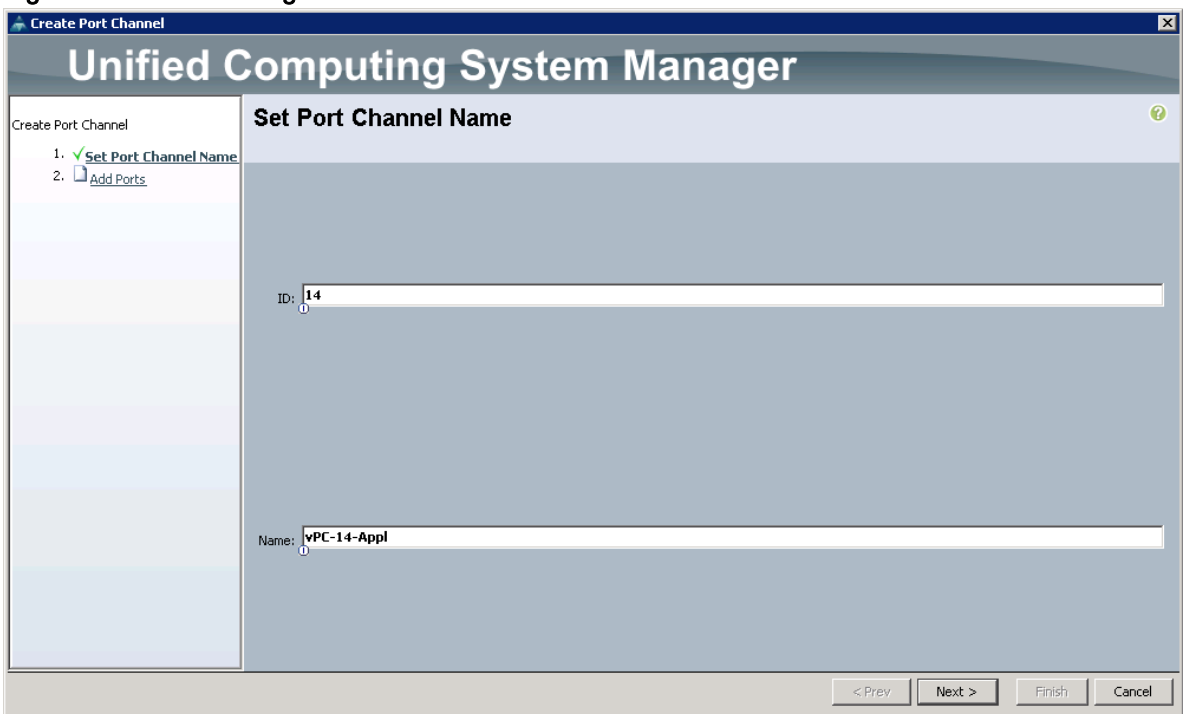
9. Click >> to add the ports to the port channel.

Figure 174 UCS Manager – Add Ports to the Port Channel




10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 14 as the unique ID of the port channel.
16. Enter vPC-14-Appl as the name of the port channel.
17. Click Next.

Figure 175 UCS Manager – Set Port Channel Name




18. Select the following ports to be added to the port channel:

— Slot ID 1 and port 1

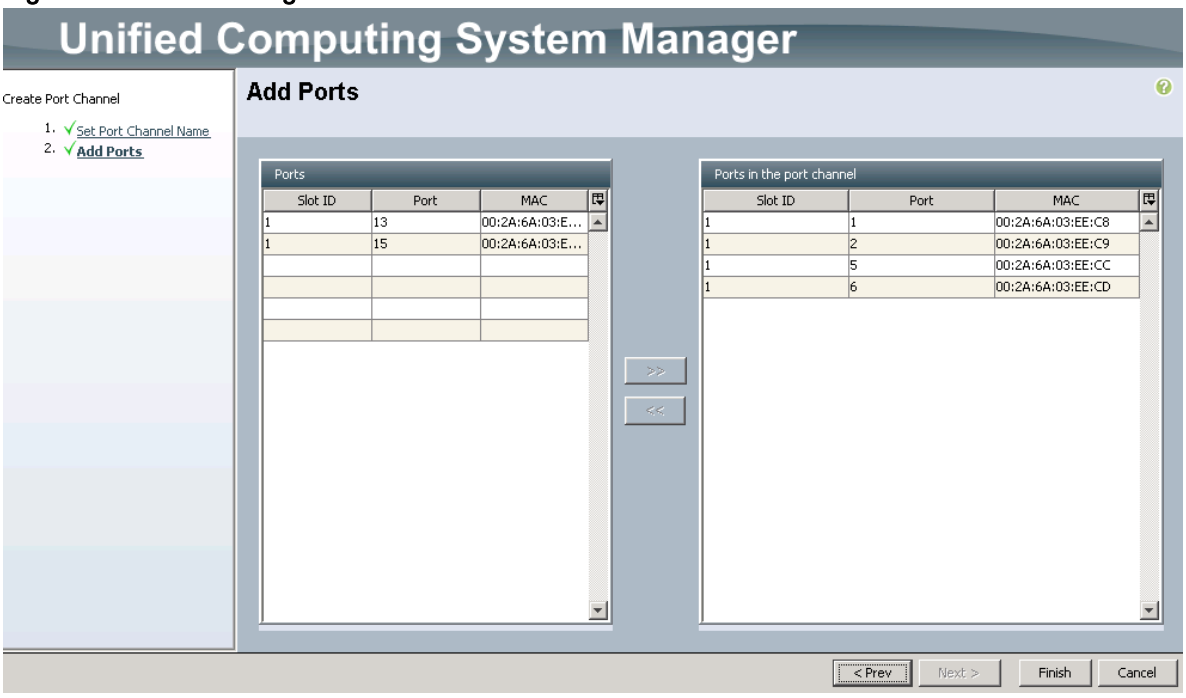
— Slot ID 1 and port 2

— Slot ID 1 and port 5

— Slot ID 1 and port 6

19. Click >> to add the ports to the port channel.

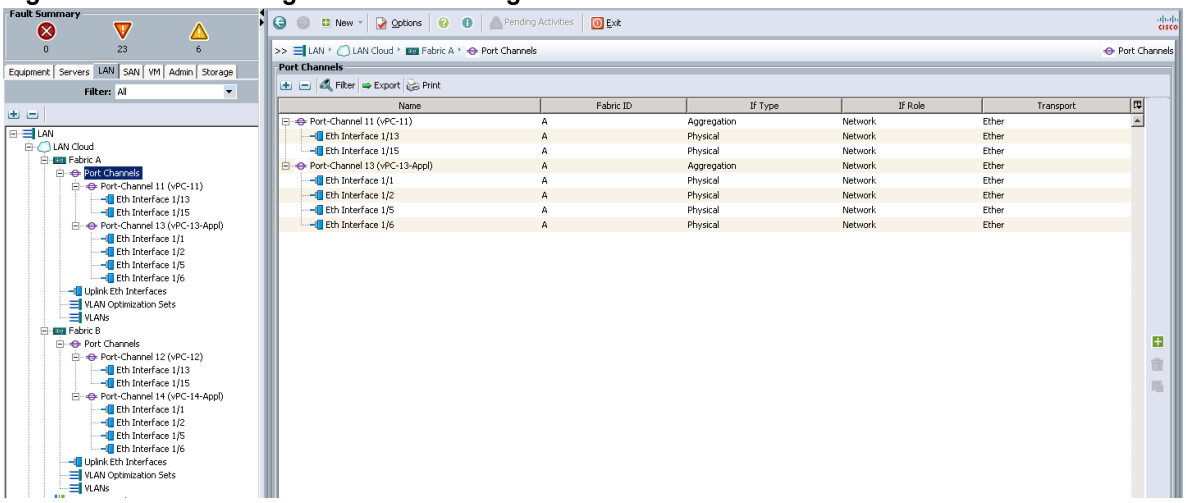
**Figure 176 UCS Manager – Add Ports to the Port Channel**




20. Click Finish to create the port channel.

21. Click OK.

**Figure 177 UCS Manager – List of Configured Port Channels**




## Ethernet Adapter Policy Configuration

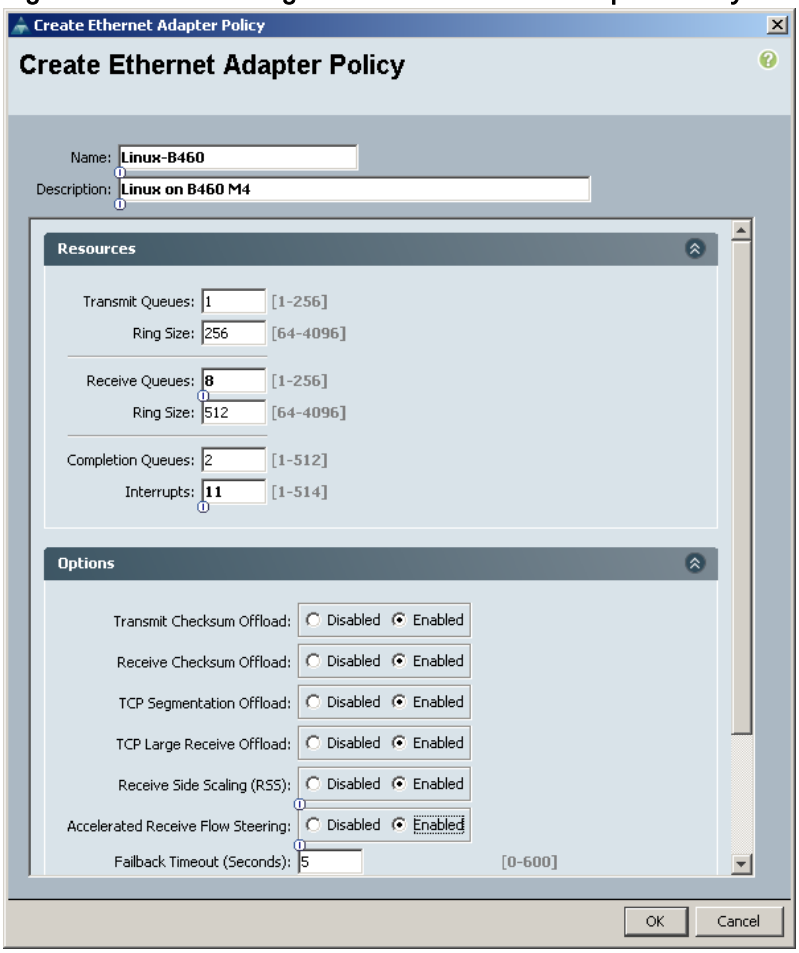
The Ethernet Adapter Policy must be used for the SAP HANA internal network to provide best network performance with SUSE and Red Hat Linux.

To create an Ethernet Adapter Policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Adapter Policies.
4. Select Create Ethernet Adapter Policy.
5. Enter <<var_eth_adapter_policy_name>> as the Ethernet Adapter policy name.
6. Expand Resources → Change the Receive Queues to 8.
7. Change the Interrupts to 11.
8. Expand Options → Change Receive Side Scaling (RSS) to Enabled
9. Change Accelerated Receive Flow Steering to Enabled
10. Click OK to create the Ethernet Adapter policy.
11. Click OK.

The screenshot below shows a newly created Ethernet Adapter Policy Linux-B460 with RSS, Receive Queues and Interrupt values.

Figure 178 UCS Manager – Create Ethernet Adapter Policy



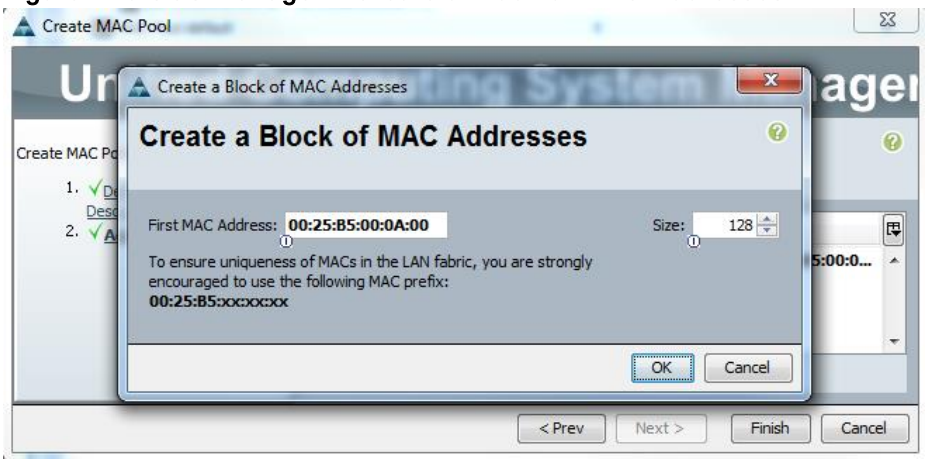

## Create MAC Address Pool(s)

To configure the necessary MAC address pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address poolError! Reference source not found..
5. Enter <<var_global_mac_pool_name>> as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Choose Assignment Order Sequential.

8. Click Next.
9. Click Add.
10. Specify a starting MAC address.
11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

**Figure 179 UCS Manager – Create a Block of MAC Addresses**



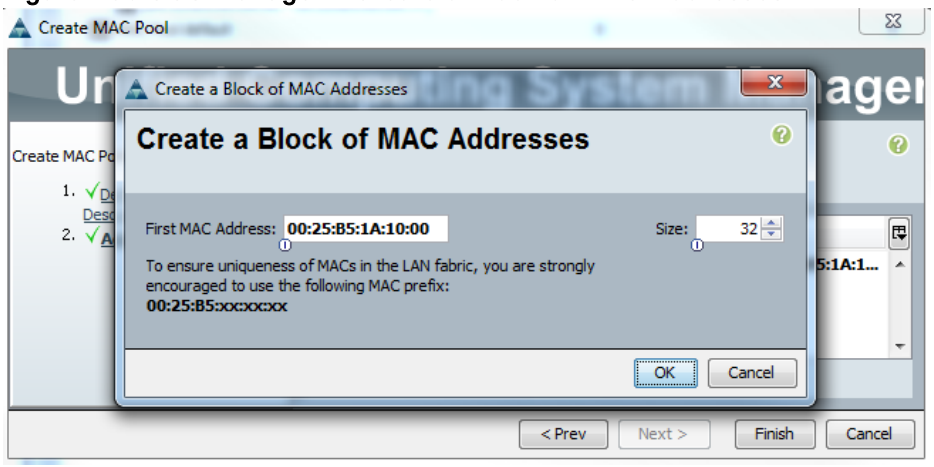

12. Click OK.
13. Click Finish.
14. In the confirmation message, click OK.

You can also define a separate MAC address pool for each Network Zone. The recommendation is to create at least a separate Pool for access Network, as MAC address of the vNIC must be unique in the data center. To create a MAC address pool for each network zone and to configure the MAC address pools for the access vNIC, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool
5. Enter <<var_access_mac_pool_name>> as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Choose Assignment Order Sequential

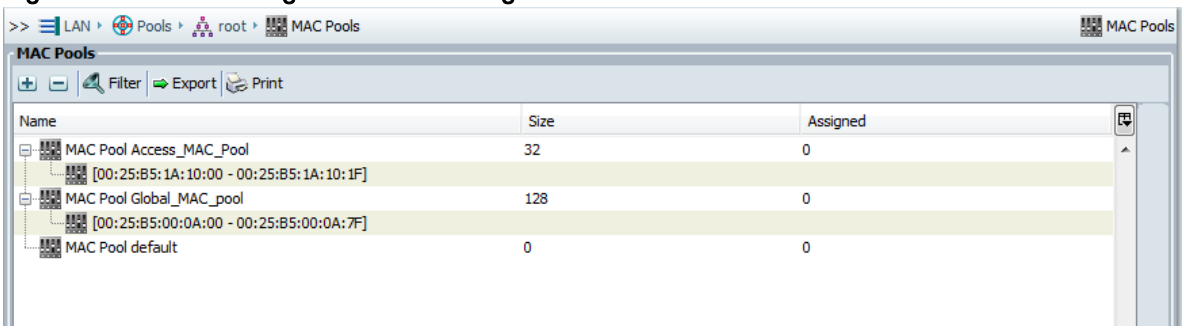
8. Click Next.
9. Click Add.
10. Specify a starting MAC address.
11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

**Figure 180 UCS Manager – Create a Block of MAC Addresses**




12. Click OK.
13. Click Finish.

**Figure 181 UCS Manager – List of configured MAC Address Pools**



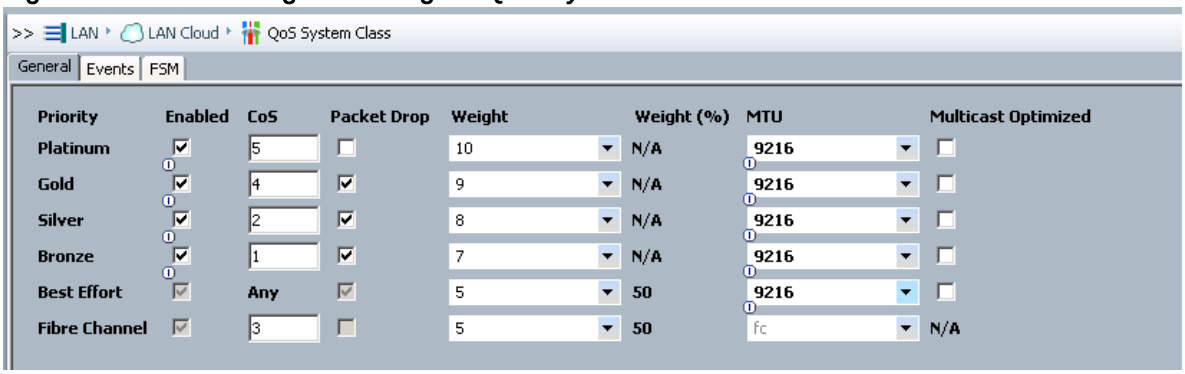

## Configure QoS System Class and Jumbo Frames

There are at least two options to enable jumbo frames on network equipment in the datacenter. The first option is to do it only when absolutely required. The second option is to enable jumbo frames on all networking equipment, so that the end-points can use it if required. In this data center reference architecture all components are configured with jumbo frames and the specific MTU size to use is done on the vNIC level.

To configure jumbo frames and enable quality of service in the Cisco UCS fabric, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the General tab.
4. On the MTU Column, enter 9216 in the box.
5. Check Enabled Under Priority for Platinum (and all other Priorities you want to use).
6. Uncheck Packet Drop for Platinum.
7. Click Save Changes in the bottom of the window.
8. Click OK.

**Figure 182 UCS Manager – Configure QoS System Classes**

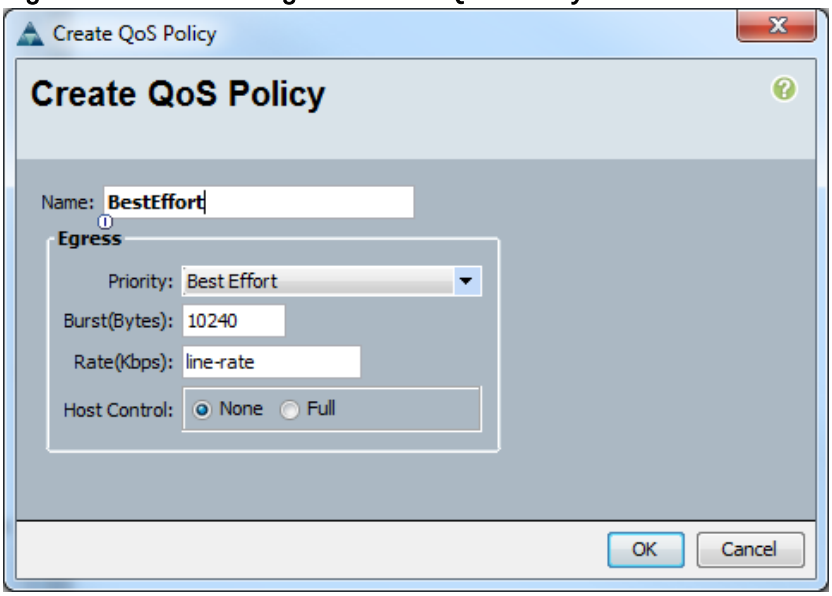



## Configure QoS Policies

To map the defined QoS System Class to a vNIC a QoS policy is required. To configure QoS policies, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > Policies.
3. Right-click QoS Policies.
4. Select Create QoS Policy.
5. Enter <<var_ucs_besteffort_policy_name>> as the name of the QoS Policy.
6. In the Priority section, select Best Effort.

Figure 183 UCS Manager – Create QoS Policy BestEffort




7. Click OK.
8. Click OK.
9. Right-click QoS Policies.
10. Select Create QoS Policy.
11. Enter <<var_ucs_platinum_policy_name>> as the name of the QoS Policy.
12. In the Priority section, select Platinum.

Figure 184 UCS Manager – Create QoS Policy Platinum




13. Click OK.

14. Click OK.

If other QoS System Classes are enabled, additional QoS policies are required. To create additional QoS policies, complete the following steps:

1. Right-click QoS Policies.
2. Select Create QoS Policy.
3. Enter <<var_ucs_gold_policy_name>> as the name of the QoS Policy.
4. In the Priority section, select Gold.

Figure 185 UCS Manager – Create QoS Policy Gold




5. Click OK.
6. Click OK.
7. Right-click QoS Policies.
8. Select Create QoS Policy.
9. Enter <<var_ucs_silver_policy_name>> as the name of the QoS Policy.
10. In the Priority section, select Silver.

Figure 186 UCS Manager – Create QoS Policy Silver




11. Click OK.
12. Click OK.
13. Right-click QoS Policies.
14. Select Create QoS Policy.
15. Enter <<var_ucs_bronze_policy_name>> as the name of the QoS Policy.
16. In the Priority section, select Bronze.

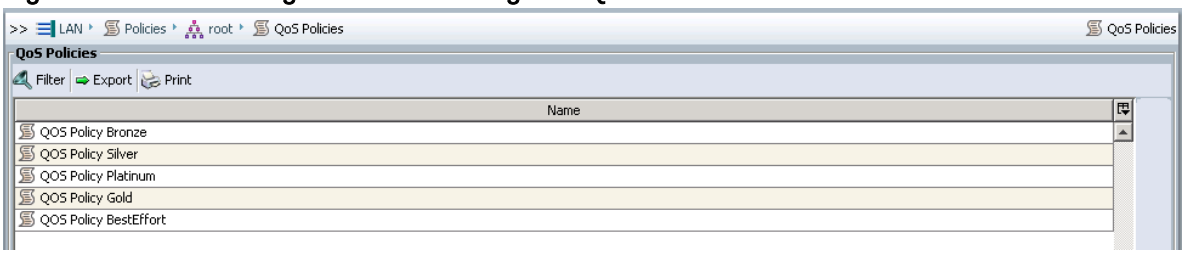
Figure 187 UCS Manager – Create QoS Policy Bronze




17. Click OK.

18. Click OK.

Figure 188 UCS Manager – List of Configured QoS Policies




## Configure VLANs and vNIC Templates

Within the Cisco UCS, all networks are reflected by defined VLANs. In this section, you will create only the Infrastructure related VLANs. All Tenant or SAP System related networks are defined in a later chapter in this document.

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, complete the following steps:

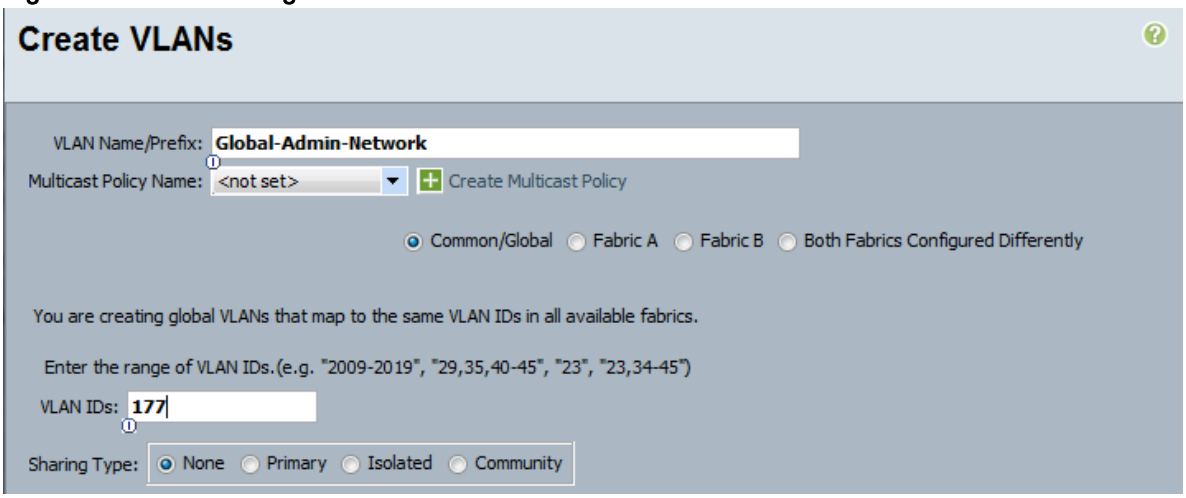
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

2. Select LAN > LAN Cloud.

3. Right-click VLANs.

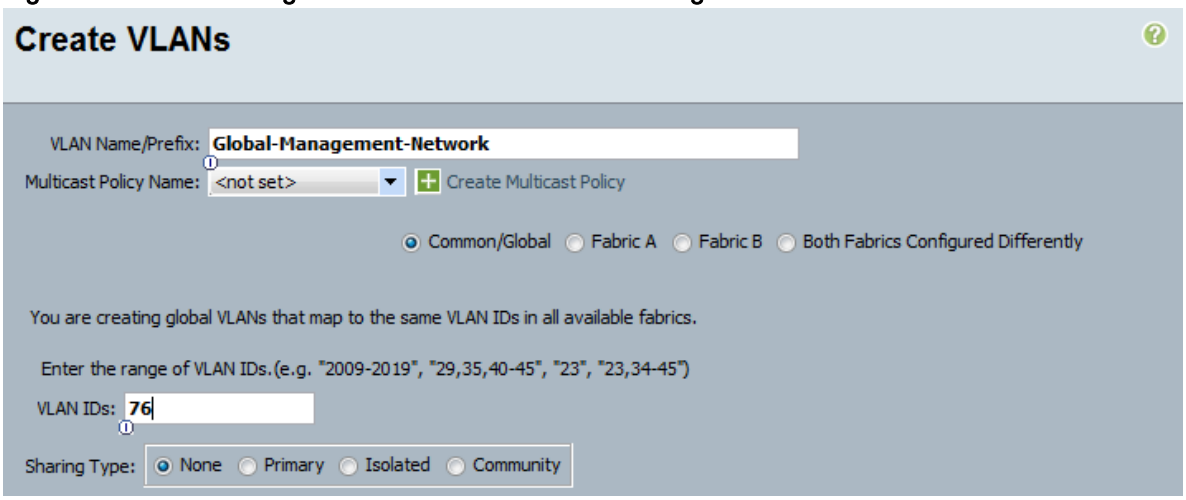
4. Select Create VLANs.
5. Enter <<var_ucs_admin_vlan_name>> as the name of the VLAN to be used for administration traffic.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter <<var_admin_vlan_id>> as the ID of the global administration VLAN.
8. Keep the Sharing Type as None.
9. Click OK, and then click OK again.

Figure 189 UCS Manager – Create VLAN Global-Admin-Network




10. Right-click VLANs.
11. Select Create VLANs.
12. Enter <<var_ucs_management_vlan_name>> as the name of the VLAN to be used for infrastructure management.
13. Keep the Common/Global option selected for the scope of the VLAN.
14. Enter the <<var_management_vlan_id>> for the infrastructure management VLAN.
15. Keep the Sharing Type as None.
16. Click OK, and then click OK again.

Figure 190 UCS Manager – Create VLAN Global-Management-Network




17. Right-click VLANs.
18. Select Create VLANs.
19. Enter <<var_ucs_esx_nfs_vlan_name>> as the name of the VLAN to be used for NFS.
20. Keep the Common/Global option selected for the scope of the VLAN.
21. Enter the <<var_esx_nfs_vlan_id>> for the NFS VLAN.
22. Keep the Sharing Type as None.
23. Click OK, and then click OK again.

Figure 191 UCS Manager – Create VLAN Global-ESX-NFS-Network




24. Right-click VLANs.

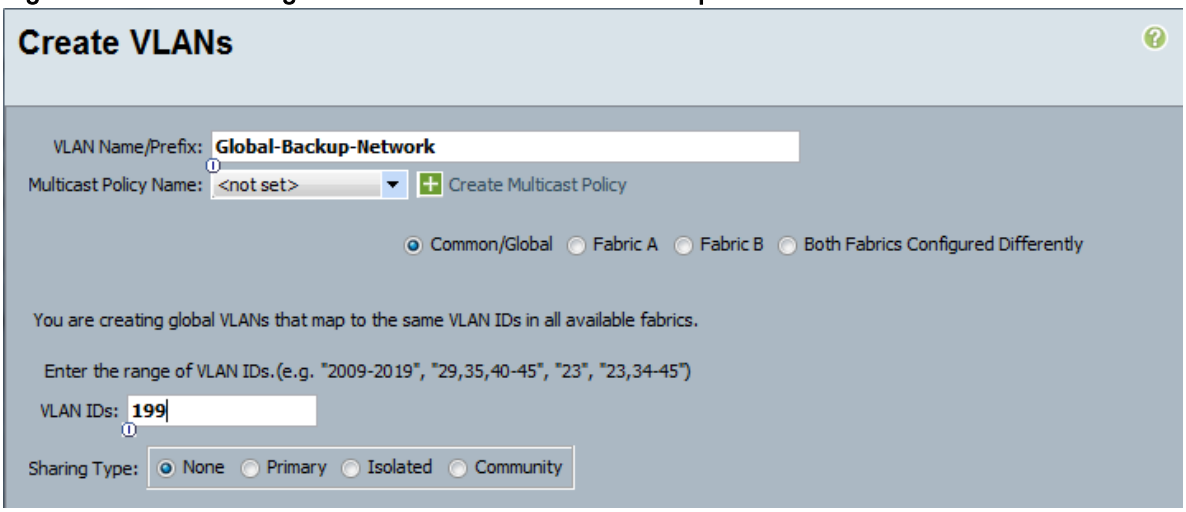
25. Select Create VLANs.
26. Enter <<var_ucs_vmotion_vlan_name>> as the name of the VLAN to be used for vMotion.
27. Keep the Common/Global option selected for the scope of the VLAN.
28. Enter the <<var_vmotion_vlan_id>> as the ID of the vMotion VLAN.
29. Keep the Sharing Type as None.
30. Click OK, and then click OK again.

Figure 192 UCS Manager – Create VLAN Global-vMotion-Network



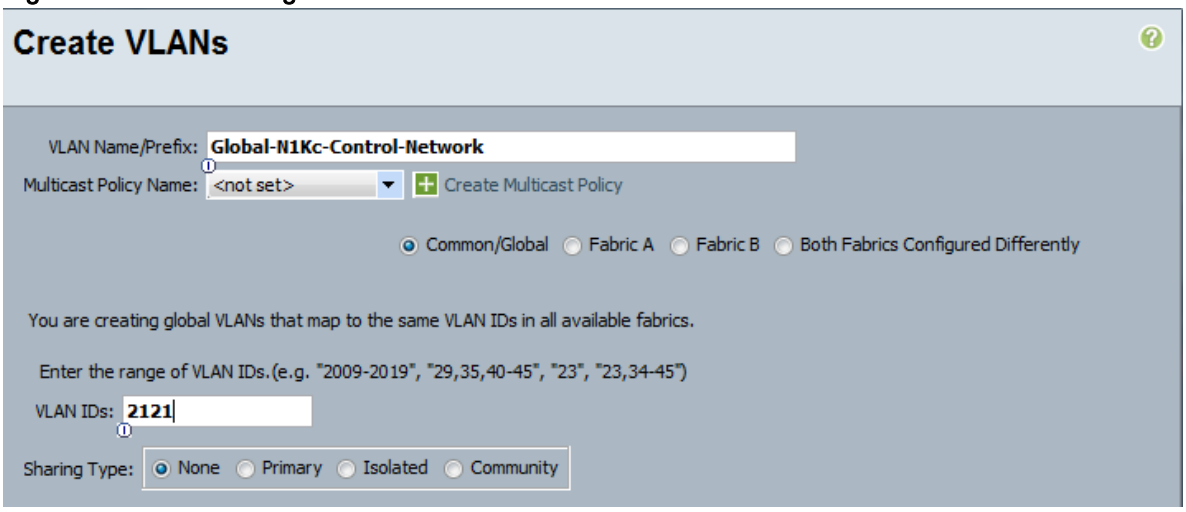

31. Right-click VLANs.
32. Select Create VLANs.
33. Enter <<var_ucs_backup_vlan_name>> as the name of the VLAN to be used for Backup.
34. Keep the Common/Global option selected for the scope of the VLAN.
35. Enter the <<var_backup_vlan_id>> as the ID of the vMotion VLAN.
36. Keep the Sharing Type as None.
37. Click OK, and then click OK again.

Figure 193 UCS Manager – Create VLAN Global-Backup-Network




38. Right-click VLANs.
39. Select Create VLANs.
40. Enter <<var_ucs_n1k_control_vlan_name>> as the name of the VLAN to be used for Nexus 1000v Control.
41. Keep the Common/Global option selected for the scope of the VLAN.
42. Enter the <<var_n1k_control_vlan_id>> as the ID of the vMotion VLAN.
43. Keep the Sharing Type as None.
44. Click OK, and then click OK again.

Figure 194 UCS Manager – Create VLAN Global-N1Kv-Control-Network




45. Right-click VLANs.

46. Select Create VLANs.
47. Enter <<var_ucs_temp_vlan_name>> as the name of the VLAN to be used for Temporary purposes.
48. Keep the Common/Global option selected for the scope of the VLAN.
49. Enter the <<var_temp_vlan_id>> as the ID of the vMotion VLAN.
50. Keep the Sharing Type as None.
51. Click OK, and then click OK again.

**Figure 195 UCS Manager – Create VLAN Temp-Network**

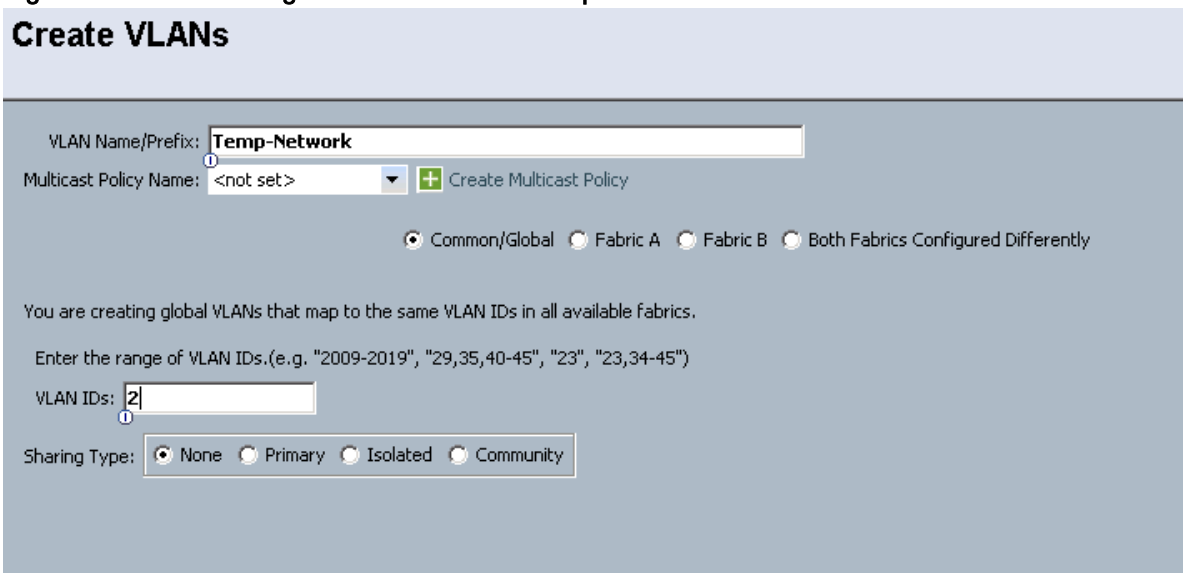
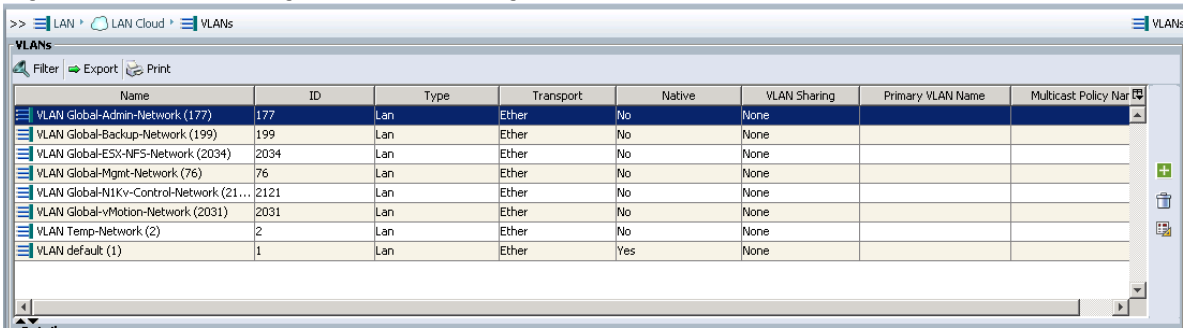



**Figure 196 UCS Manager – List of Configured VLANs**




## Create VLAN Groups

To map VLANs to specific Uplink ports or port channels on the Cisco UCS Fabric Interconnects, you need to define VLAN Groups. The following VLAN Groups were defined in this solution.

You will need to provide the following information previously defined:

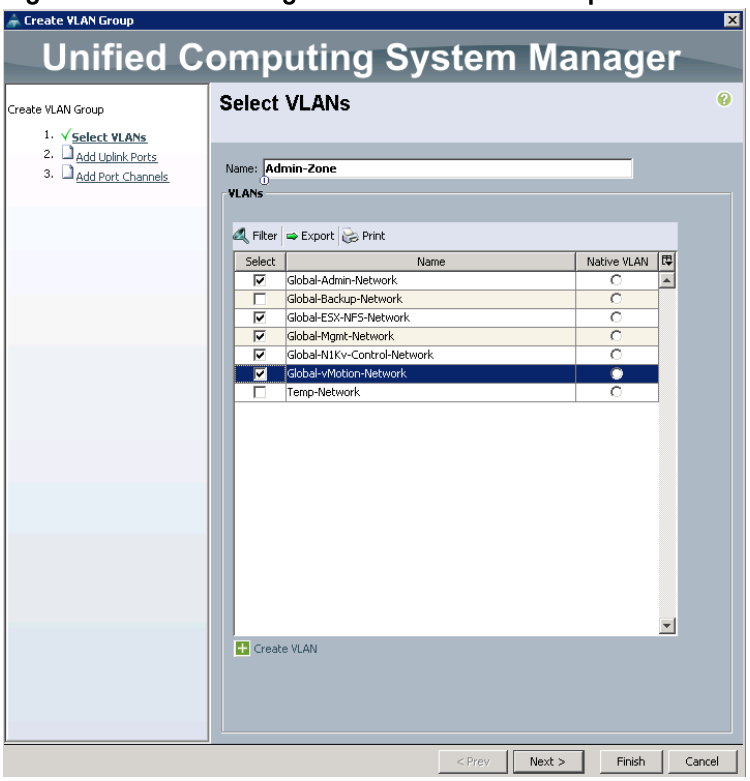
- Admin Zone

- Client Zone
- Internal Zone
- Backup Network
- Replication Network

To configure the necessary VLAN Groups for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. In this procedure, five VLAN Groups are created. Based on the solution requirement create VLAN groups, it not required to create all five VLAN groups.
3. Select LAN > LAN Cloud.
4. Right-click VLAN Groups
5. Select Create VLAN Groups.
6. Enter <<var_ucs_admin_zone>> as the name of the VLAN Group used for Infrastructure network.
7. Select <<var_ucs_management_vlan_name>> ,<<var_ucs_admin_vlan_name>>, <<var_ucs_esx_nfs_vlan_name>>, <<var_ucs_vmotion_vlan_name>>, <<var_ucs_n1kv_control_vlan_name>>

Figure 197 UCS Manager – Create VLAN Group Admin-Zone

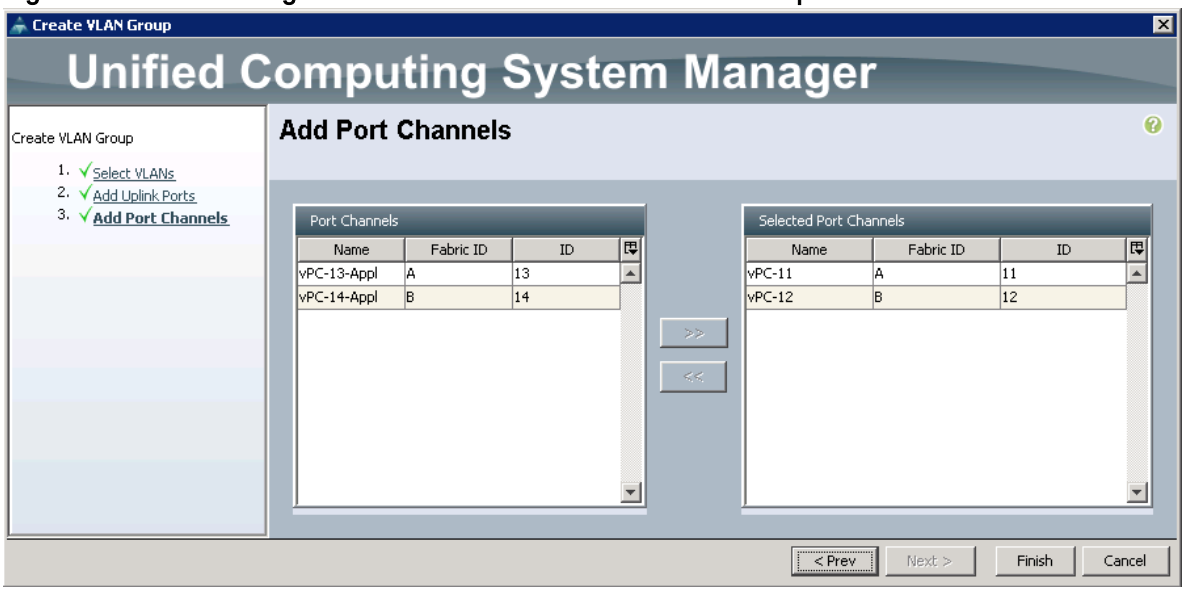



8. Click Next.

9. Click Next on Add Uplink Ports.

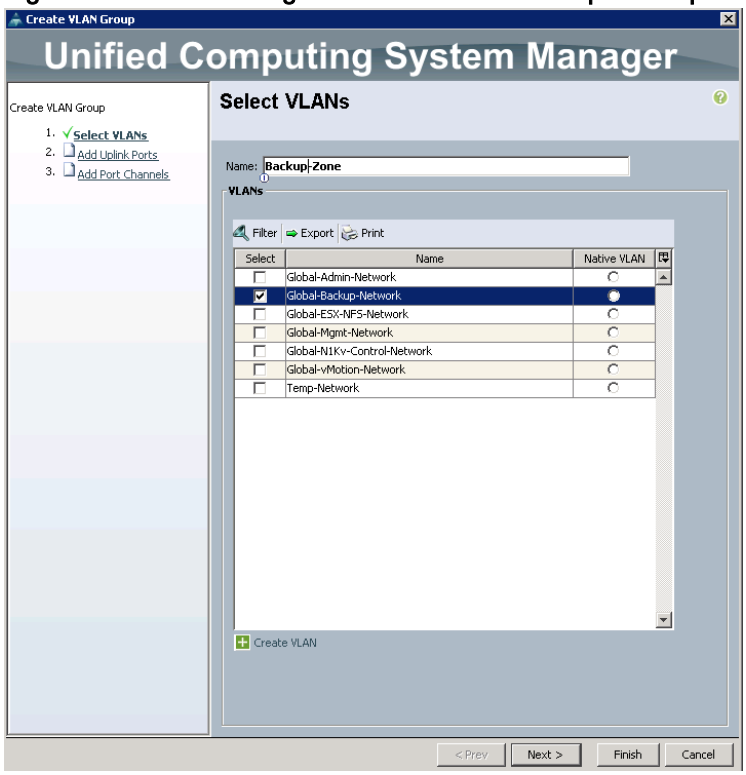
10. Choose Port channels Created for Admin Network (vpc-11 and vpc-12).

Figure 198 UCS Manager – Add Port Channels to a VLAN Group



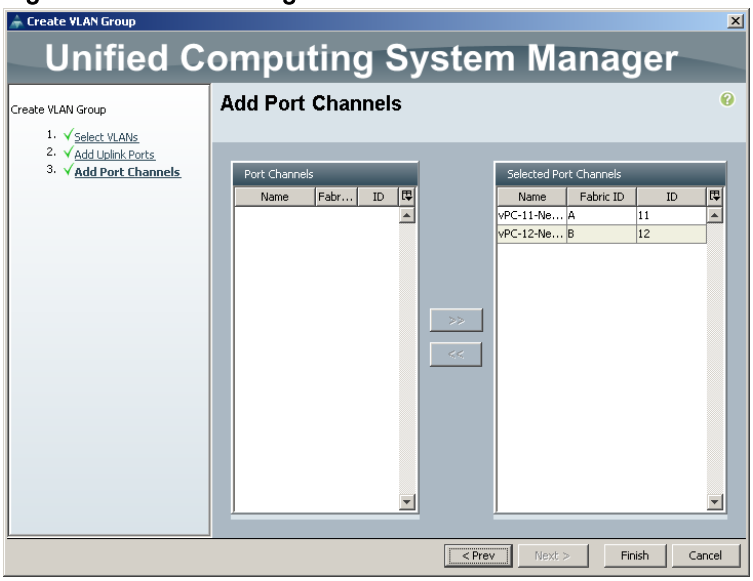
11. Click Finish.
12. Right-click VLAN Groups.
13. Select Create VLAN Groups.
14. Enter <<var_ucs_backup_zone>> as the name of the VLAN Group used for Infrastructure related backup network.
15. Select <<var_backup_vlan_name>>.

**Figure 199 UCS Manager – Create VLAN Group Backup-Zone**



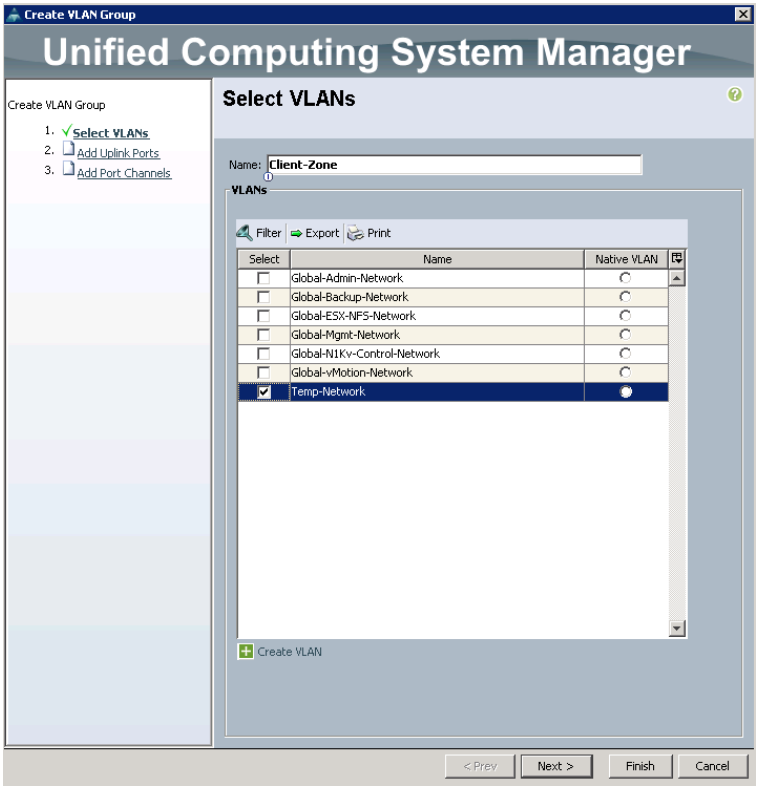

16. Click Next.
17. Click Next on Add Uplink Ports, since we will use Port channel.
18. Choose Port channels Created for Admin Network (vpc-11 and vpc-12) or Backup Network.

Figure 200 UCS Manager – Add Port Channel to a VLAN Group




19. Click Finish.
20. Right-click VLAN Groups.
21. Select Create VLAN Groups.
22. Enter <<var_ucs_client_zone>> as the name of the VLAN Group used for client and application networks.
23. Do not select a VLAN now; the Client/Tenant VLANs are not defined yet.

Figure 201 UCS Manager – Create VLAN Group Client-Zone

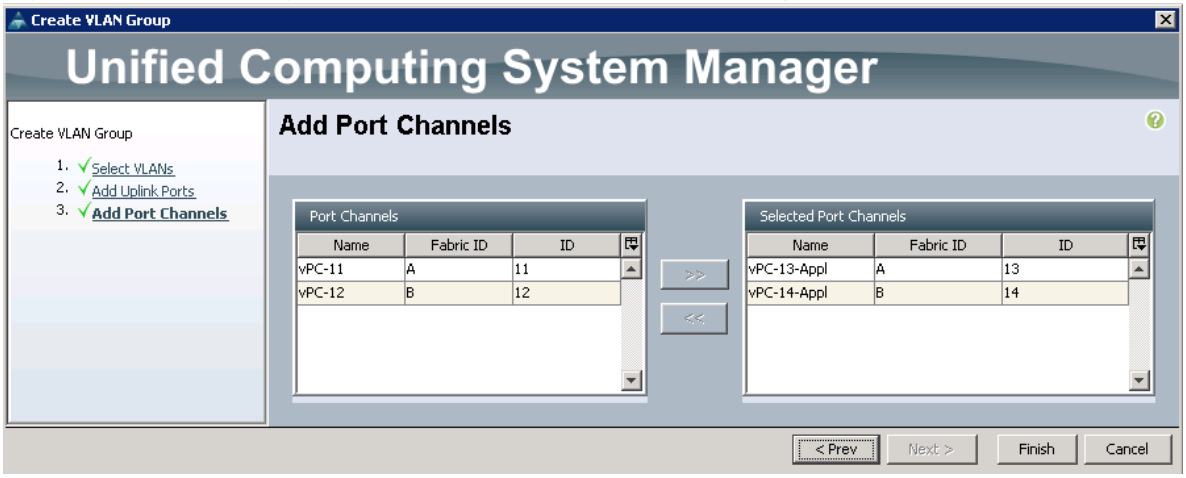



24. Click Next.

25. Click Next on Add Uplink Ports, since we will use Port channel.

26. Choose Port channels Created for Application Network (vpc-13 and vpc-14).

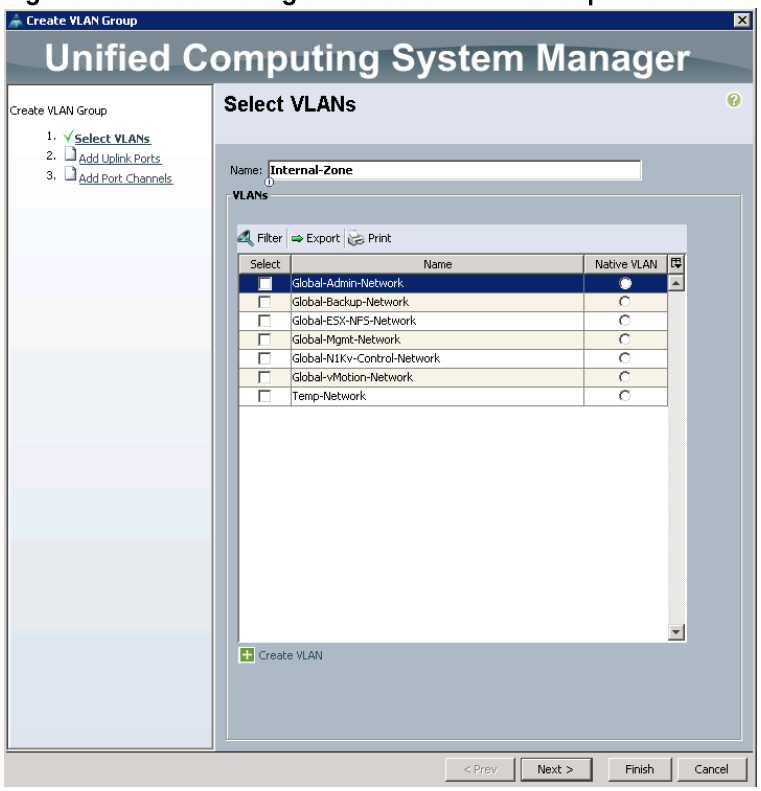
Figure 202 UCS Manager – Add Port Channel to a VLAN Group




27. Click Finish.

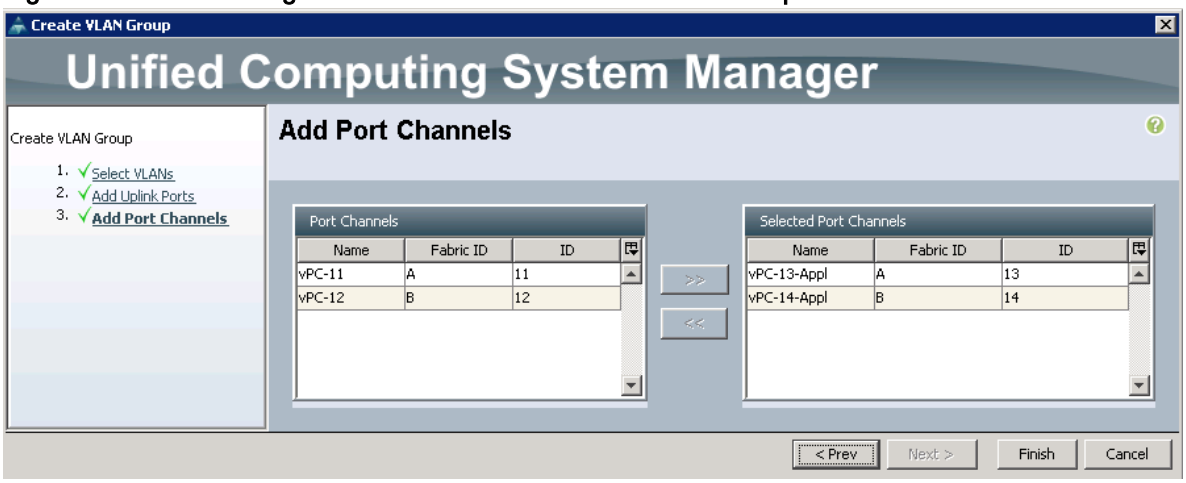
28. Right-click VLAN Groups.
29. Select Create VLAN Groups.
30. Enter <<var_ucs_internal_zone>> as the name of the VLAN Group used for SAP HANA internal networks.
31. Do not select a VLAN now; the Client/Tenant VLANs are not defined yet.

**Figure 203 UCS Manager – Create VLAN Group Internal-Zone**




32. Click Next.
33. Click Next on Add Uplink Ports, since we will use Port channel.
34. Choose Port channels Created for Application Network (vpc-13 and vpc-14).

Figure 204 UCS Manager – Add Port Channel to a VLAN Group




35. Click Finish.

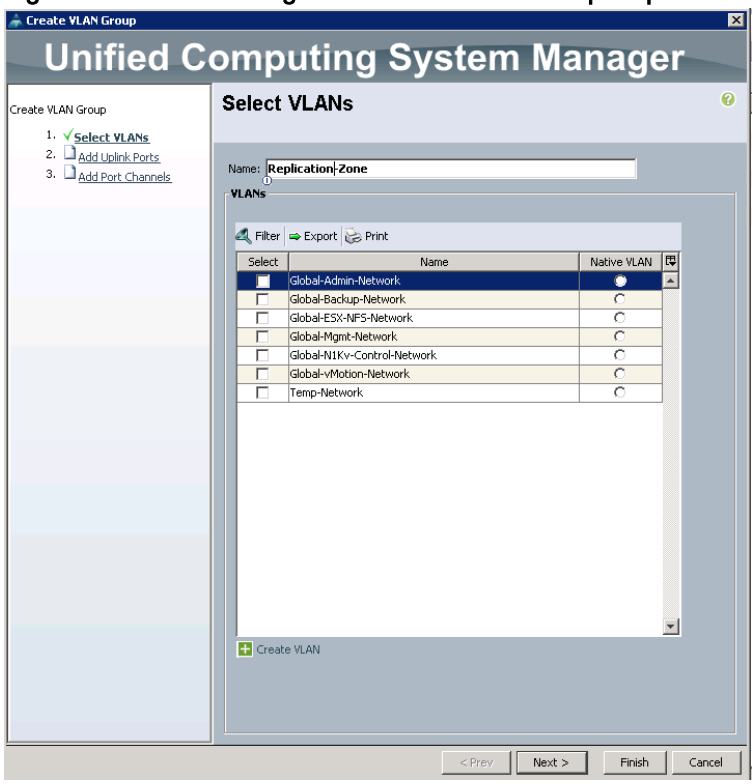
36. Right-click VLAN Groups.

37. Select Create VLAN Groups.

38. Enter <<var_ucs_replication_zone>> as the name of the VLAN Group used for SAP HANA Replication network.

39. Do not select a VLAN now; the Client/Tenant VLANs are not defined yet.

Figure 205 UCS Manager – Create VLAN Group Replication-Zone

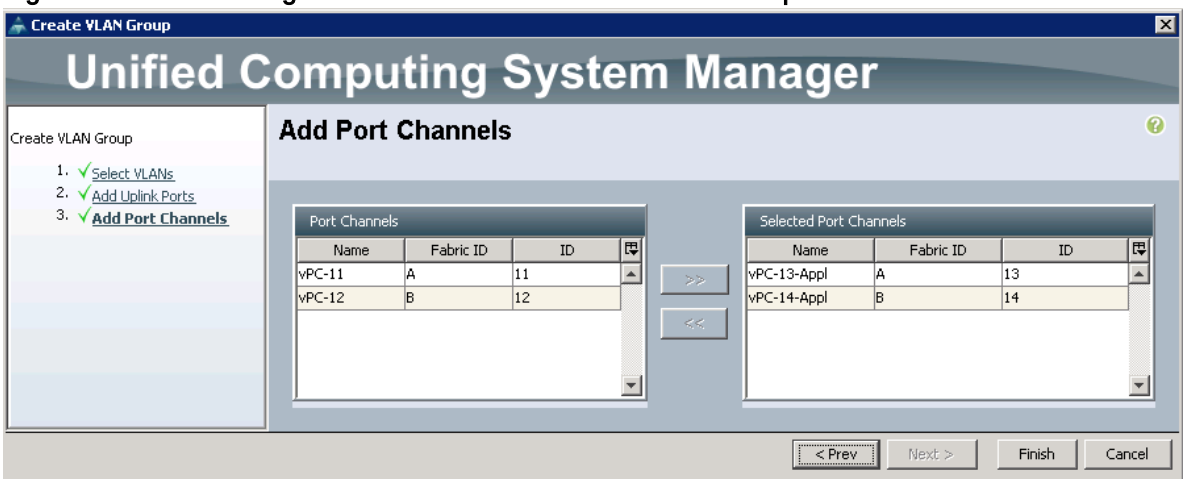



40. Click Next.

41. Click Next on Add Uplink Ports, since we will use Port channel.

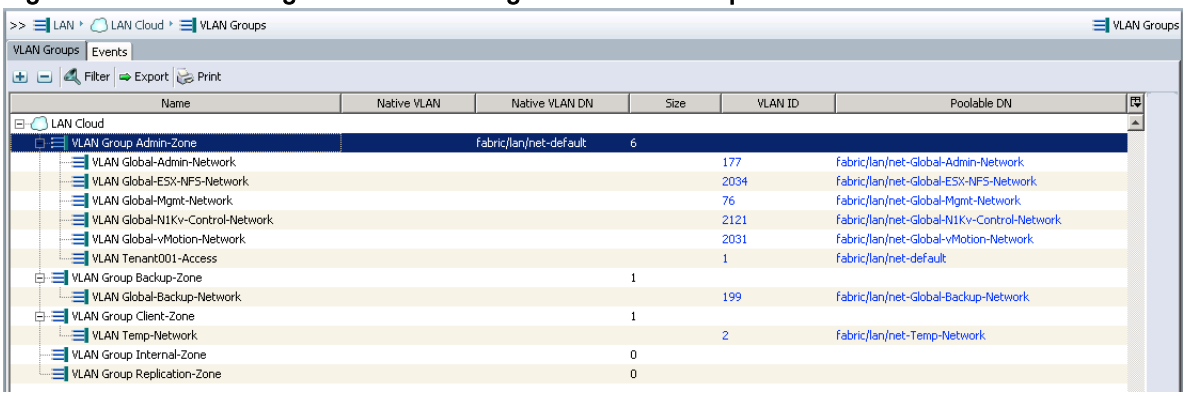
42. Choose Port channels Created for Application Network (vpc-13 and vpc-14).

Figure 206 UCS Manager – Add Port Channel to a VLAN Group




43. Click Finish.

**Figure 207 UCS Manager – List of Configured VLAN Groups**




## Create a vNIC Template

Each VLAN is mapped to a vNIC template to specify the characteristic of a specific network. Parts of the vNIC template configuration are settings like MTU size, failover capabilities and MAC-Address pools.

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps:

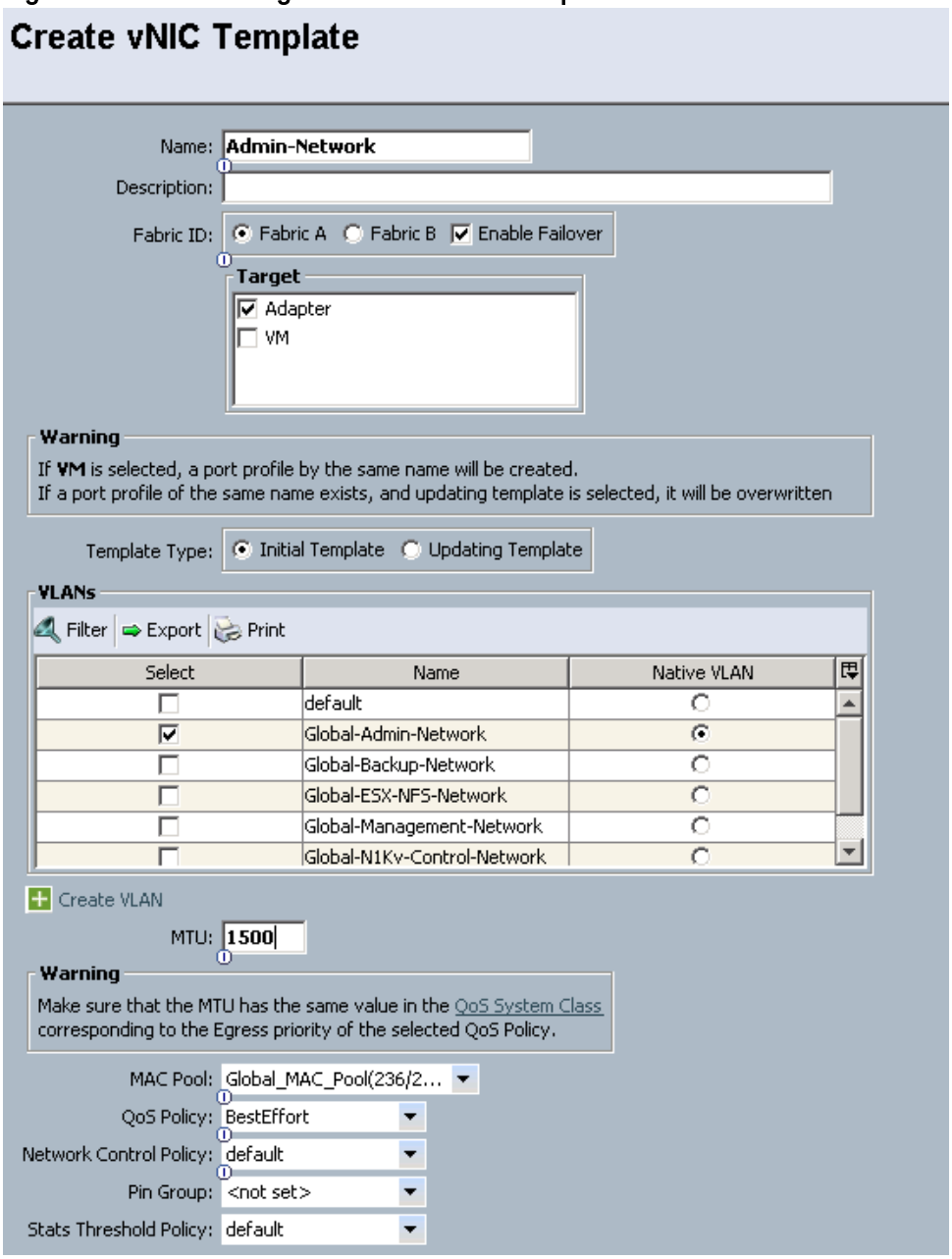


The following vNIC template is used for Admin traffic on Bare Metal servers.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter <<var_ucs_admin_vlan_name>> (or a short version of it) as the vNIC template name.
6. Keep Fabric A selected.
7. Select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANs, select the checkboxes for <<var_ucs_admin_vlan_name>>.
11. Set <<var_ucs_admin_vlan_name>> as the native VLAN.
12. For MTU, enter 1500.
13. In the MAC Pool list, select <<var_global_mac_pool_name>>.

14. In the QoS Policy list, select <<var_ucs_besteffort_policy_name>>

Figure 208 UCS Manager – Create vNIC Template Admin-Network




15. Click OK.

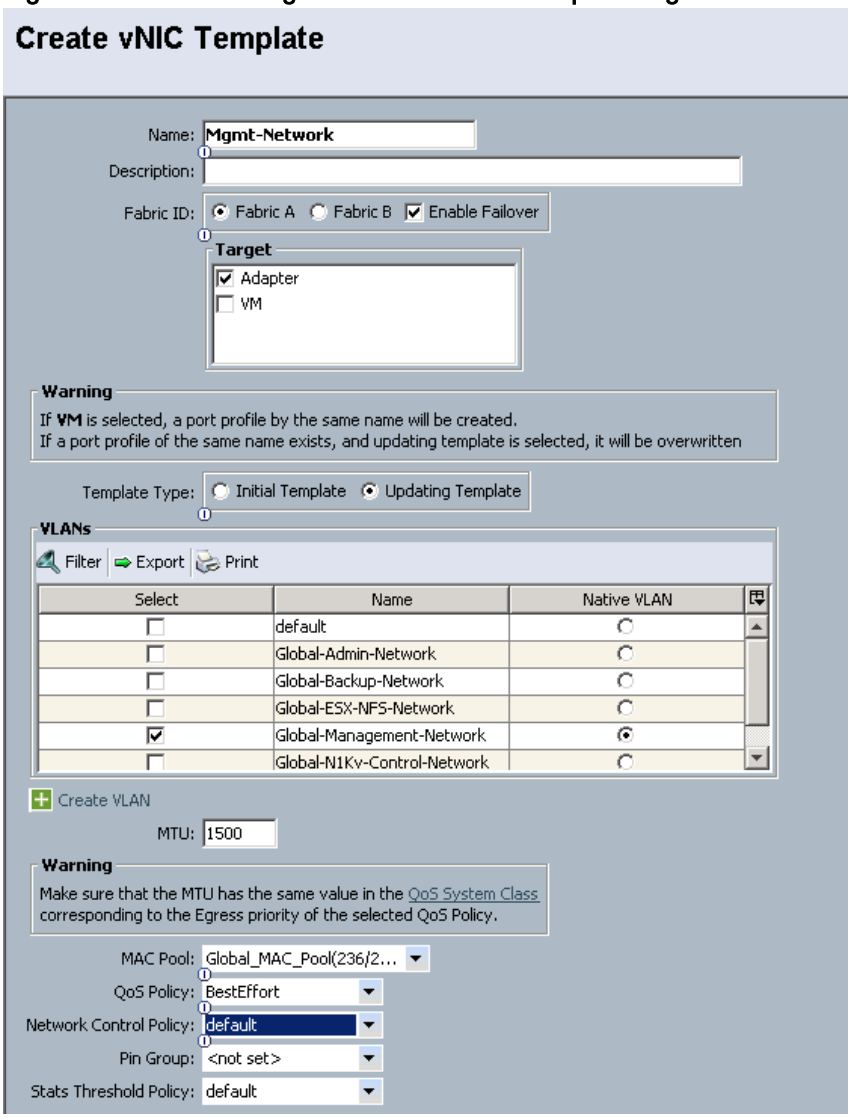
16. Click OK.

The following vNIC template is used for Infrastructure Management traffic on Bare Metal servers.

17. In Cisco UCS Manager, click the LAN tab in the navigation pane.

18. Select Policies > root.
19. Right-click vNIC Templates.
20. Select Create vNIC Template.
21. Enter <<var_ucs_management_vlan_name>> (or a short version of it) as the vNIC template name.
22. Keep Fabric A selected.
23. Select the Enable Failover checkbox.
24. Under Target, make sure that the VM checkbox is not selected.
25. Select Updating Template as the Template Type.
26. Under VLANs, select the checkboxes for <<var_ucs_backup_vlan_name>>.
27. Set <<var_ucs_backup_vlan_name>> as the native VLAN.
28. In the MAC Pool list, select <<var_global_mac_pool_name>>.
29. In the QoS Policy list, select <<var_ucs_besteffort_policy_name>>.

Figure 209 UCS Manager – Create vNIC Template Mgmt-Network

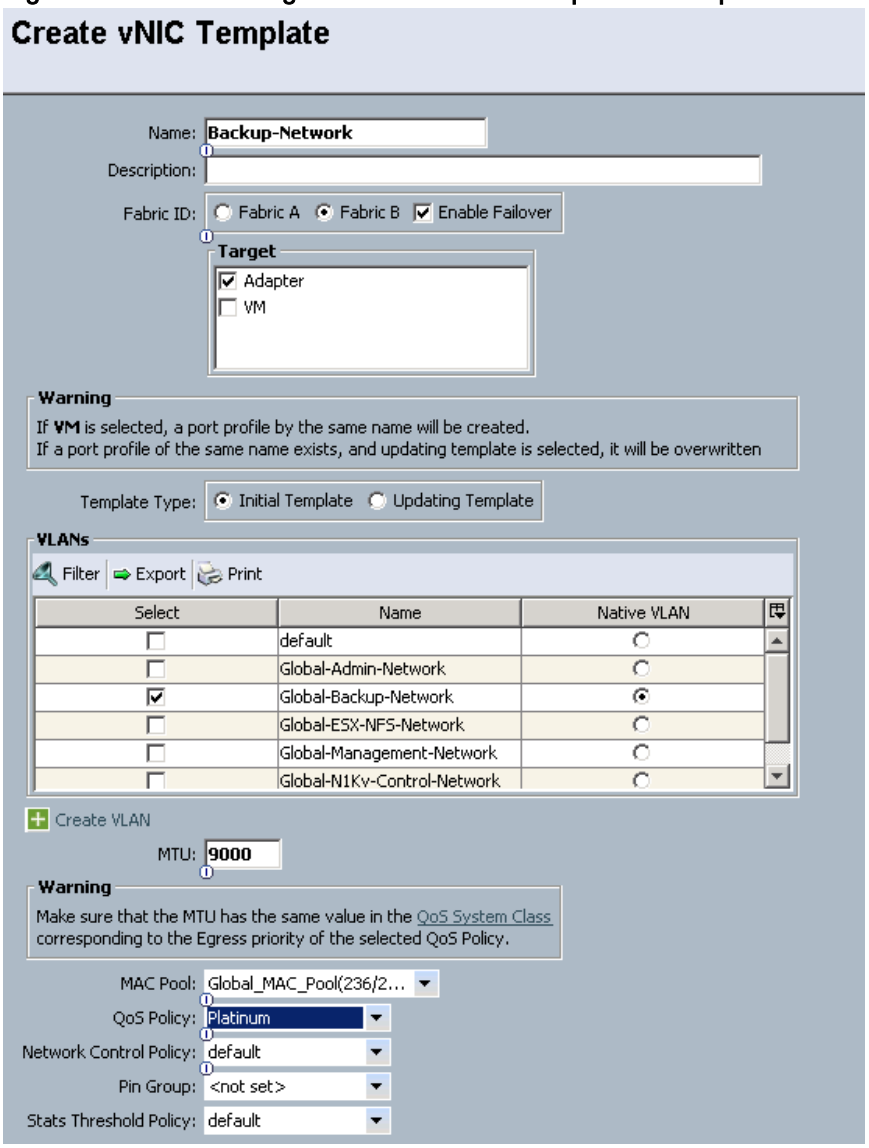



The following vNIC template is used for Backup traffic on Bare Metal servers.

30. In Cisco UCS Manager, click the LAN tab in the navigation pane.
31. Select Policies > root.
32. Right-click vNIC Templates.
33. Select Create vNIC Template.
34. Enter <<var_ucs_backup_vlan_name>> (or a short version of it) as the vNIC template name.
35. Keep Fabric A selected.

36. Select the Enable Failover checkbox.
37. Under Target, make sure that the VM checkbox is not selected.
38. Select Updating Template as the Template Type.
39. Under VLANs, select the checkboxes for <<var_ucs_backup_vlan_name>>.
40. Set <<var_ucs_backup_vlan_name>> as the native VLAN.
41. For MTU, enter 9000. (Please double check with your Backup Admin if the Backup Destination is configured with MTU 9000 as well.
42. In the MAC Pool list, select <<var_global_mac_pool_name>>.
43. In the QoS Policy list, select <<var_ucs_platinum_policy_name>> (This enables MTU 9000).

Figure 210 UCS Manager – Create vNIC Template Backup-Network



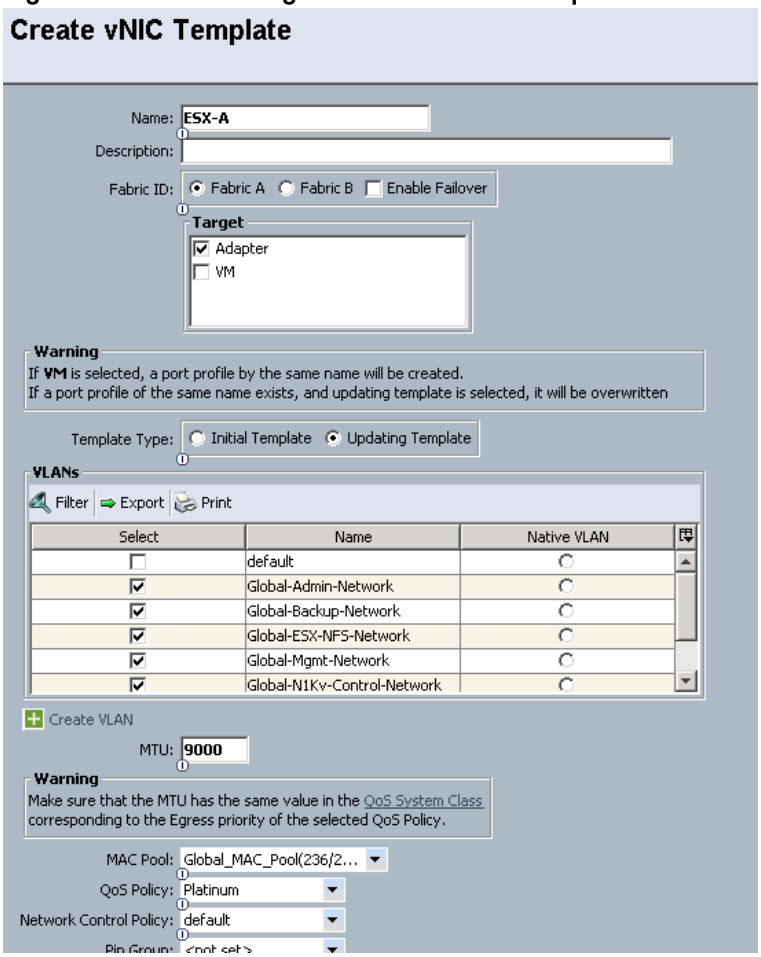

The following vNIC template is used for all traffic on VMware ESX servers.

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.

5. Enter <<var_ucs_esx_a_vnic_name>> as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANs, select the checkboxes for <<var_ucs_admin_vlan_name>>,<<var_ucs_esx_nfs_vlan_name>>,<<var_ucs_vmotion_vlan_name>>,<<var_ucs_backup_vlan_name>>,<<var_ucs_n1k_control_vlan_name>>
11. Set no native VLAN.
12. For MTU, enter 9000.
13. In the MAC Pool list, select <<var_global_mac_pool_name>>.
14. In the QoS Policy list, select <<var_ucs_platinum_policy_name>>.
15. Click OK to create the vNIC template.
16. Click OK.

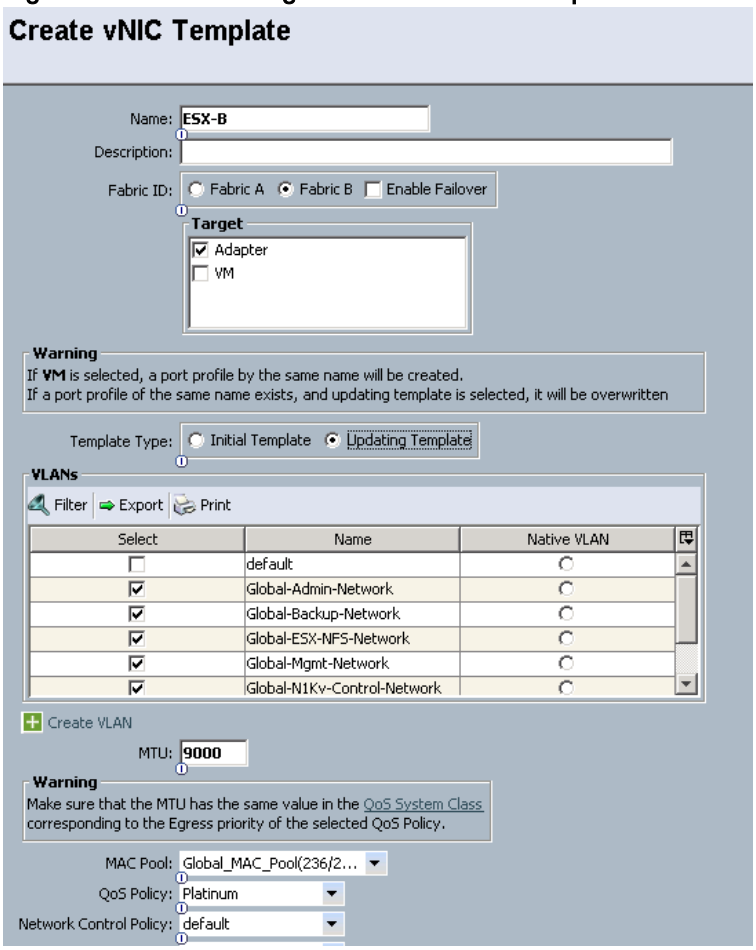
Figure 211 UCS Manager – Create vNIC Template ESX-A




17. Right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter <<var_ucs_esx_b_vnic_name>> as the vNIC template name.
20. Keep Fabric B selected.
21. Do not select the Enable Failover checkbox.
22. Under Target, make sure that the VM checkbox is not selected.
23. Select Updating Template as the Template Type.
24. Under VLANs, select the checkboxes for <<var_ucs_admin_vlan_name>>,<<var_ucs_esx_nfs_vlan_name>>,<<var_ucs_vmotion_vlan_name>>,<<var_ucs_backup_vlan_name>>,<<var_ucs_n1k_control_vlan_name>>.
25. Set no native VLAN.

26. For MTU, enter 9000.
27. In the MAC Pool list, select <<var_global_mac_pool_name>>.
28. In the QoS Policy list, select <<var_ucs_platinum_policy_name>>.
29. Click OK to create the vNIC template.
30. Click OK.

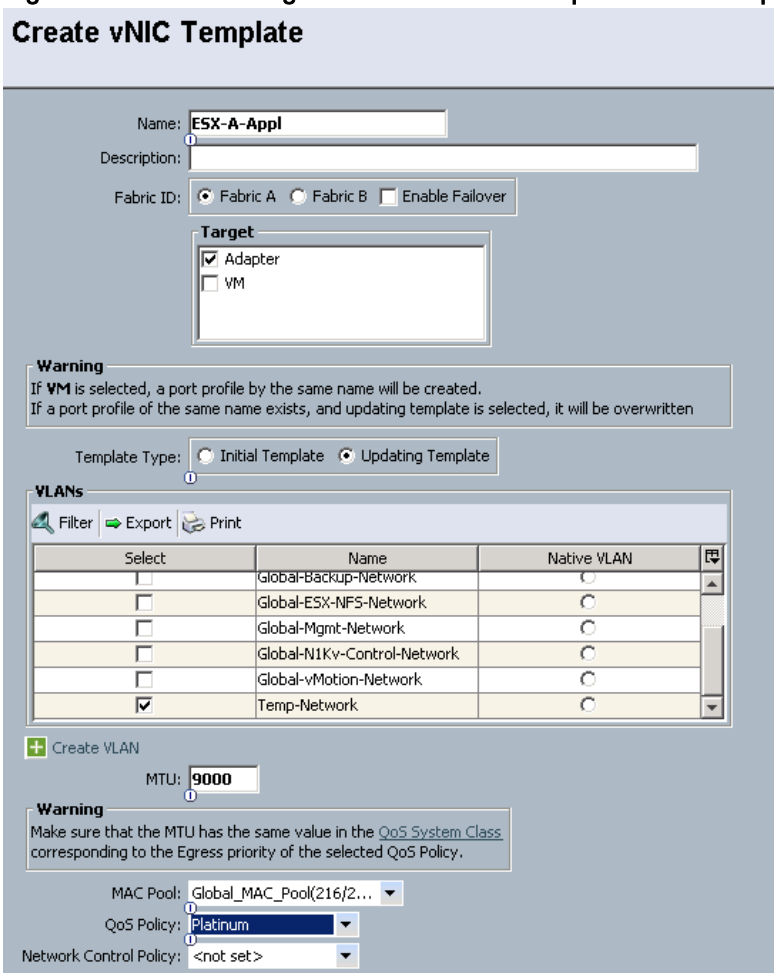
Figure 212 UCS Manager – Create vNIC Template ESX-B




31. Right-click vNIC Templates.
32. Select Create vNIC Template.
33. Enter <<var_ucs_esx_a_appl_vnic_name>> as the vNIC template name.
34. Keep Fabric A selected.
35. Do not select the Enable Failover checkbox.

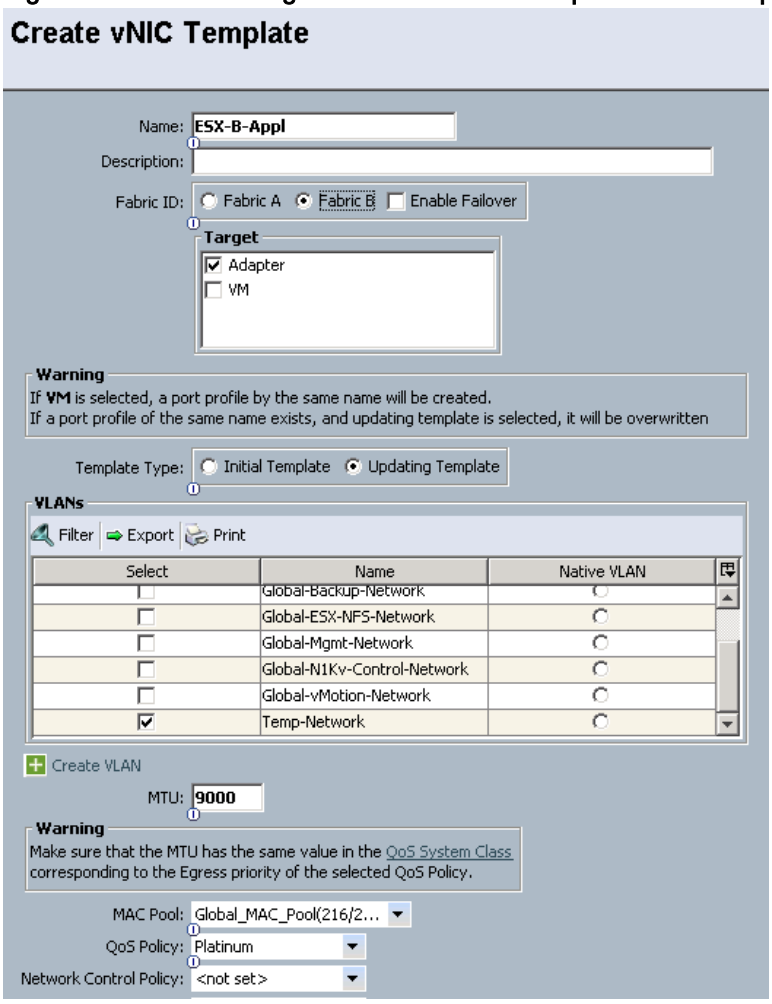
36. Under Target, make sure that the VM checkbox is not selected.
37. Select Updating Template as the Template Type.
38. Under VLANs, select the checkboxes for <<var_ucs_temp_vlan_name>>
39. Set no native VLAN.
40. For MTU, enter 9000.
41. In the MAC Pool list, select <<var_global_mac_pool_name>>.
42. In the QoS Policy list, select <<var_ucs_platinum_policy_name>>.
43. Click OK to create the vNIC template.
44. Click OK.

**Figure 213 UCS Manager – Create vNIC Template ESX-A-Appl**



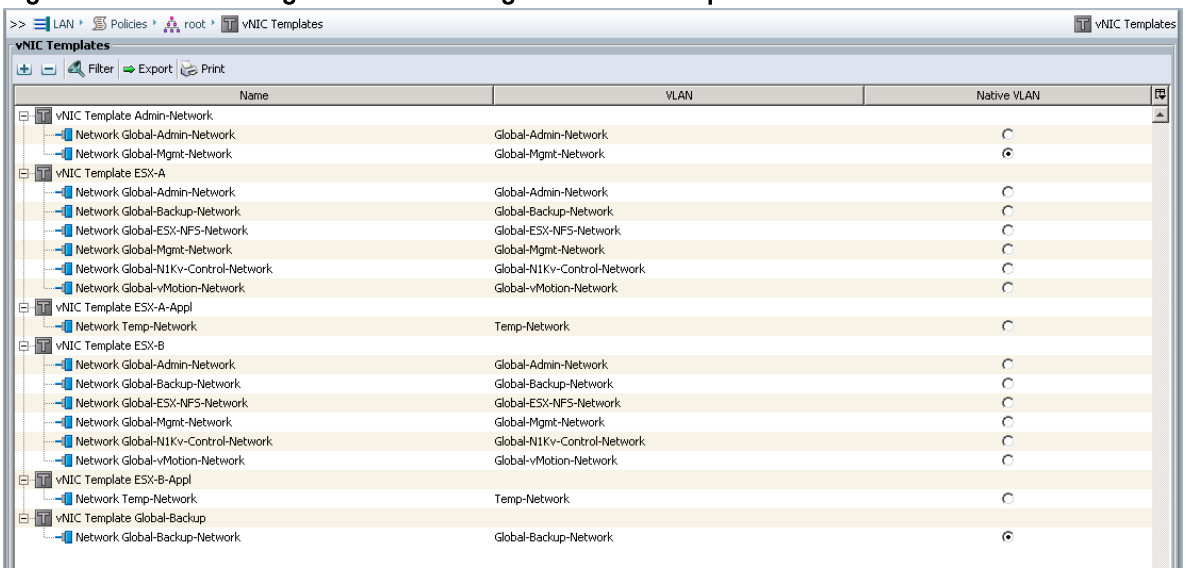
45. Right-click vNIC Templates.
46. Select Create vNIC Template.
47. Enter <<var_ucs_esx_b_appl_vnic_name>> as the vNIC template name.
48. Keep Fabric B selected.
49. Do not select the Enable Failover checkbox.
50. Under Target, make sure that the VM checkbox is not selected.
51. Select Updating Template as the Template Type.
52. Under VLANs, select the checkboxes for <<var_ucs_temp_vlan_name>>.
53. Set no native VLAN.
54. For MTU, enter 9000.
55. In the MAC Pool list, select <<var_global_mac_pool_name>>.
56. In the QoS Policy list, select <<var_ucs_platinum_policy_name>>.
57. Click OK to create the vNIC template.
58. Click OK.

Figure 214 UCS Manager – Create vNIC Template ESX-B-Appl




The list of configured vNIC Templates is shown below:

**Figure 215 UCS Manager – List of configured vNIC Templates**




## Create LAN Connectivity Policy

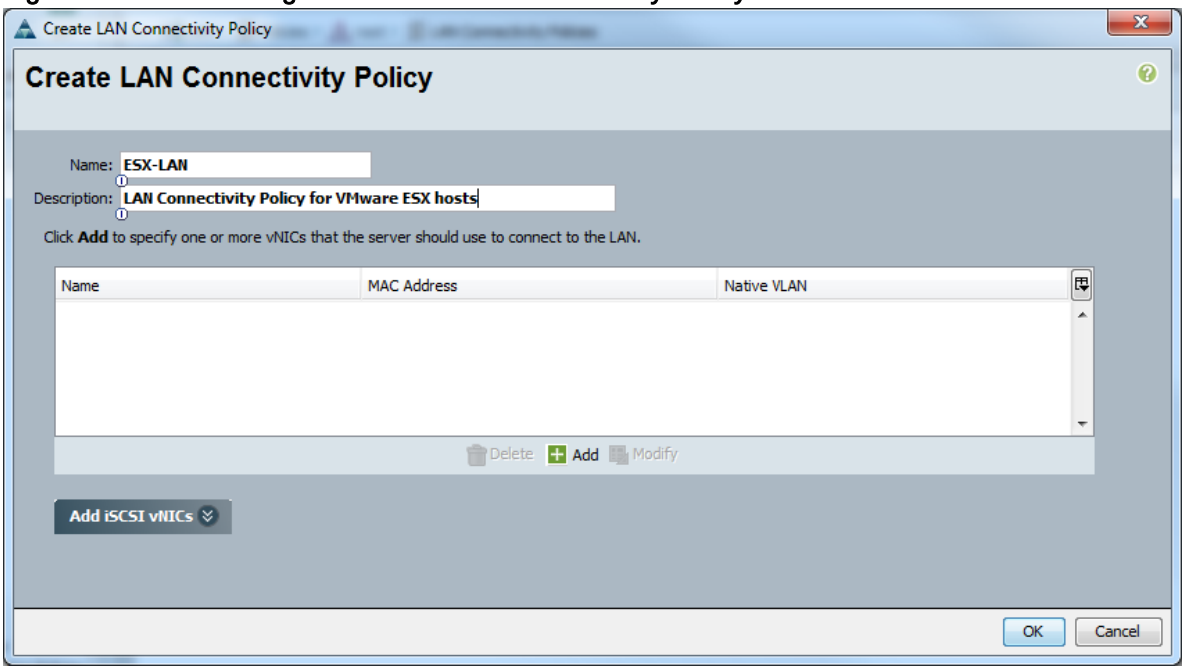
For VMware ESX together with Cisco Nexus1000V only one LAN Connectivity Policy is required.

LAN Connectivity Policy for VMware ESX

To create the LAN Connectivity Policy for the VMware ESX hosts complete the following steps:

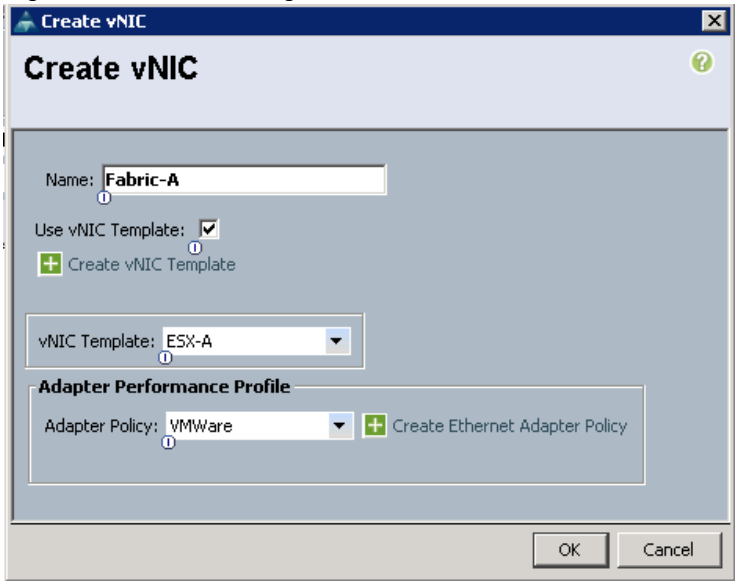
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter <<var_ucs_esx_lan_connect_policy_name>> as the name.
6. Enter an optional description.
7. Click Add.

Figure 216 UCS Manager – Create LAN Connectivity Policy ESX-LAN



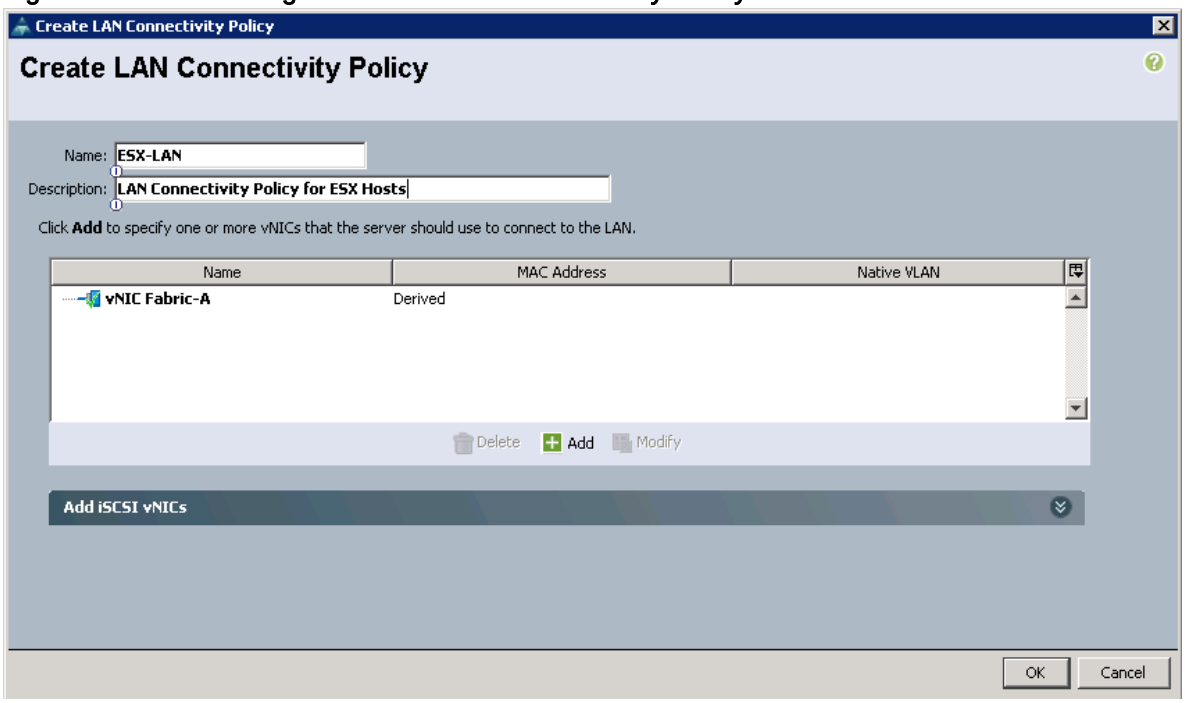

8. Enter Fabric-A in the name field.
9. Select the checkbox to Use vNIC Template.
10. In the vNIC Template list, select <<var_ucs_esx_a_vnic_name>>.
11. In the Adapter Policy list, select VMWare.
12. Click OK.

Figure 217 UCS Manager – Create vNIC Fabric-A



13. Click Add.

Figure 218 UCS Manager – Create LAN Connectivity Policy




14. Enter Fabric-B in the name field.

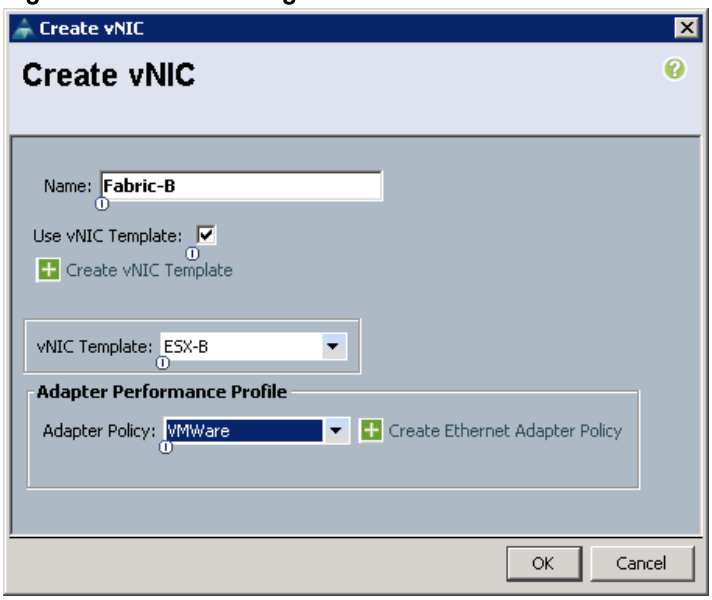
15. Select the checkbox to Use vNIC Template.

16. In the vNIC Template list, select <<var_ucs_esx_b_vnic_name>>.

17. In the Adapter Policy list, select VMWare.

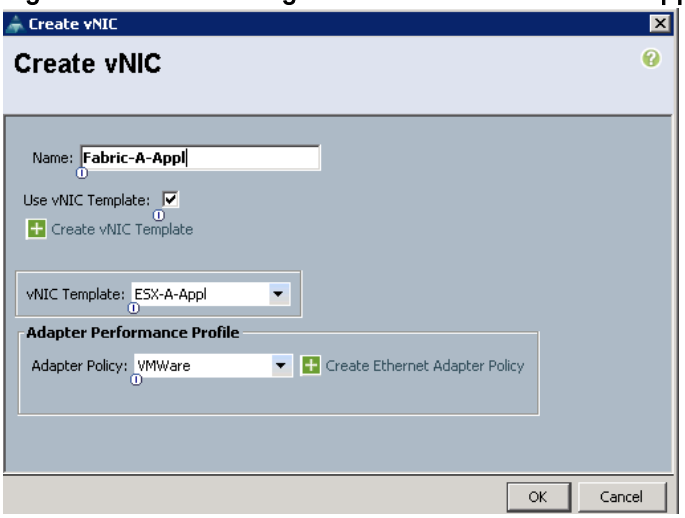
18. Click OK.

Figure 219 UCS Manager – Create vNIC Fabric-B



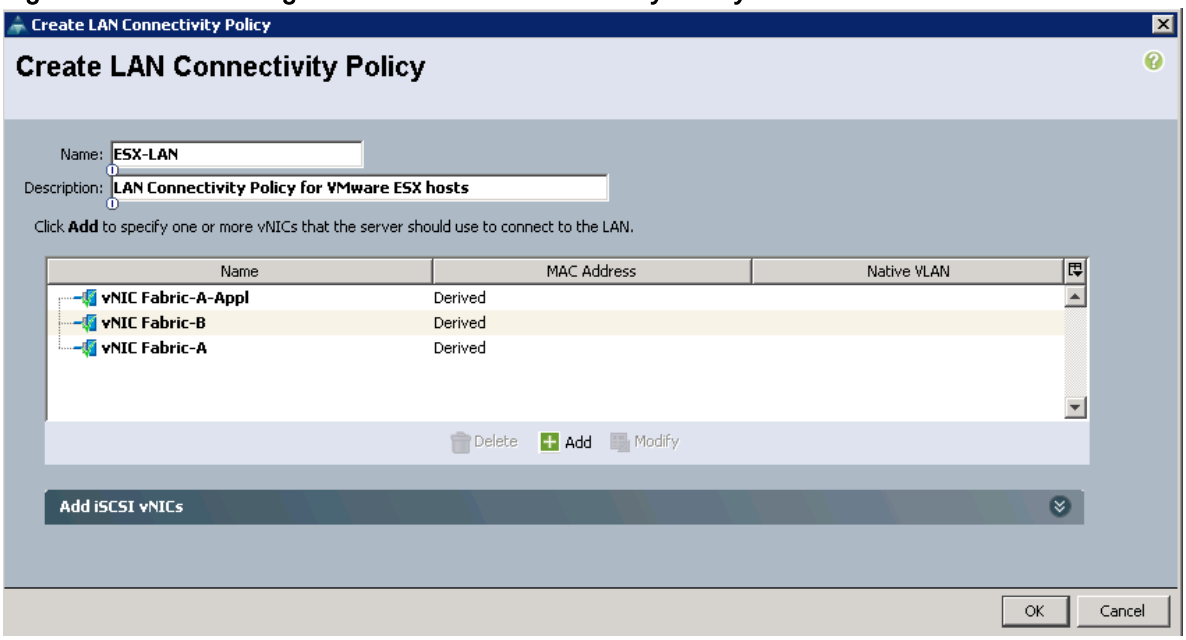

19. Click Add.
20. Enter Fabric-A-Appl in the name field.
21. Select the checkbox to Use vNIC Template .
22. In the vNIC Template list, select <<var_ucs_esx_a_appl_vnic_name>>.
23. In the Adapter Policy list, select VMWare.
24. Click OK.

Figure 220 UCS Manager – Create vNIC Fabric-A-Appl



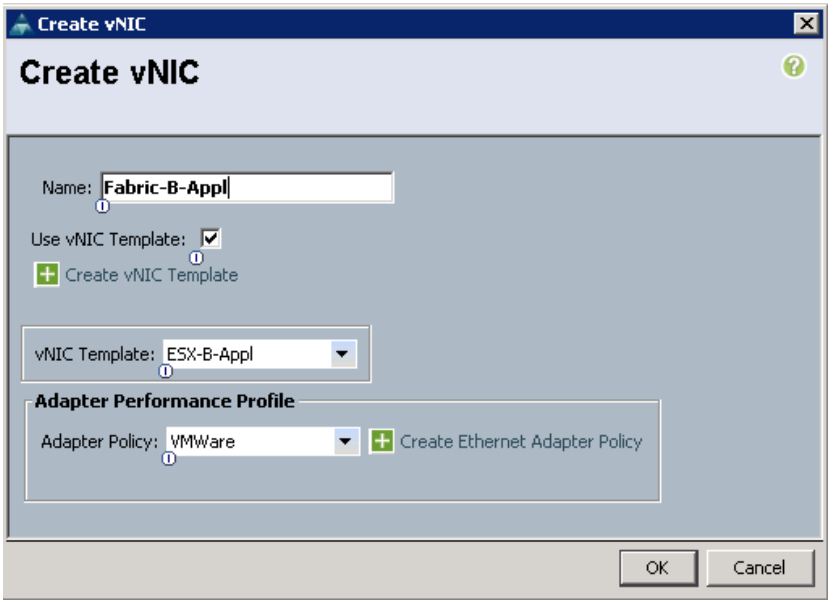

25. Click Add.

Figure 221 UCS Manager – Create LAN Connectivity Policy




26. Enter Fabric-B in the name field.
27. Select the checkbox to Use vNIC Template.
28. In the vNIC Template list, select <<var_ucs_esx_b_appl_vnic_name>>.
29. In the Adapter Policy list, select VMWare.
30. Click OK.

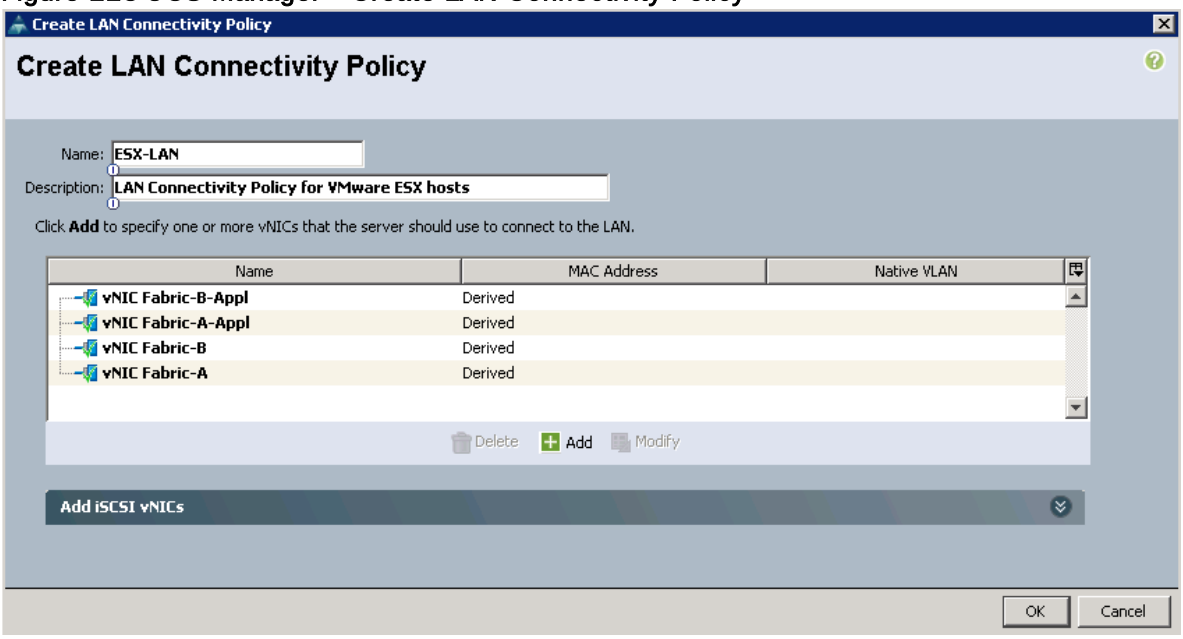
Figure 222 UCS Manager – Create vNIC Fabric-B-Appl



31. Click OK.

32. Click OK.

Figure 223 UCS Manager – Create LAN Connectivity Policy




Section “Tenant/SAP System Configuration” details how to create the LAN Connectivity Policies for Bare Metal SAP HANA nodes.

## Configure SAN Settings

This section details how to configure SAN for Cisco UCS.

Table 30 SAN for the Cisco UCS in this Cisco UCS Integrated Infrastructure.

Table 30 Information to Setup Cisco UCS in the Reference Architecture

| Name | Variable |
|---|---|
| Fibre Channel Port Channel ID on Fabric A | <<var_ucs_fcpc_a_id>> |
| Fibre Channel Port Channel Name on Fabric A | <<var_ucs_fcpc_a_name>> |
| Fibre Channel Port Channel ID on Fabric B | <<var_ucs_fcpc_b_id>> |
| Fibre Channel Port Channel Name on Fabric B | <<var_ucs_fcpc_b_name>> |
| Name of the Global World Wide Node Name Pool | <<var_ucs_global_wwnn_pool_name>> |
| Name of the Global World Wide Port Name Pool on Fabric A | <<var_ucs_global_wwpn_a_pool_name>> |

| Name | Variable |
|---|---|
| Name of the Global World Wide Port Name Pool on Fabric B | <<var_ucs_global_wwpn_b_pool_name>> |
| Name of the VSAN on Fabric A | <<var_ucs_vsan_a_name>> |
| ID of the VSAN on Fabric A | <<var_vsan_a_id>> |
| VLAN ID for FCoE traffic of the VSAN on Fabric A | <<var_vsan_a_fcoe_id>> |
| Name of the VSAN on Fabric B | <<var_ucs_vsan_b_name>> |
| ID of the VSAN on Fabric B | <<var_vsan_b_id>> |
| VLAN ID for FCoE traffic of the VSAN on Fabric B | <<var_vsan_b_fcoe_id>> |
| Name of the SAN Connection Policy for ESX | <<var_ucs_esx_san_connect_policy_name>> |
| Name of the vHBA Template on Fabric A | <<var_ucs_vhba_a_templ_name>> |
| Name of the vHBA Template on Fabric B | <<var_ucs_vhba_b_templ_name>> |
| Name of the first vHBA in a Service Profile | <<var_ucs_vhba_1_name>> |
| Name of the second vHBA in a Service Profile | <<var_ucs_vhba_2_name>> |
| SAN Connection Policy for SAP HANA Scale-Up | <<var_ucs_hana_su_connect_policy_name>> |
| Name of the third vHBA in a Service Profile | <<var_ucs_vhba_3_name>> |
| Name of the forth vHBA in a Service Profile | <<var_ucs_vhba_4_name>> |
| SAN Connection Policy for SAP HANA Scale-Out | <<var_ucs_hana_so_connect_policy_name>> |
| | |

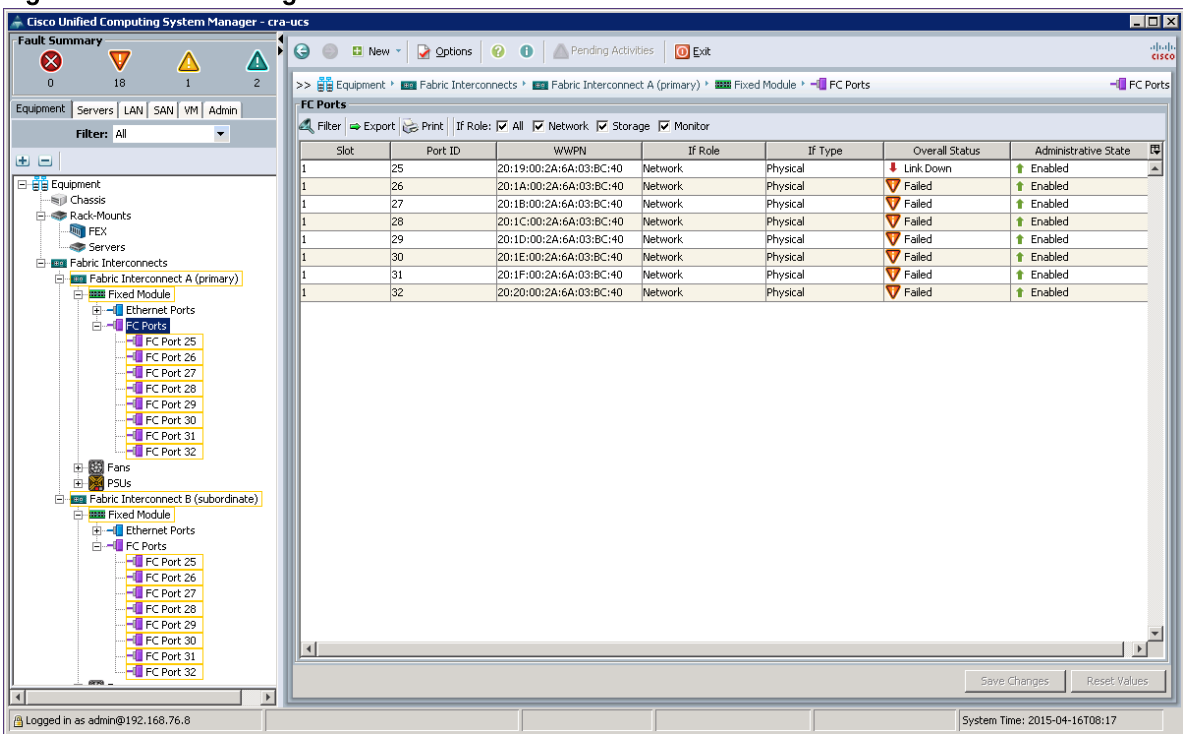
### Configure SAN Uplink Ports

To enable uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand FC Ports.
4. In case the IF role is already Network you can skip this and proceed with the creation of the FC Port Channels

5. Select ports that are connected to the Cisco MDS switches, right-click them, and select Configure as Uplink Port.
6. Click Yes to confirm uplink ports and click OK.
7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
8. Expand FC Ports.
9. Select ports that are connected to the Cisco MDS switches, right-click them, and select Configure as Uplink Port.
10. Click Yes to confirm the uplink ports and click OK.

**Figure 224 UCS Manager – List of Fibre Channel Ports on Fabric Interconnect A**




## Configure FC Uplink Port Channels to Cisco MDS Switches

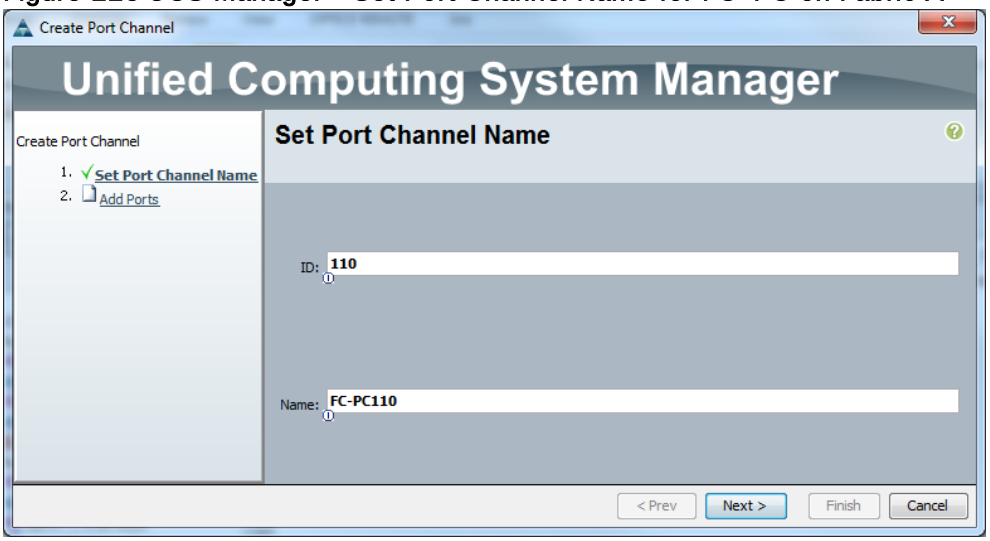
A Uplink Port Channel is created for storage traffic. For example, create a FC Port channel 110 on Fabric Interconnect A and Port channel 120 on Fabric Interconnect B for storage traffic to the Cisco MDS switches.

To configure a FC Uplink Port Channel, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > SAN Cloud.
3. Expand Fabric A.

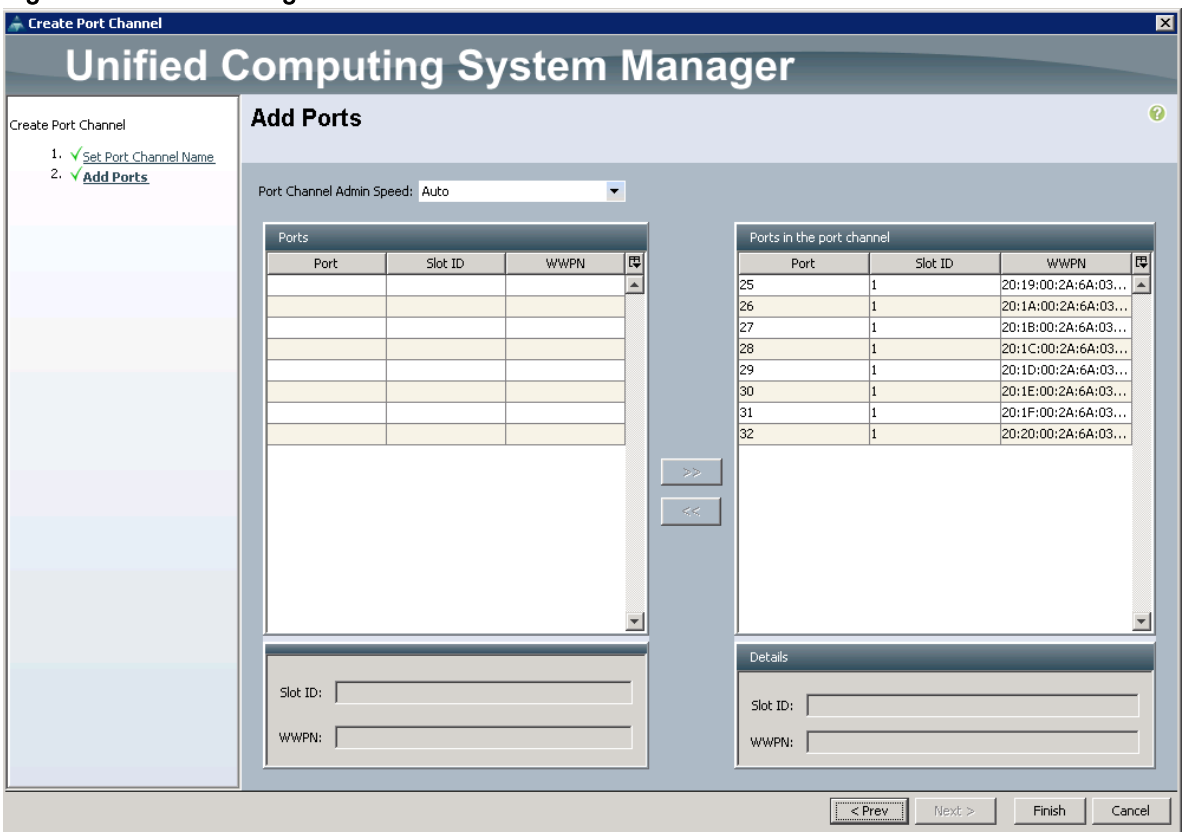
4. Right-click FC Port Channels.
5. Select Create Port Channel.
6. Enter <<var_ucs_fcpc_a_id>> as the ID of the Port Channel.
7. Enter <<var_ucs_fcpc_a_name>> as the name of the Port Channel.
8. Click Next.

Figure 225 UCS Manager – Set Port Channel Name for FC-PC on Fabric A



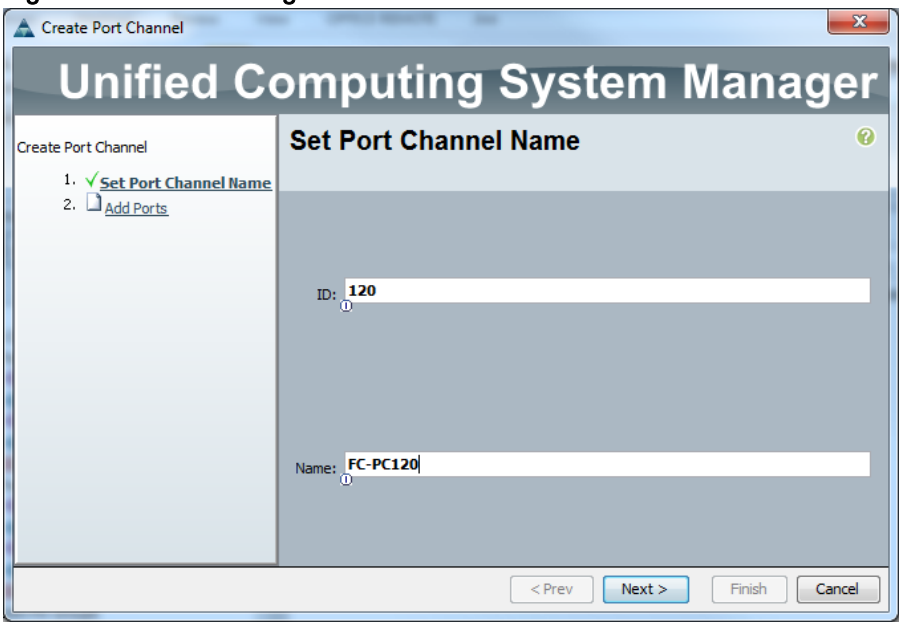

9. Select all FC ports connected to the Cisco MDS 9148-A switch.
10. Click >> to add them into the Port Channel.
11. Click Finish.
12. Click OK.

Figure 226 UCS Manager – Add Ports to a FC Port Channel



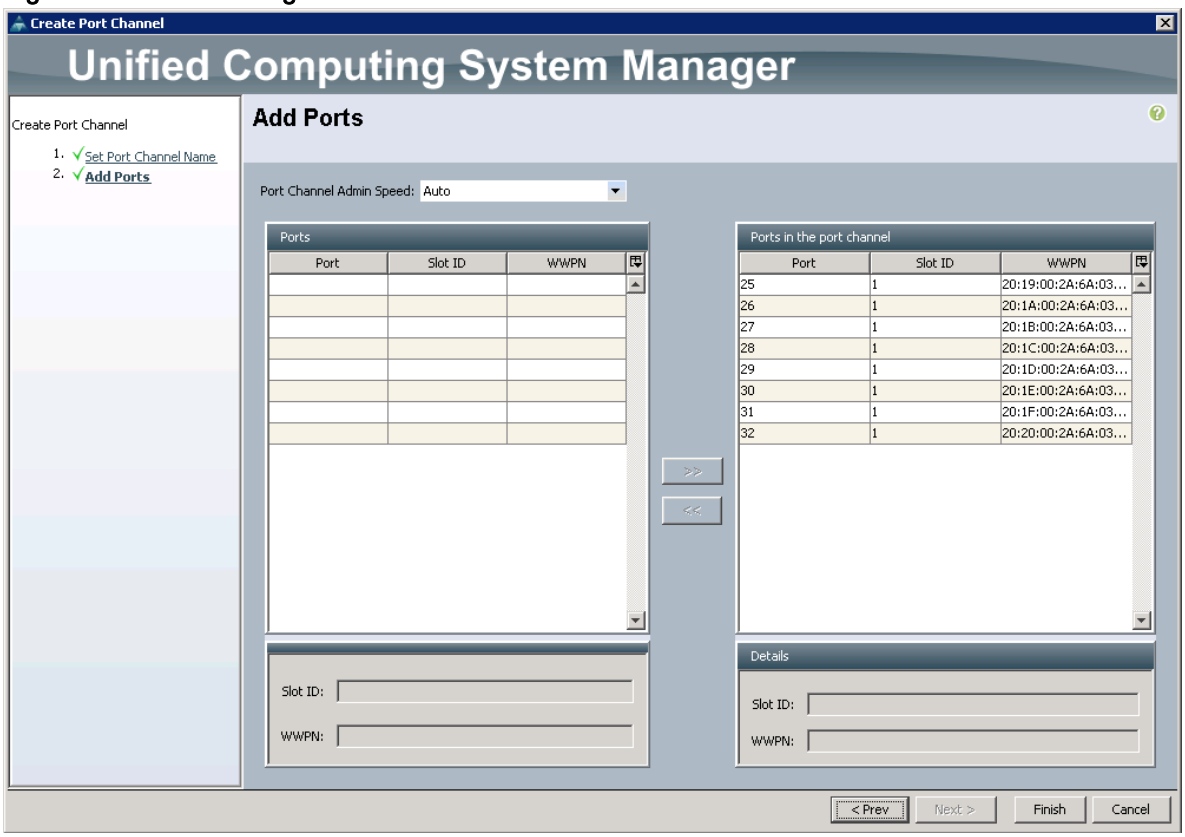

13. Expand Fabric B.
14. Right-click FC Port Channels.
15. Select Create Port Channel.
16. Enter <<var_ucs_fcpc_b_id>> as the ID of the Port Channel.
17. Enter <<var_ucs_fcpc_b_name>> as the name of the Port Channel.
18. Click Next.

Figure 227 UCS Manager – Set Port Channel Name for FC-PC on Fabric B



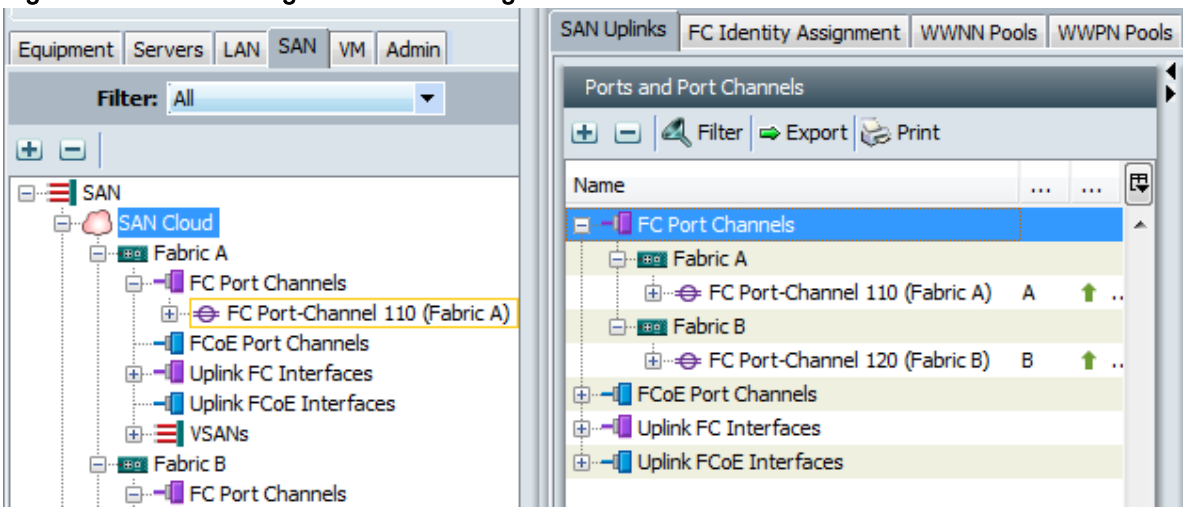

19. Select all FC ports connected to the Cisco MDS 9148-B switch.
20. Click >> to add them into the Port Channel.
21. Click Finish.
22. Click OK.

Figure 228 UCS Manager – Add Ports to a FC Port Channel




23. To see the list of defined FC Port Channels Select SAN > SAN Cloud and expand on the right pane the FC Port Channels Section.

Figure 229 UCS Manager – List of configured FC Port Channel

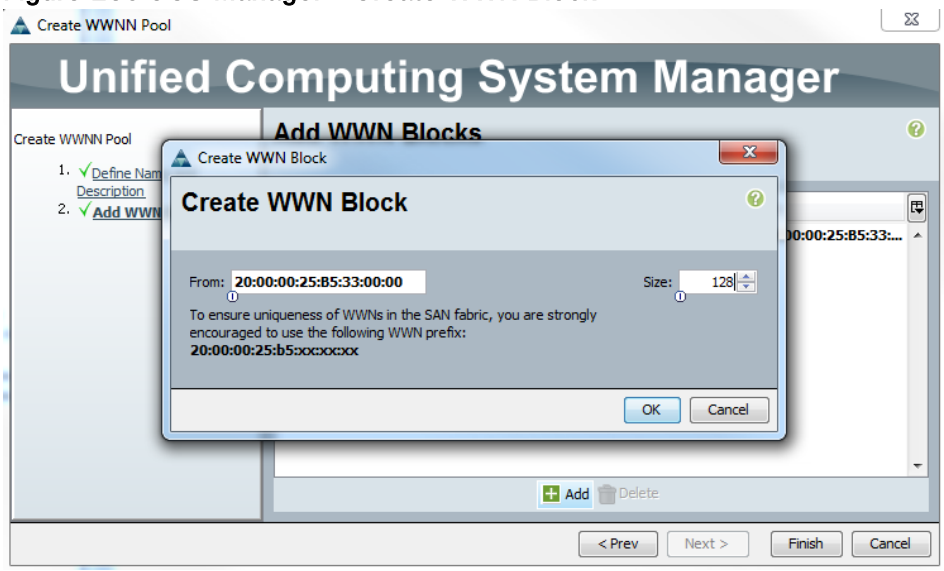


## Create WWNN and WWPN Address Pool(s)

To configure a necessary WWNN (World Wide Node Name) and WWPN (World Wide Port Name) address pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN address pool.
5. Enter <<var_ucs_global_wwnn_pool_name>> as the name of the WWNN pool.
6. Optional: Enter a description for this pool.
7. Choose Assignment Order Sequential.
8. Click Next.
9. Click Add.
10. Specify a starting WWNN address.
11. Specify a size for the WWNN address pool that is sufficient to support the available blade or server resources. Only one WWNN is required per server.
12. Click Finish.

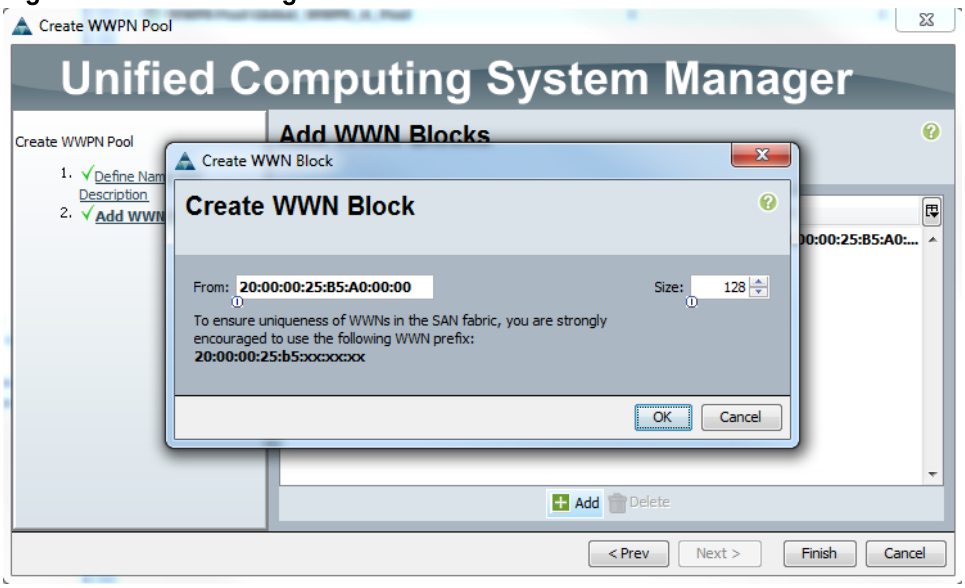
**Figure 230 UCS Manager – Create WWN Block**




13. Right-click WWPN Pools under the root organization.

14. Select Create WWPN Pool to create the WWPN address poolError! Reference source not found..
15. Enter <<var_ucs_global_wwpn_a_pool_name>> as the name of the WWPN pool.
16. Optional: Enter a description for this pool.
17. Choose Assignment Order Sequential.
18. Click Next.
19. Click Add.
20. Specify a starting WWPN address.
21. Specify a size for the WWPN address pool that is sufficient to support the available blade or server resources. One WWPN is required per HBA and it is possible to have multiple HBAs configured per server.
22. Click Finish.

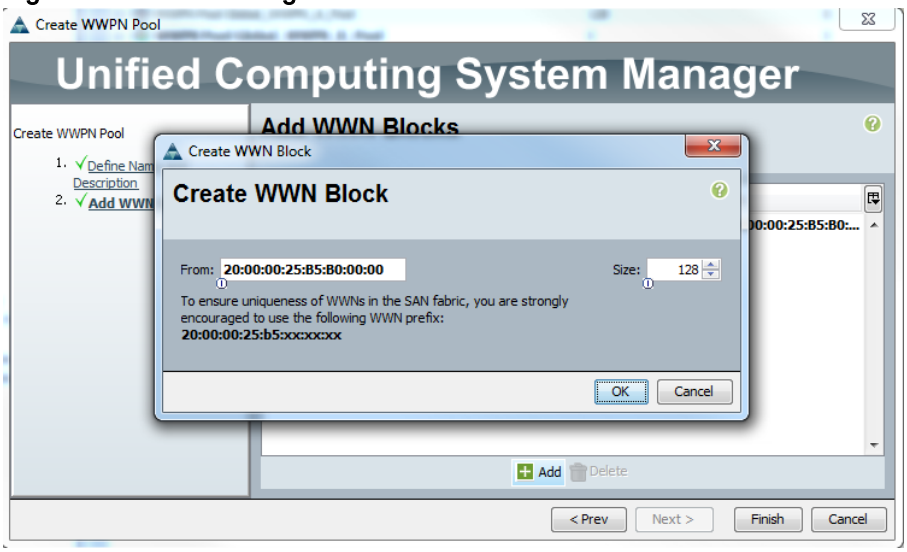
**Figure 231 UCS Manager – Create WWN Block**




23. Right-click WWPN Pools under the root organization.
24. Select Create WWPN Pool to create the WWPN address poolError! Reference source not found..
25. Enter <<var_ucs_global_wwpn_b_pool_name>> as the name of the WWPN pool.
26. Optional: Enter a description for this pool.
27. Choose Assignment Order Sequential.

28. Click Next.
29. Click Add.
30. Specify a starting WWPN address.
31. Specify a size for the WWPN address pool that is sufficient to support the available blade or server resources. One WWPN is required per HBA and it is possible to have multiple HBAs configured per server.
32. Click Finish.

Figure 232 UCS Manager – Create WWN Block




## Configure VSANs and vHBA Templates

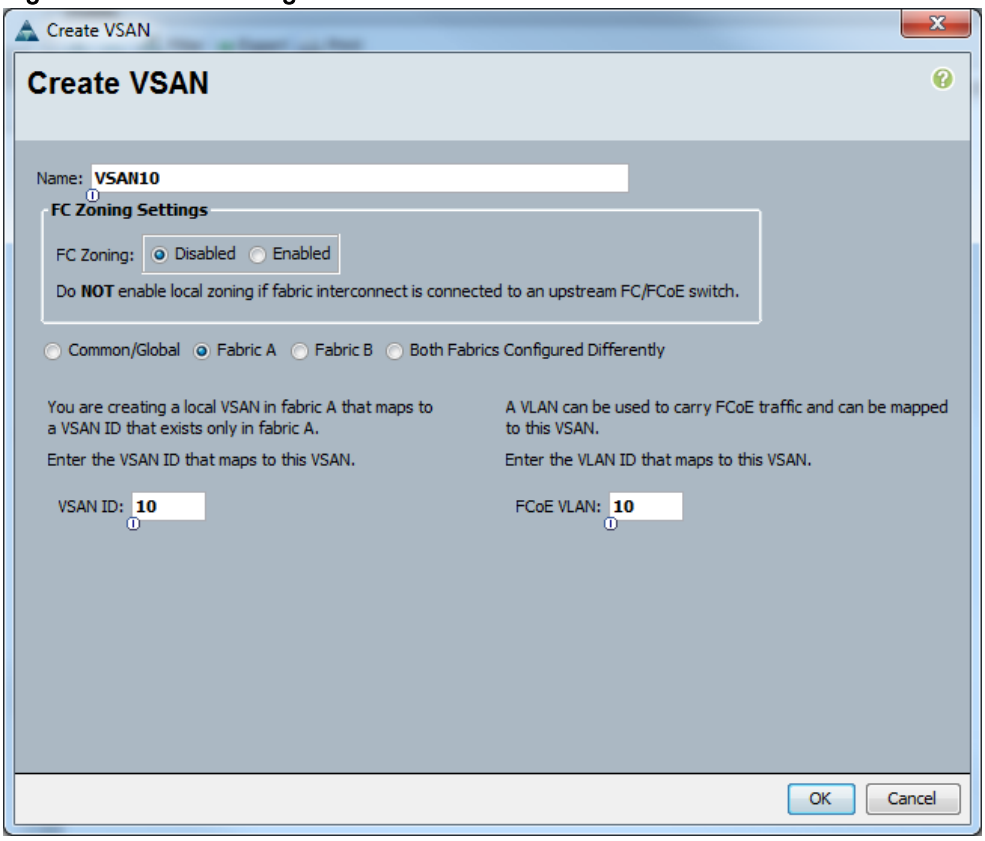
The main storage access in this architecture uses Fibre Channel SAN.

To configure the necessary virtual storage area networks (VSANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > SAN Cloud.
3. Expand Fabric A.
4. Right-click VSANs.
5. Select Create VSANs.
6. Enter <<var_ucs_vsan_a_name>> as the name of the VSAN.

7. Enter <<var_vsan_a_id>> as the VSAN ID and <<var_vsan_a_fcoe_id>> as the FCoE VLAN ID. FCoE VLAN ID should not have conflict with any of the VLANs configured before.
8. Select Fabric A.
9. Leave the FC zoning disabled (default).
10. Click OK.
11. Click OK.

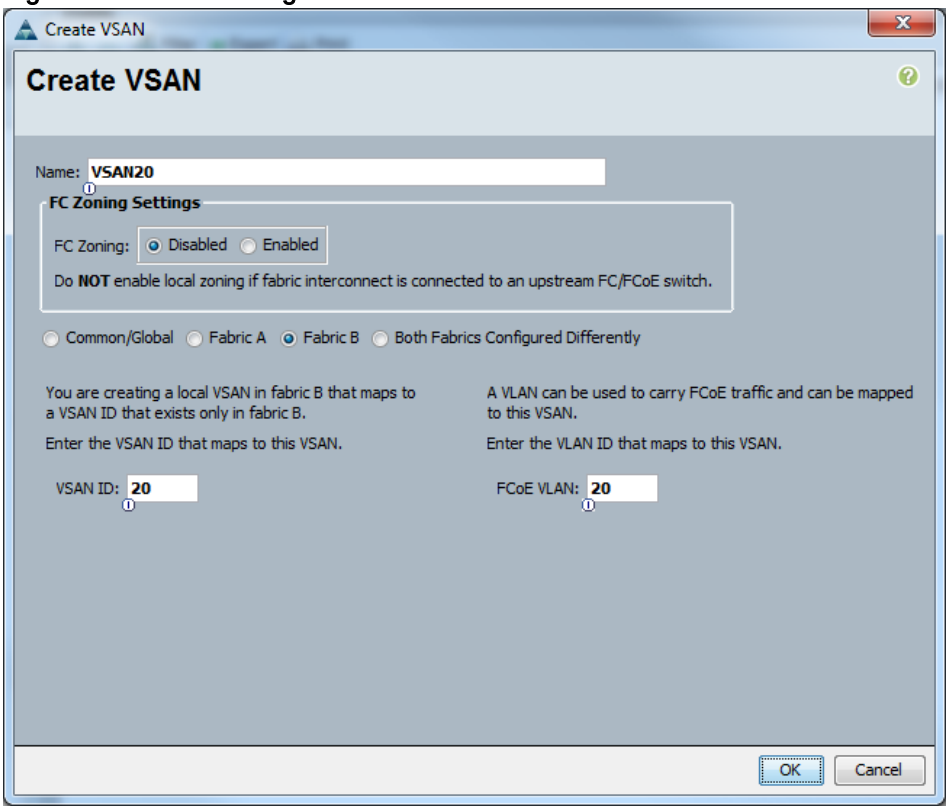
**Figure 233 UCS Manager – Create VSAN on Fabric A**




12. Expand Fabric B.
13. Right-click VSANs.
14. Select Create VSANs.
15. Enter <<var_ucs_vsan_b_name>> as the name of the VSAN.
16. Enter <<var_vsan_b_id>> as the VSAN ID and <<var_vsan_b_fcoe_id>> as the FCoE VLAN ID. FCoE VLAN ID should not have conflict with any of the VLANs configured before.

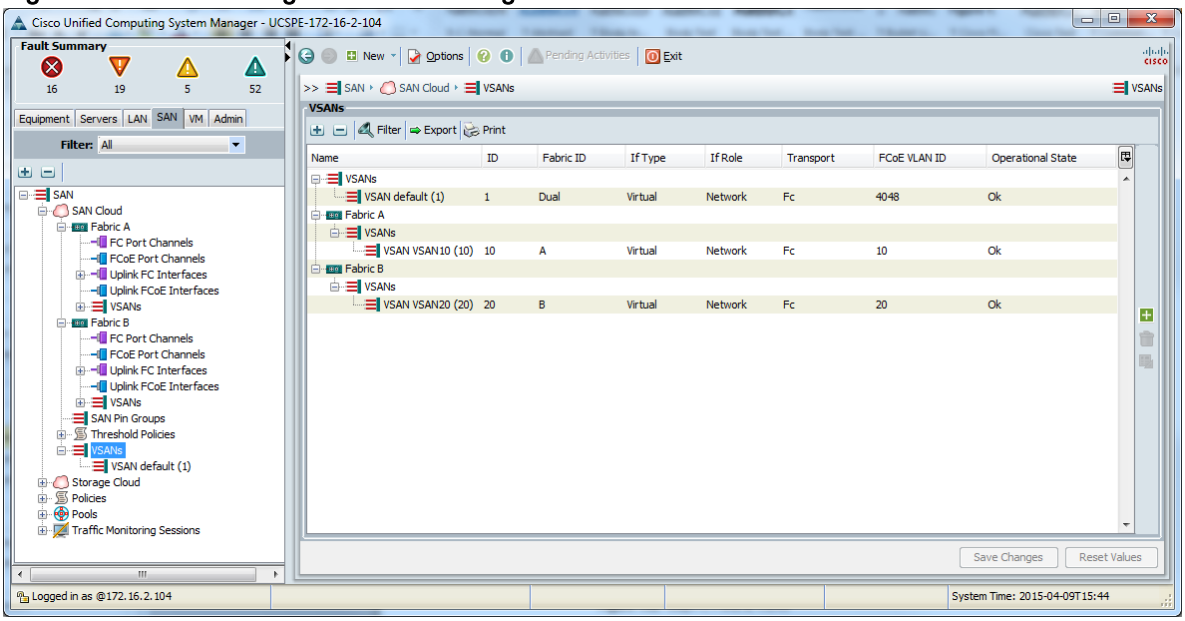
17. Select Fabric B.
18. Leave the FC zoning disabled (default).
19. Click OK.
20. Click OK.

Figure 234 UCS Manager – Create VSAN on Fabric B




21. Click SAN Cloud > VSANs (not in one of the Fabrics) to see the list of defined VSANs.

**Figure 235 UCS Manager – List of configured VSANs**

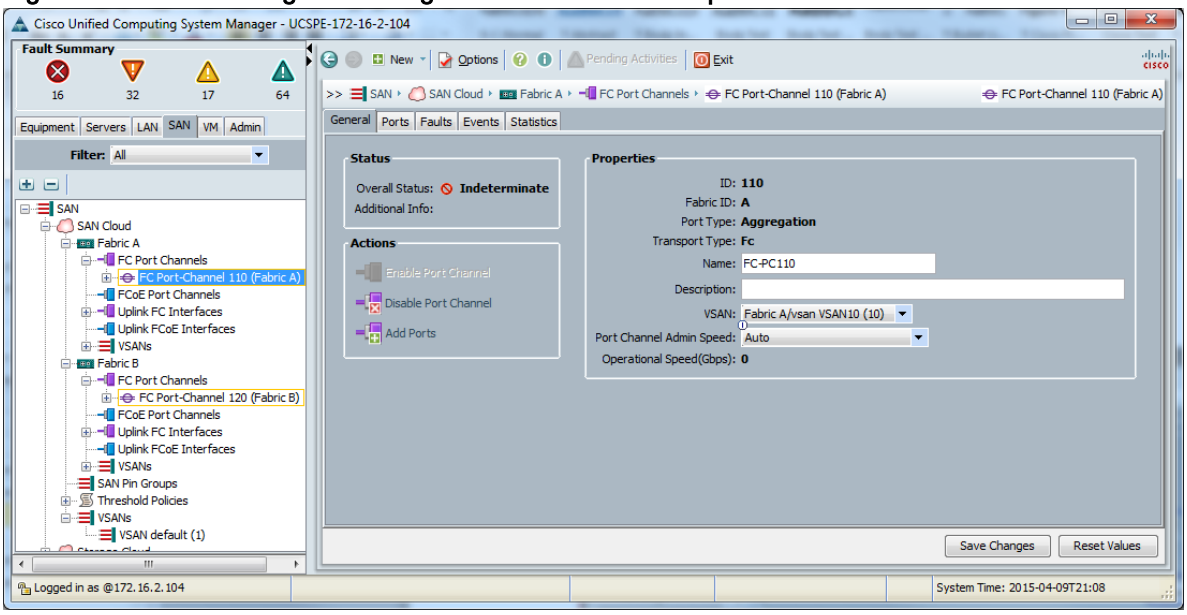



## Map FC ports to the VSAN

To map the FC ports to the created VSANs complete the following steps:

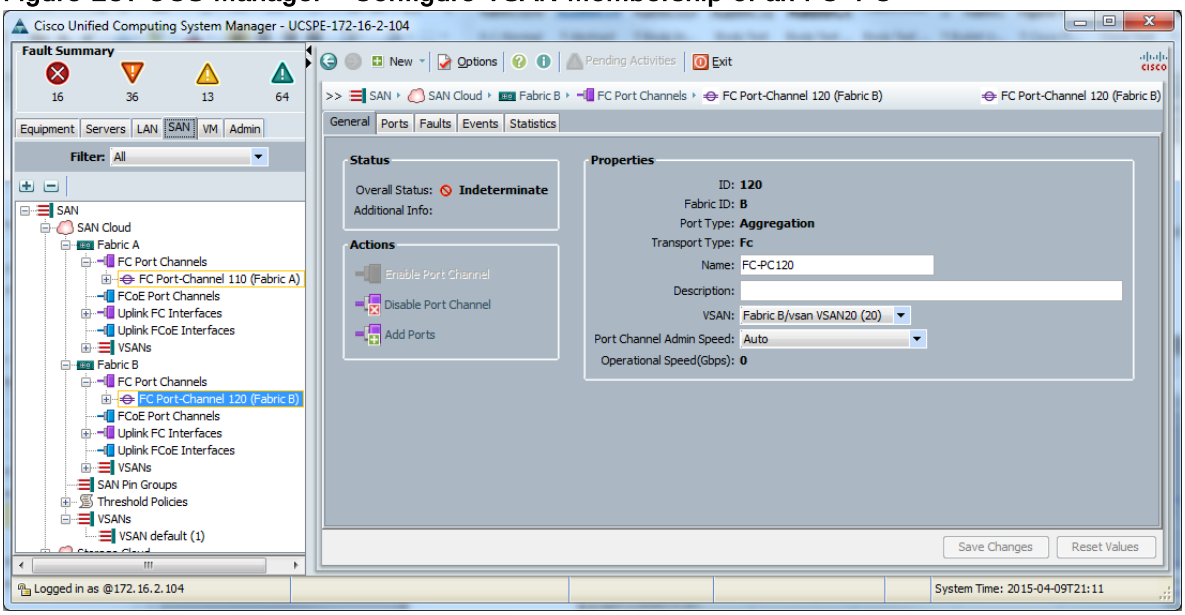
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > SAN Cloud.
3. Expand Fabric A.
4. Expand FC Port Channels.
5. Choose a FC Port Channel <<var_ucs_fcpc_a_name>>.
6. Change the VSAN to <<var_ucs_vsan_a_name>>; this is the Storage VSAN that was previously created.
7. Click Save Changes.
8. Click OK.

Figure 236 UCS Manager – Configure VSAN Membership of an FC-PC




9. Expand Fabric B.
10. Expand FC Port Channels.
11. Choose a FC Port Channel <<var_ucs_fcpc_b_name>>.
12. Change the VSAN to <<var_ucs_vsan_b_name>>, the Storage VSAN that was created in steps before.
13. Click Save Changes.
14. Click OK.

**Figure 237 UCS Manager – Configure VSAN Membership of an FC-PC**

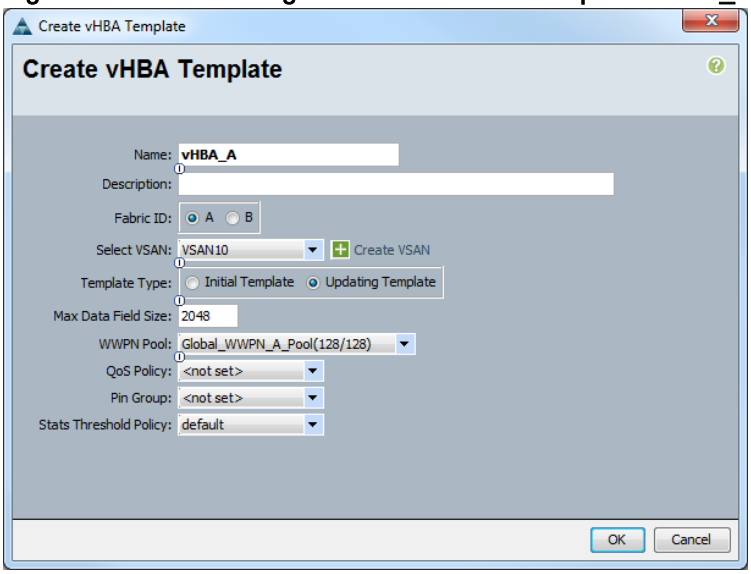



## Configure vHBA Templates

There are two required vHBA templates, one for Fabric A and one for Fabric B. To configure the vHBA templates, complete the following steps:

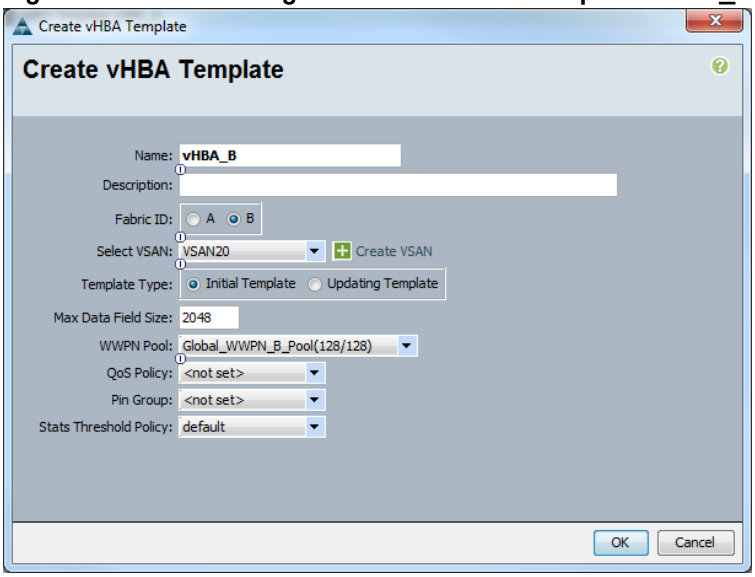
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter <<var_ucs_vhba_a_templ_name>> as the vHBA template name.
6. Keep Fabric A selected.
7. In the Select VSAN list, select <<var_ucs_vsan_a_name>>.
8. Select Updating Template as the Template type.
9. Select <<var_ucs_global_wwpn_a_pool_name>> as WWPN Pool.
10. Click OK.
11. Click OK.

Figure 238 UCS Manager – Create vHBA Template vHBA_A




12. Right-click vHBA Templates.
13. Select Create vHBA Template.
14. Enter <<var_ucs_vhba_b_templ_name>>  as the vHBA template name.
15. Keep Fabric B selected.
16. In the Select VSAN list, select <<var_ucs_vsan_b_name>>.
17. Select Updating Template as the Template type.
18. Select  <<var_ucs_global_wwpn_b_pool_name>> as WWPN Pool.
19. Click OK.
20. Click OK.

Figure 239 UCS Manager – Create vHBA Template vHBA_B




## Create SAN Connectivity Policy

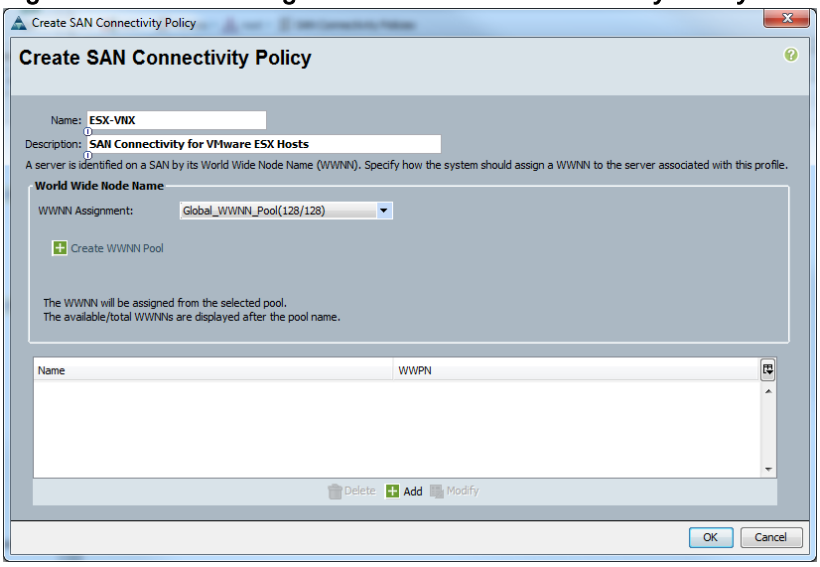
There are a few SAN Connectivity Policies required for the different use cases in this architecture. There is one for the VMware ESX hosts, one for SAP HANA scale-up and an additional one for SAP HANA scale-out. Based on your requirements, there may be more policy to define.

VMware ESX

To create the SAN Connectivity Policy for the VMware ESX hosts, complete the following steps:

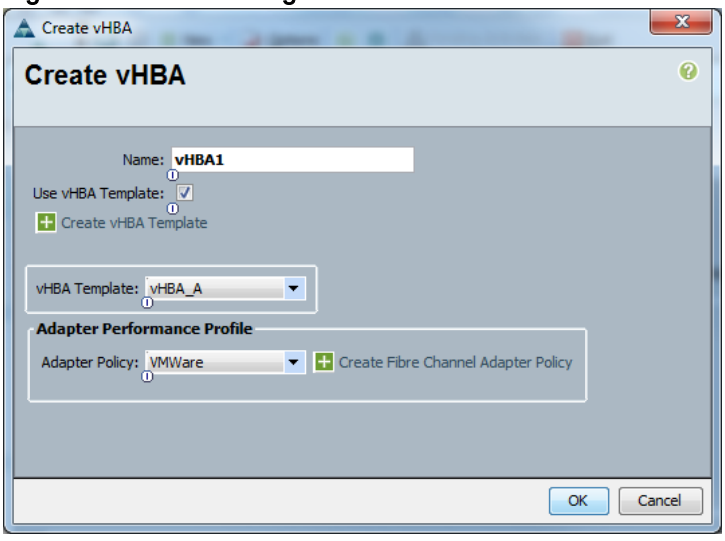
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter <<var_ucs_esx_san_connect_policy_name>> as the name.
6. Enter an optional description.
7. In the WWNN Assignment list, select <<var_ucs_global_wwnn_pool_name>>.
8. Click Add.

Figure 240 UCS Manager – Create SAN Connectivity Policy ESX-VNX



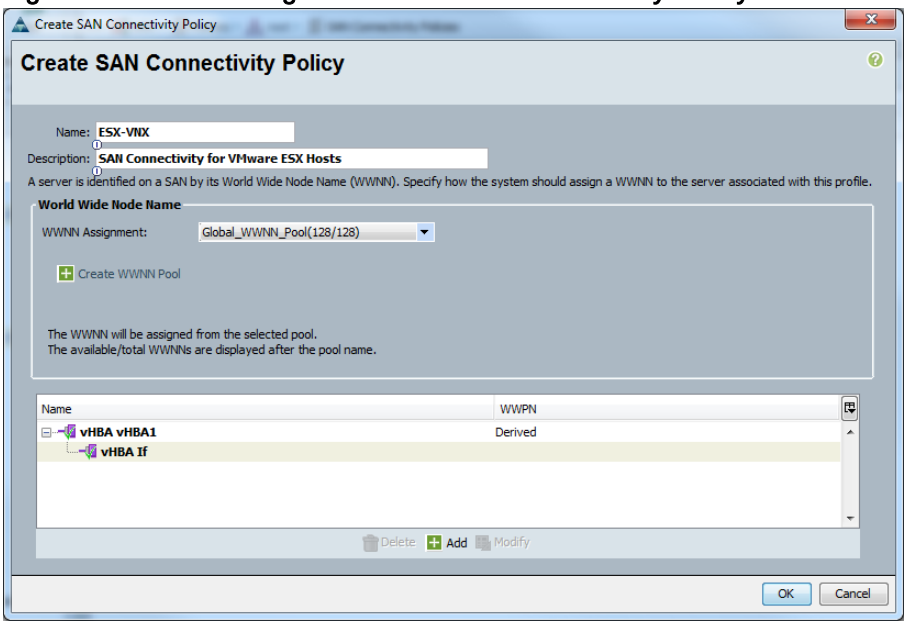

9. Enter <<var_ucs_vhba_1_name>> in the name field.
10. Select the checkbox to Use vHBA Template.
11. In the vHBA Template list, select <<var_ucs_vhba_a_templ_name>> .
12. In the Adapter Policy list, select VMWare.
13. Click OK.

Figure 241 UCS Manager – Create vHBA vHBA1



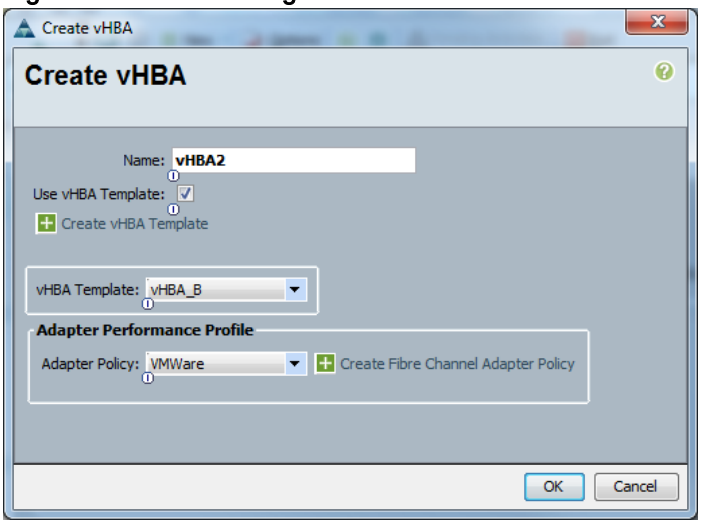

14. Click Add.

Figure 242 UCS Manager – Create SAN Connectivity Policy ESX-VNX




15. Enter <<var_ucs_vhba_2_name>> in the name field.
16. Select the checkbox to Use vHBA Template.
17. In the vHBA Template list, select <<var_ucs_vhba_b_templ_name>>.
18. In the Adapter Policy list, select VMWare.
19. Click OK.

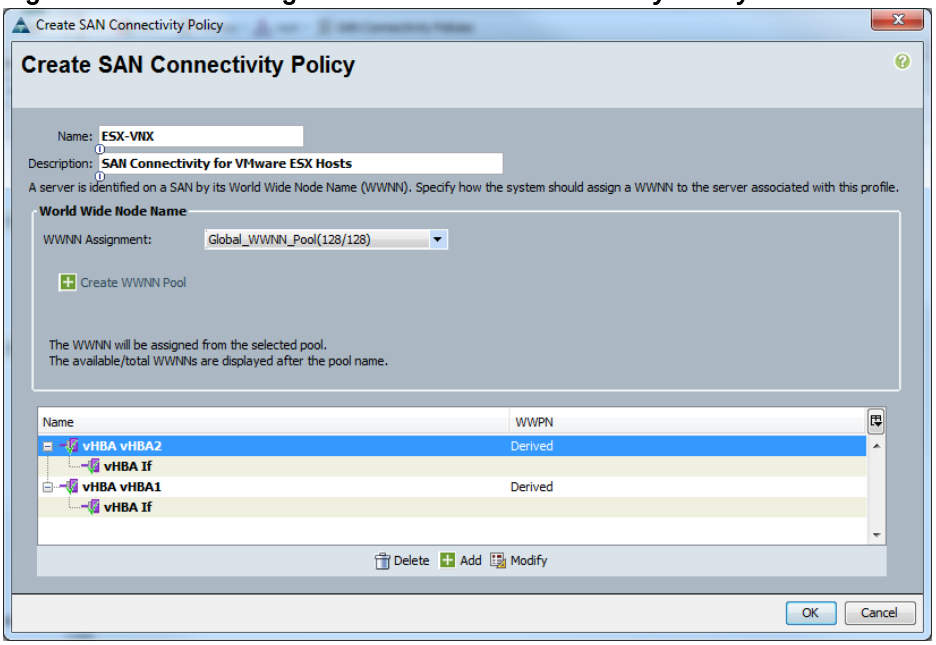
Figure 243 UCS Manager – Create vHBA vHBA2




20. Click OK.

21. Click OK.

**Figure 244 UCS Manager – Create SAN Connectivity Policy ESX-VNX**

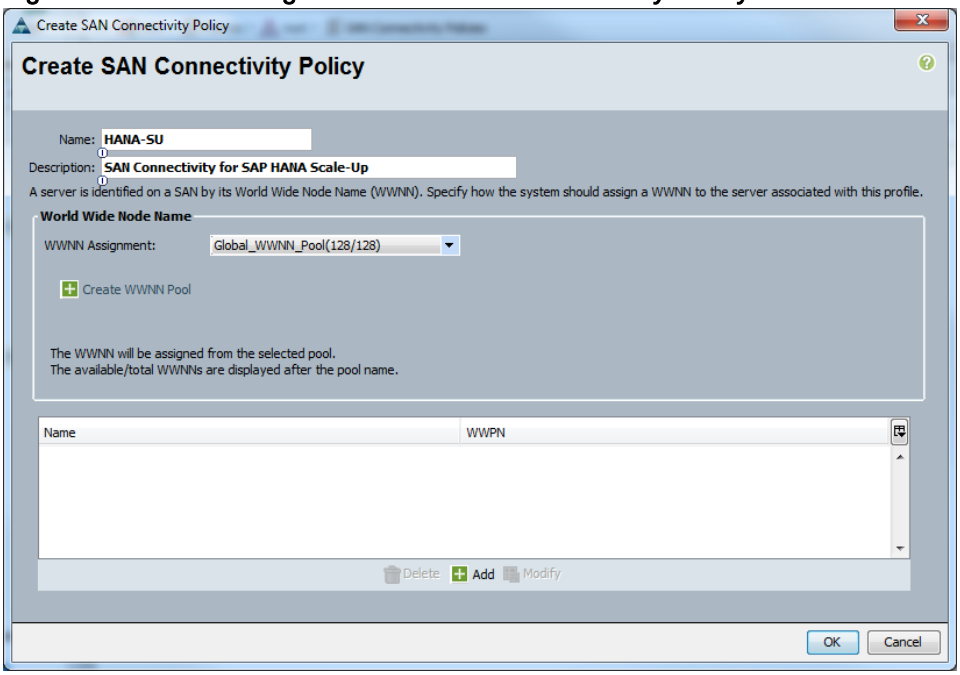



## SAP HANA Scale-Up

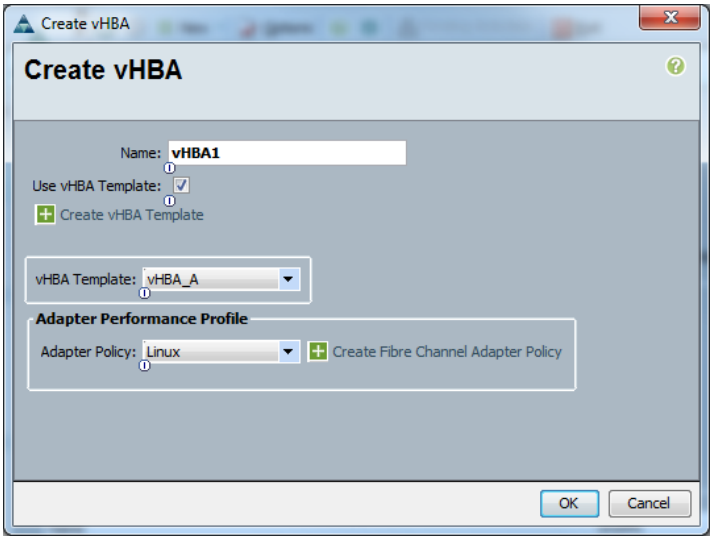
To create the SAN Connectivity Policy for the SAP HANA Scale-Out hosts, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter <<var_ucs_hana_su_connect_policy_name>> as the name.
6. Enter an optional description.
7. In the WWNN Assignment list, select <<var_ucs_global_wwnn_pool_name>>.
8. Click Add.

Figure 245 UCS Manager – Create SAN Connectivity Policy HANA-SU

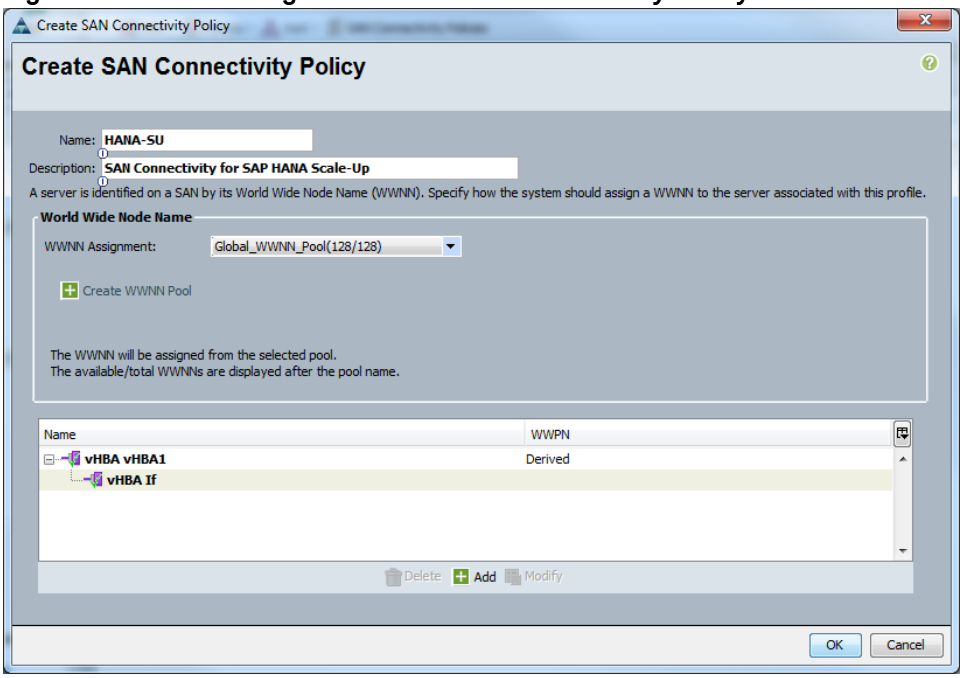



9. Enter <<var_ucs_vhba_1_name>> in the name field.
10. Select the checkbox to Use vHBA Template .
11. In the vHBA Template list, select <<var_ucs_vhba_a_templ_name>>.
12. In the Adapter Policy list, select Linux.
13. Click OK.
14. UCS Manager – Create vHBA vHBA1



15. Click Add.

Figure 246 UCS Manager – Create SAN Connectivity Policy HANA-SU




16. Enter <<var_ucs_vhba_2_name>> in the name field.

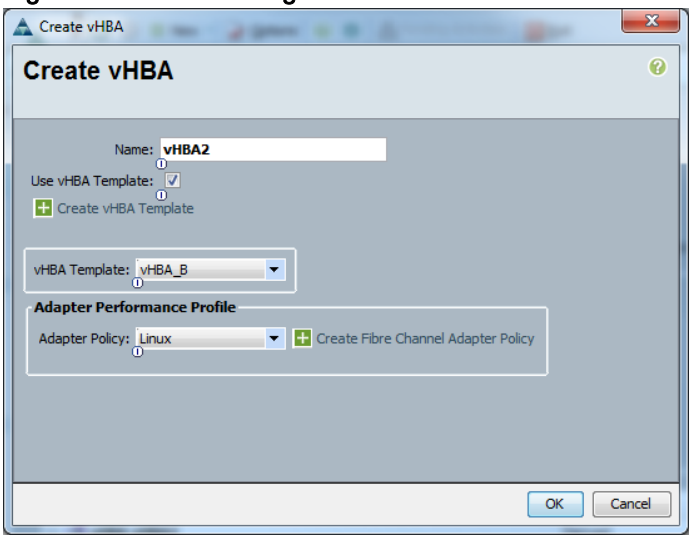
17. Select the checkbox to Use vHBA Template.

18. In the vHBA Template list, select <<var_ucs_vhba_b_templ_name>>.

19. In the Adapter Policy list, select Linux.

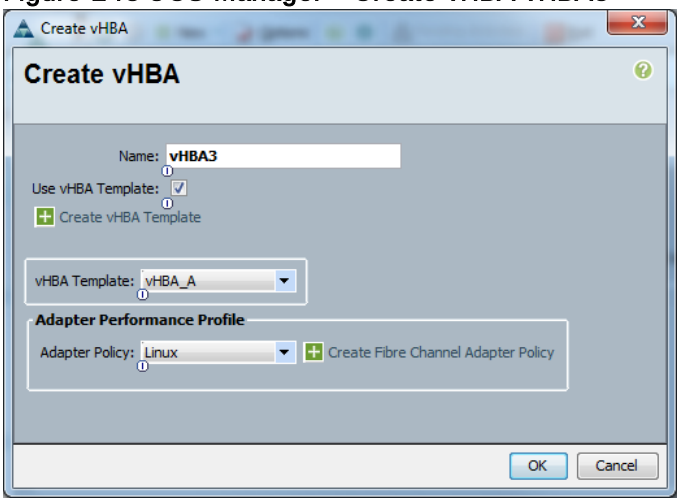
20. Click OK.

Figure 247 UCS Manager – Create vHBA vHBA2




21. Click OK.
22. Click Add.
23. Enter <<var_ucs_vhba_3_name>> in the name field.
24. Select the checkbox to Use vHBA Template.
25. In the vHBA Template list, select <<var_ucs_vhba_a_templ_name>>.
26. In the Adapter Policy list, select Linux.
27. Click OK.

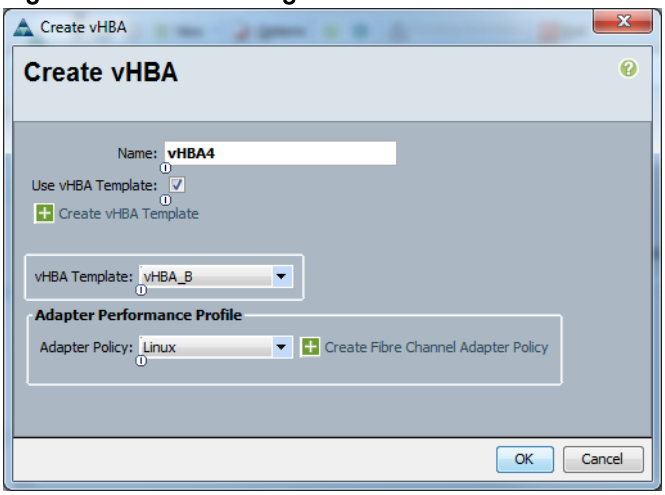
Figure 248 UCS Manager – Create vHBA vHBA3




28. Click OK.

29. Click Add.
30. Enter <<var_ucs_vhba_4_name>> in the name field.
31. Select the checkbox to Use vHBA Template.
32. In the vHBA Template list, select <<var_ucs_vhba_b_templ_name>>.
33. In the Adapter Policy list, select Linux.
34. Click OK.

Figure 249 UCS Manager – Create vHBA vHBA4




35. Click OK.
36. Click OK.

Figure 250 UCS Manager – Create SAN Connectivity Policy HANA-SU

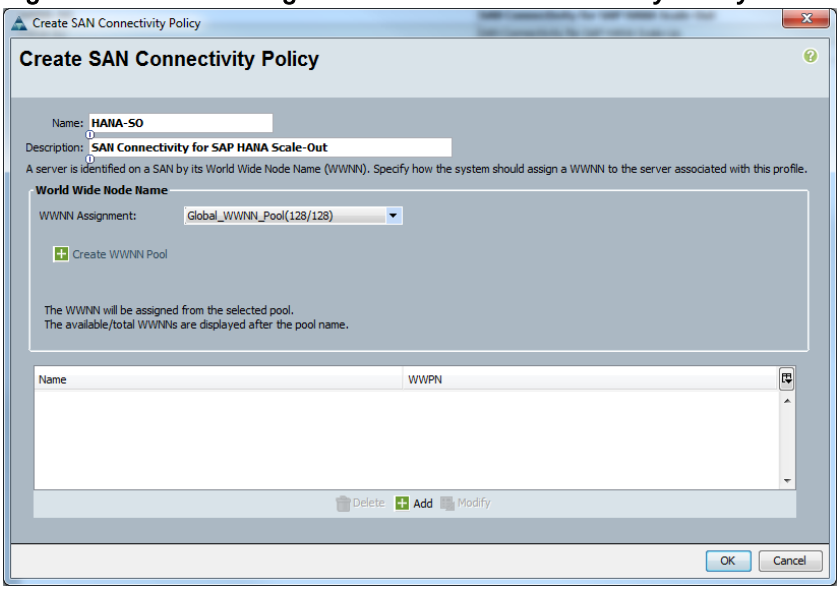



## SAP HANA Scale-Out

To create the SAN Connectivity Policy for the SAP HANA Scale-Out hosts, complete the following steps:

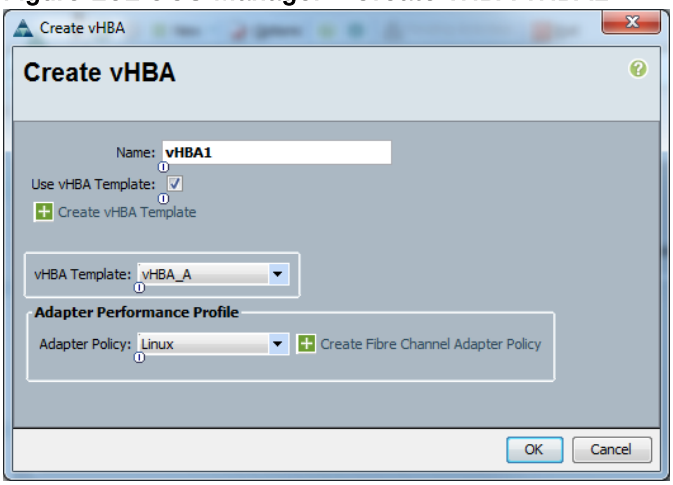
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter <<var_ucs_hana_so_connect_policy_name>> as the name.
6. Enter an optional description.
7. In the WWNN Assignment list, select <<var_ucs_global_wwnn_pool_name>>
8. Click Add.

Figure 251 UCS Manager – Create SAN Connectivity Policy HANA-SO



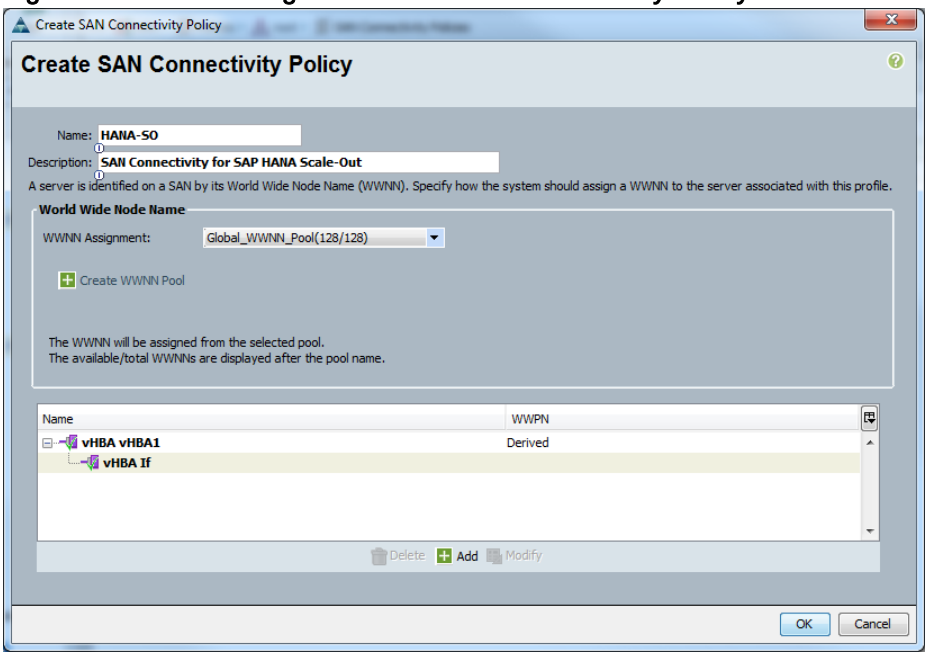

9. Enter <<var_ucs_vhba_1_name>> in the name field.
10. Select the checkbox to Use vHBA Template.
11. In the vHBA Template list, select <<var_ucs_vhba_a_templ_name>>.
12. In the Adapter Policy list, select Linux.
13. Click OK.

Figure 252 UCS Manager – Create vHBA vHBA1



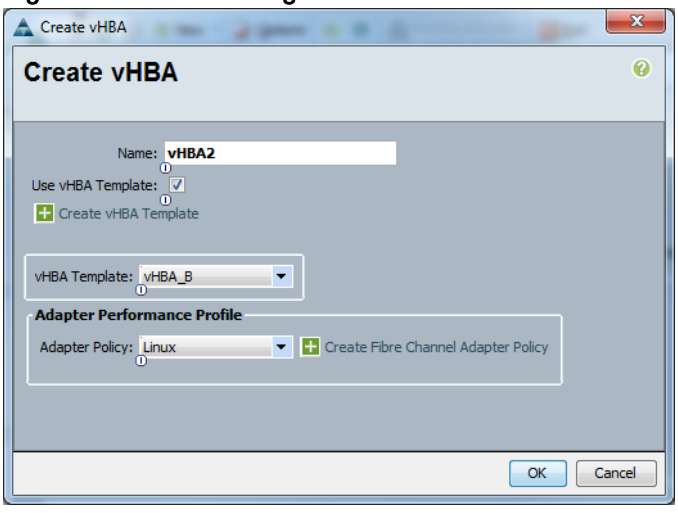

14. Click Add.

Figure 253 UCS Manager – Create SAN Connectivity Policy HANA-SO




15. Enter <<var_ucs_vhba_2_name>>  in the name field.
16. Select the checkbox to Use vHBA Template.
17. In the vHBA Template list, select <<var_ucs_vhba_b_templ_name>>.
18. In the Adapter Policy list, select Linux.
19. Click OK.

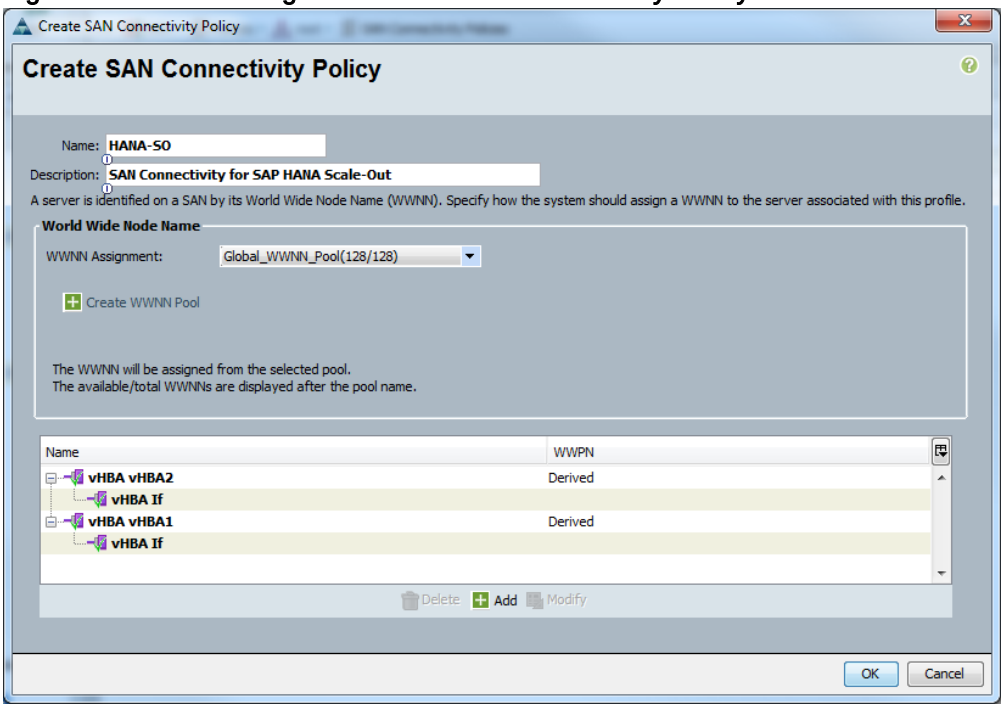
Figure 254 UCS Manager – Create vHBA vHBA2



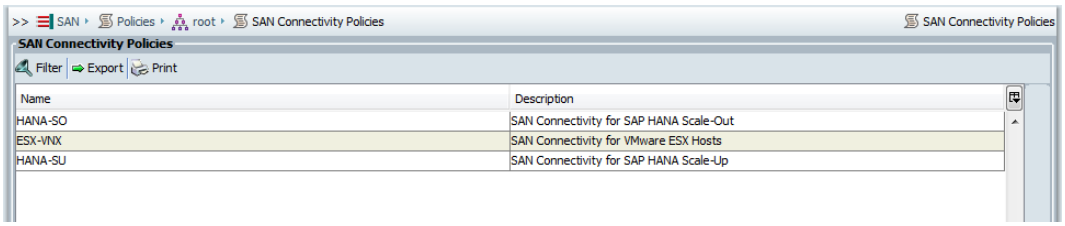

20. Click OK.

21. Click OK.

**Figure 255 UCS Manager – Create SAN Connectivity Policy HANA-SO**




Create additional SAN Connectivity Policies if required for your landscape.




## Configure Server (Service Profile) Policies and Pools

This section details the Server specific policy and pool configuration.

Table 31 lists the required information to setup the Server for the Cisco UCS in this Cisco UCS Integrated Infrastructure.

**Table 31 Information to Setup Cisco UCS in the Reference Architecture**

| Name | Variable |
|---|---|
| Name of the Power Control Policy | <<var_ucs_power_cont_policy>> |
| Name of Firmware Package for SAP HANA | <<var_ucs_hana_fw_package_name>> |

| Name | Variable |
|---|---|
| UCS Manager Version | <<var_ucs_manager_version>> |
| Name of the BIOS Policy for SAP HANA | <<var_ucs_hana_bios_policy_name>> |
| Name of the BIOS Policy for VMware ESX | <<var_ucs_esx_bios_policy_name>> |
| Name of the Serial Over LAN Profile | <<var_ucs_sol_profile>> |
| Name of the IPMI Policy | <<var_ucs_ipmi_policy>> |
| IPMI Admin User Name | <<var_ucs_ipmi_user>> |
| Password for the IPMI Admin User | <<var_ucs_ipmi_user_passwd>> |
| Name of the global UUID Pool | <<var_ucs_uuid_pool_name>> |
| Name of the Server Pool for SAP HANA | <<var_ucs_hana_server_pool>> |
| Name of the Server Qualification Policy for SAP HANA | <<var_ucs_hana_server_pool_qual_policy>> |
| Name of the Server Pool Policy for SAP HANA | <<var_ucs_hana_server_pool_policy>> |
| Name of the Server Pool for Non-SAP HANA Workloads | <<var_ucs_non-hana_server_pool>> |
| Name of the Boot Policy for SAN Boot | <<var_ucs_san_boot_policy>> |
| Name of the first vHBA in a Service Profile | <<var_ucs_vhba_1_name>> |
| Name of the second vHBA in a Service Profile | <<var_ucs_vhba_2_name>> |

### Power Control Policy

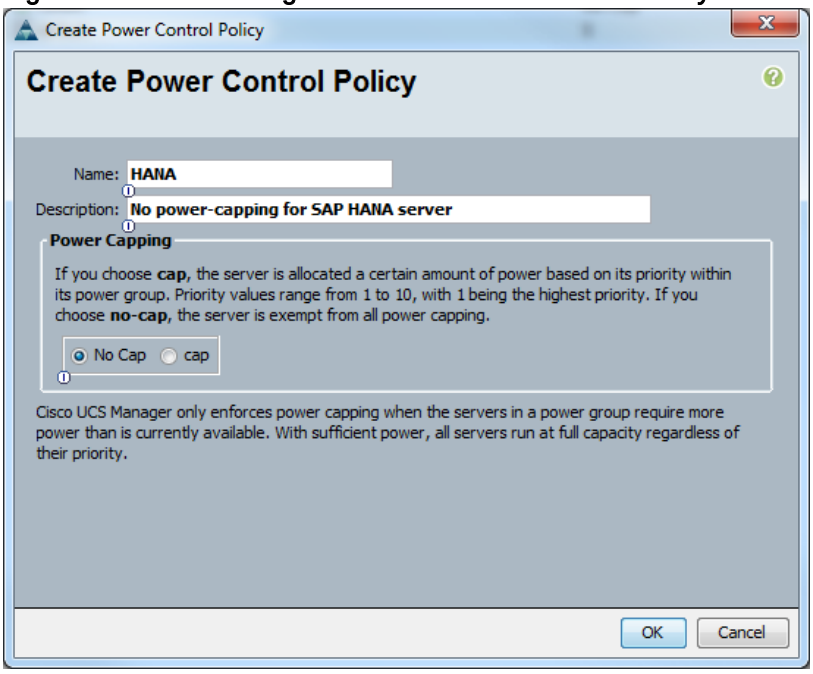
The Cisco UCS feature, power-capping, is designed to save power with legacy data center use cases. This feature does not fit to the high performance behavior of SAP HANA. In case power-capping is configured on a UCS global base this power control policy for the SAP HANA nodes takes care that the power-capping does not apply to the nodes. The Power Capping feature must be defined as No Cap.

To create a power control policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Power Control Policies.
4. Select Create Power Control Policy.

5. Enter <<var_ucs_power_cont_policy>> as the power control policy name.
6. Change the power capping setting to No Cap.
7. Click OK to create the power control policy.
8. Click OK.

Figure 256 UCS Manager – Create Power Control Policy




## Create Host Firmware Package

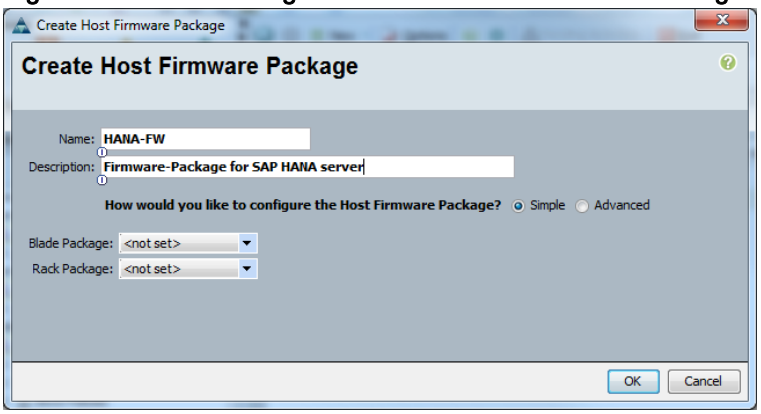
Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter <<var_ucs_hana_fw_package_name>> as the name of the host firmware package.
6. Leave Simple selected.

7. Select the version <<var_ucs_manager_version>> for both the Blade and Rack Packages.
8. Click OK to create the host firmware package.
9. Click OK.

**Figure 257 UCS Manager – Create Host Firmware Package**

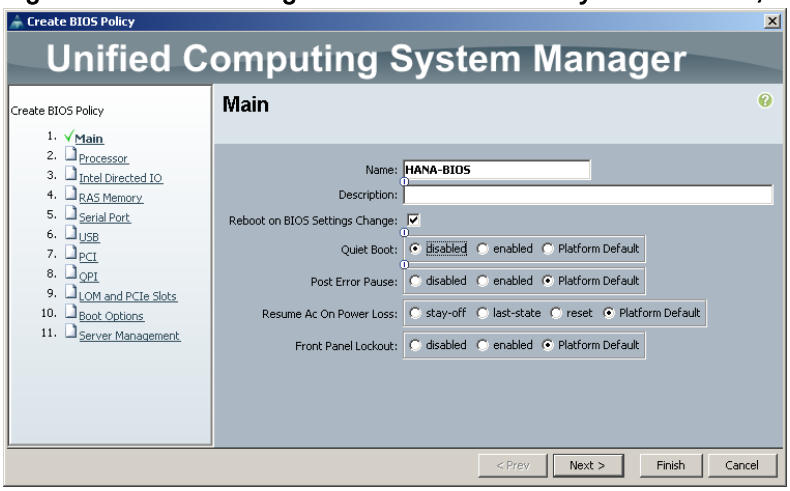



## Create Server BIOS Policy for SAP HANA Bare Metal

To get best performance for HANA it is required to configure the Server BIOS accordantly. To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter <<var_ucs_hana_bios_policy_name>> as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.

Figure 258 UCS Manager – Create BIOS Policy HANA-BIOS, Main Settings

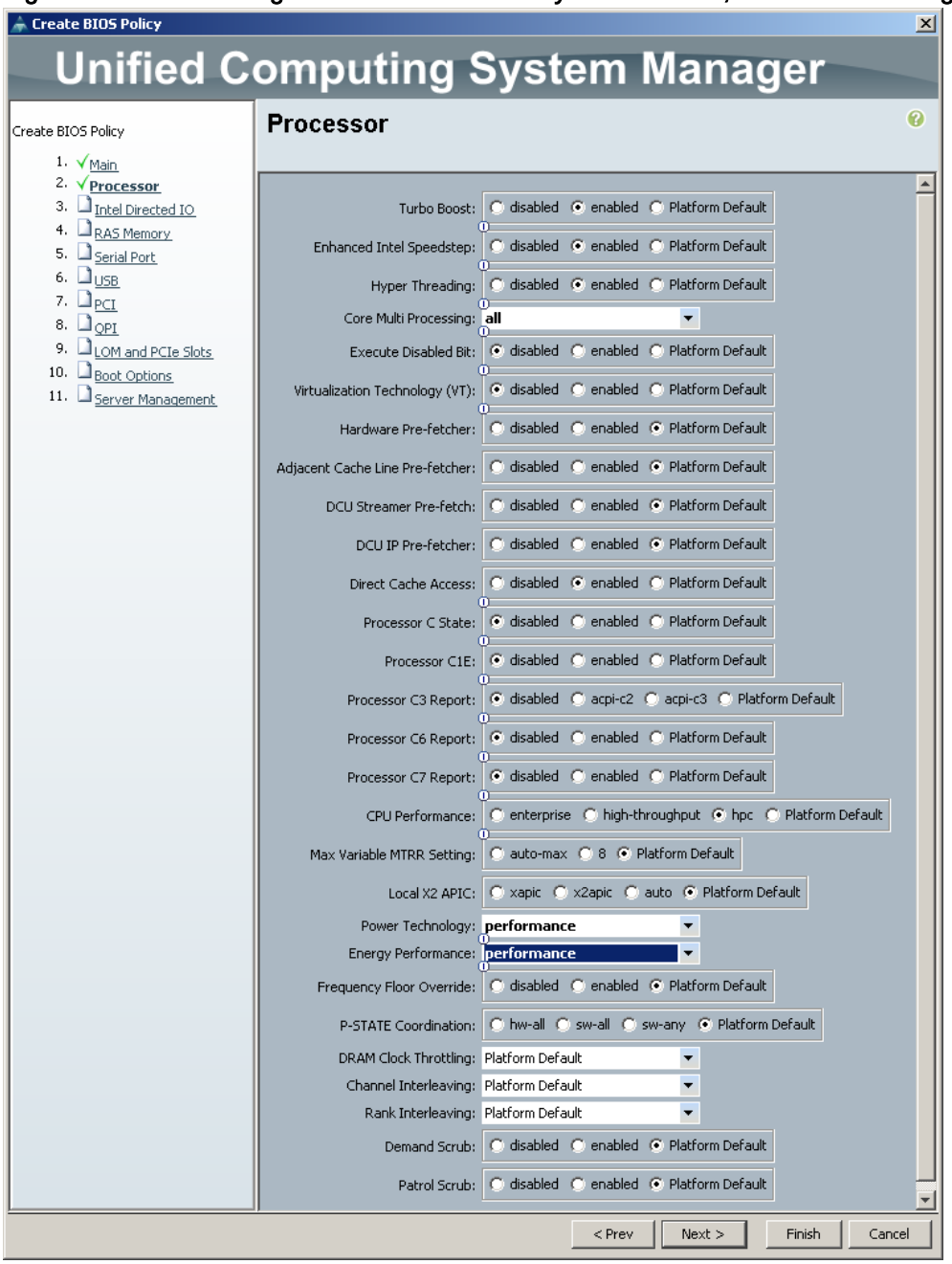



7. Click Next.



The recommendation from SAP for SAP HANA is to disable all Processor C States. This will force the CPU to stay on maximum frequency and allow SAP HANA to run with best performance.

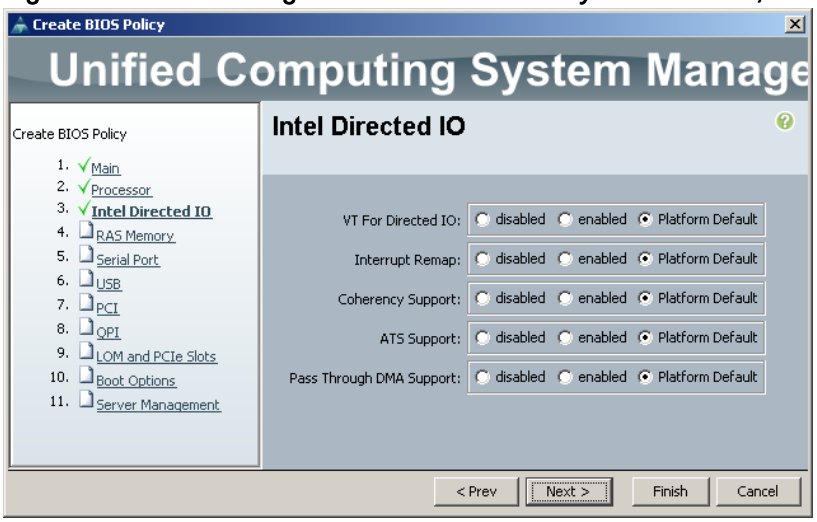
Figure 259 UCS Manager – Create BIOS Policy HANA-BIOS, Processor Settings




8. Click Next.

9. No changes are required at the Intel Direct IO.

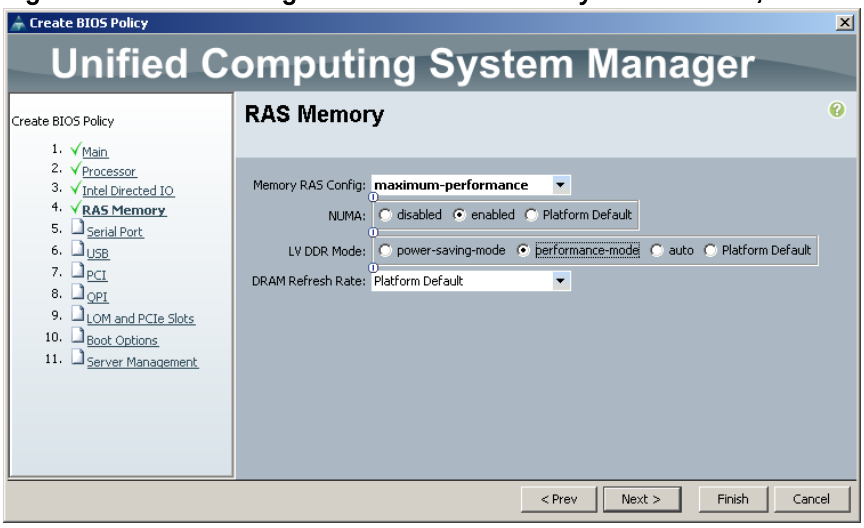
Figure 260 UCS Manager – Create BIOS Policy HANA-BIOS, Intel Direct IO Settings




10. Click Next.

11. In the RAS Memory Tab, select maximum-performance and enable NUMA.

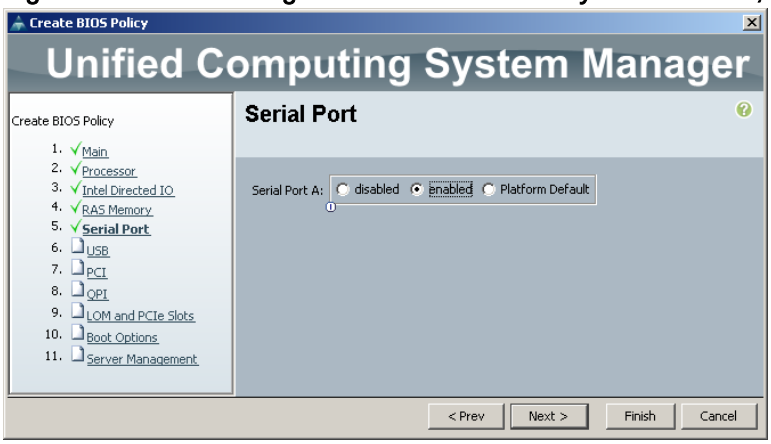
Figure 261 UCS Manager – Create BIOS Policy HANA-BIOS, RAS Memory settings




12. Click Next.

13. In the Serial Port Tab the Serial Port A: must be enabled.

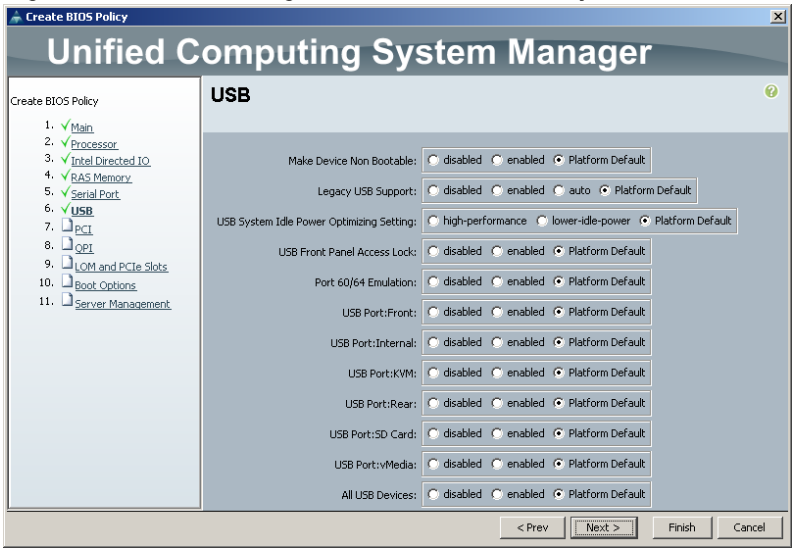
Figure 262 UCS Manager – Create BIOS Policy HANA-BIOS, Serial Port settings




14. Click Next.

15. No changes are required for the USB settings.

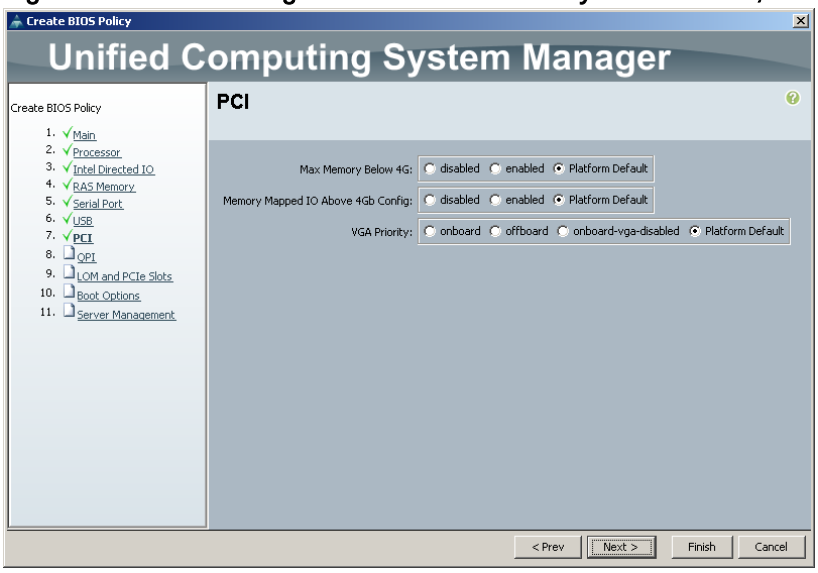
Figure 263 UCS Manager – Create BIOS Policy HANA-BIOS, USB Settings




16. Click Next.

17. No changes are required for the PCI Configuration.

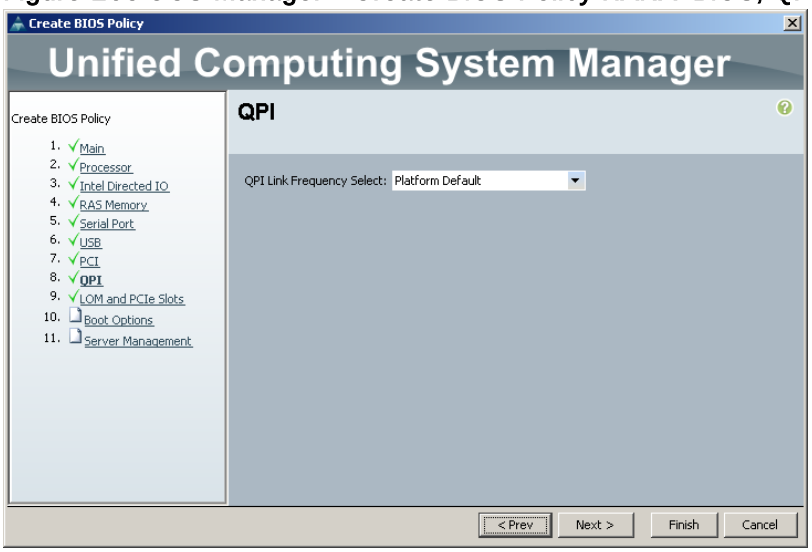
Figure 264 UCS Manager – Create BIOS Policy HANA-BIOS, PCI Settings




18. Click Next.

19. No changes are required for the QPI.

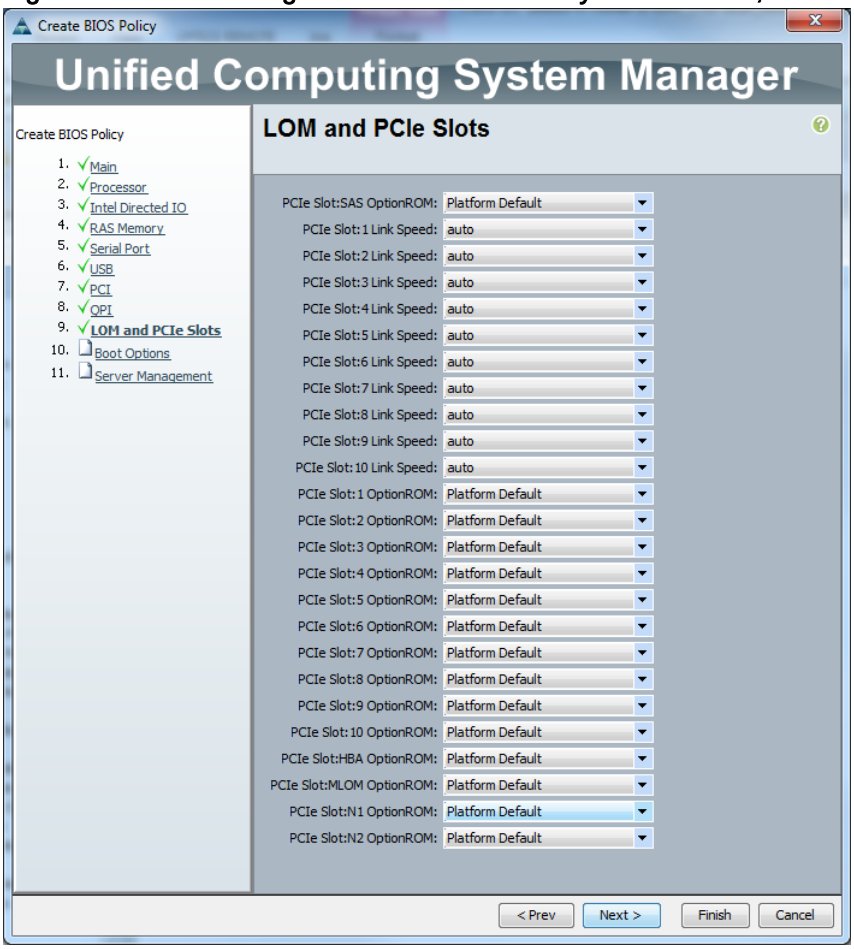
Figure 265 UCS Manager – Create BIOS Policy HANA-BIOS, QPI Settings




20. Click Next.

21. Select auto for all PCIe Slot Link Speed entries.

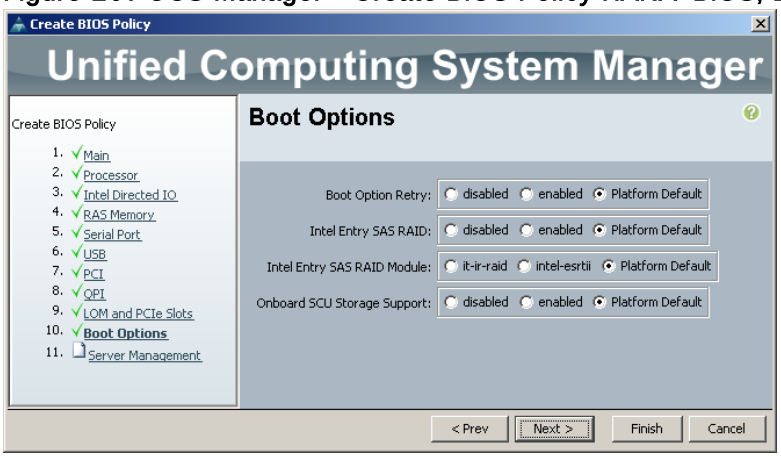
Figure 266 UCS Manager – Create BIOS Policy HANA-BIOS, LOM and PCIe Slots Settings




22. Click Next.

23. No changes are required for the Boot Options.

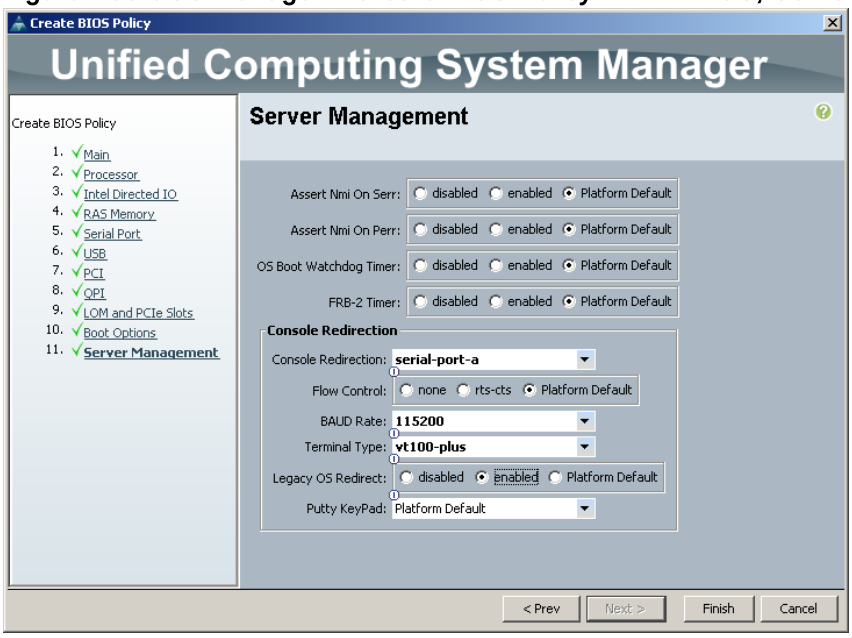
Figure 267 UCS Manager – Create BIOS Policy HANA-BIOS, Boot Options Settings




24. Click Next.

25. Configure the Console Redirection to serial-port-a with the BAUD Rate 115200 and enable the feature Legacy OS redirect. This is used for Serial Console Access over LAN to all SAP HANA servers.

Figure 268 UCS Manager – Create BIOS Policy HANA-BIOS, Server Management Settings




26. Click Finish to Create BIOS Policy.

27. Click OK.

## Create Server BIOS Policy for VMware ESX

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter <<var_ucs_esx_bios_policy_name>> as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.
7. Click Next.
8. Select Hyper Threading enabled.
9. Select Virtualization Technology (VT) enabled.

10. Click Finish to create the BIOS policy.

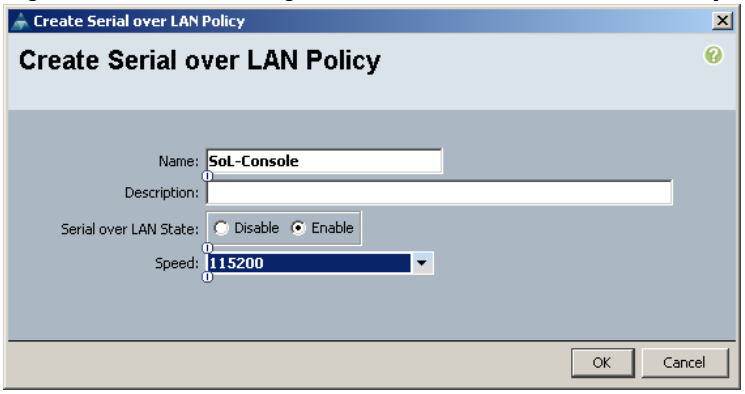
### Create Serial over LAN Policy

The Serial over LAN policy is required to get console access to all SAP HANA servers through SSH from the management network. This is used in case the server hangs or a Linux kernel crash dump is required. Configure the speed as the same as in the Server Management Tab of the BIOS Policy.

To create the Serial over LAN policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Serial over LAN Policies.
4. Select Create Serial over LAN Policy.
5. Enter <<var_ucs_sol_profile>> as the Policy name.
6. Select Serial over LAN State to enable.
7. Change the Speed to 115200.
8. Click OK.

**Figure 269 UCS Manager – Create Serial over LAN Policy**




### Update the Default Maintenance Policy

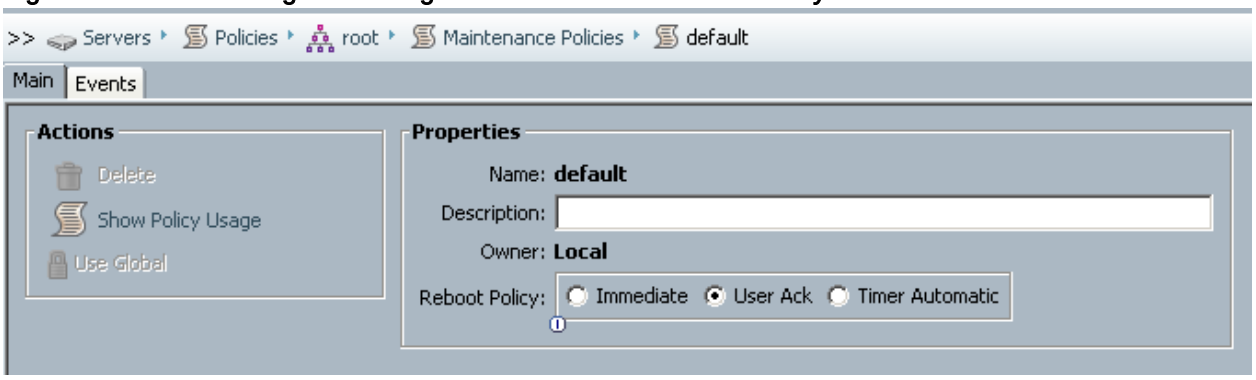
It is recommended to update the default Maintenance Policy with the Reboot Policy “User Ack” for the SAP HANA server. This policy will wait for administrator to acknowledge the reboot for the servers after the Cisco UCS configuration change has taken effect.

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.

3. Select Maintenance Policies > default.
4. Change the Reboot Policy to User Ack.
5. Click Save Changes.
6. Click OK to accept the change.

**Figure 270 UCS Manager – Configure Default Maintenance Policy**



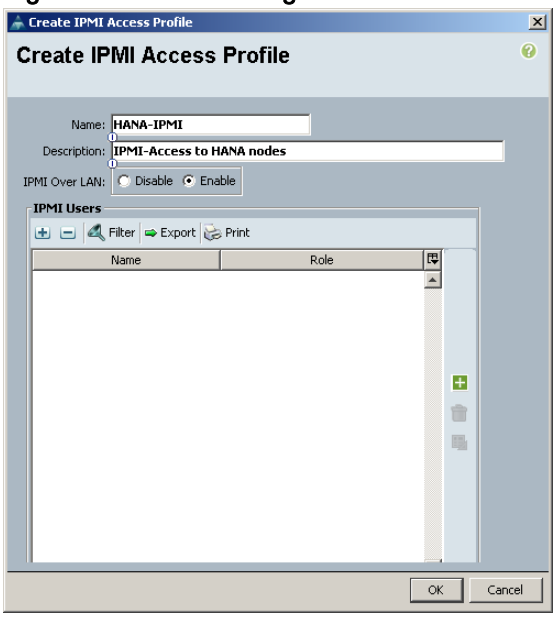

## IPMI Access Profiles

The Serial over LAN access requires an IPMI access control to the board controller. This is also used for the STONITH function of the SAP HANA mount API to kill a hanging server. The default user in the configuration is sapadm with the password “cisco”. You can specify this user as required for your configuration.

To create an IPMI Access Profile, complete the following steps:

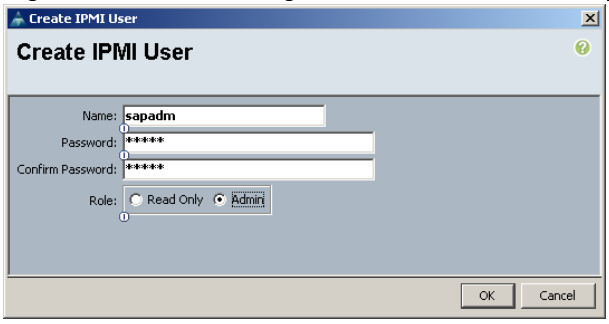
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click IPMI Access Profiles.
4. Select Create IPMI Access Profile.
5. Enter <<var_ucs_ipmi_policy>> as the Profile name.

Figure 271 UCS Manager – Create IPMI Access Profile HANA-IPMI



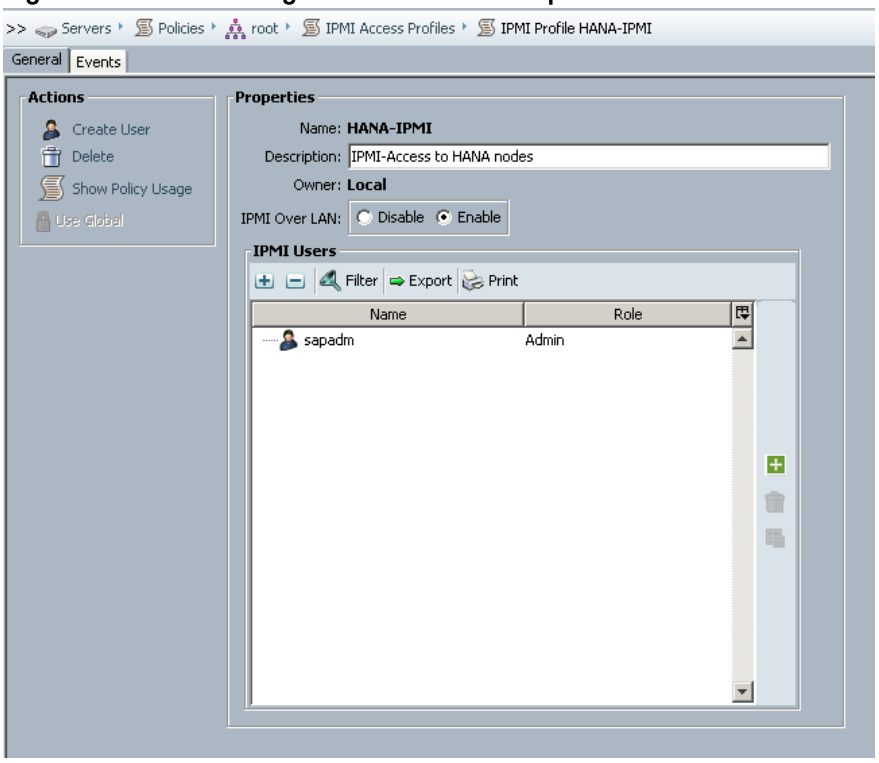

6. Click + (add) button.
7. Enter <<var_ucs_ipmi_user>> in the Name field.
8. Enter <<var_ucs_ipmi_user_passwd>> in the Password and Confirm Password fields.
9. Select Admin as Role.

Figure 272 UCS Manager – Create IPMI User sapadm




10. Click OK to create user.
11. Click OK to Create IPMI Access Profile.
12. Click OK.

Figure 273 UCS Manager – IMPI Profile Properties

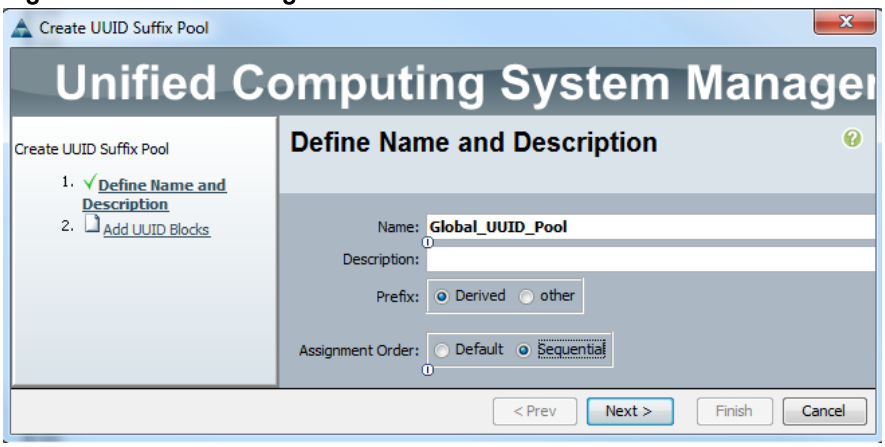



## Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

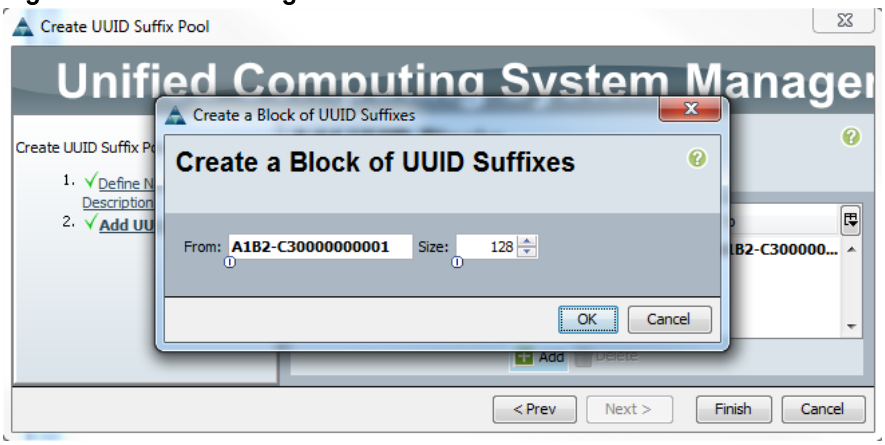
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter <<var_ucs_uuid_pool_name>> as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for Assignment Order.
9. Click Next.

Figure 274 UCS Manager – Create UUID Suffix Pool




10. Click Add to add a block of UUIDs.
11. Keep the From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.

Figure 275 UCS Manager – Create a Block of UUID Suffixes




13. Click OK.
14. Click Finish.
15. Click OK.

## Server Pool for SAP HANA

The configuration of a server to run SAP HANA is well defined by SAP. Within Cisco UCS it is possible to specify a Policy to collect all servers for SAP HANA in a pool. The definition for all servers with 1024 GB memory and 60 cores running a higher frequency is 2800 MHz. Create the server pool(s) in a way that best fits your needs.

### Create Server Pool

To configure the necessary server pools for the Cisco UCS environment, complete the following steps:



Consider creating unique server pools to achieve the granularity that is required in your environment.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter <<var_ucs_hana_server_pool>> as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Click Finish.
9. Click OK.

### Create Server Pool Policy Qualifications

To configure the qualification for the server pool, complete the following steps:

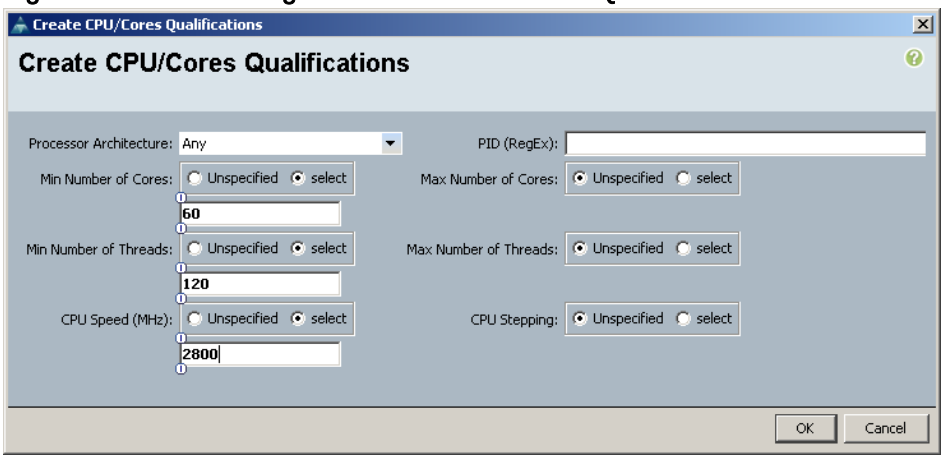


Consider creating unique server pools for each type of SAP HANA servers. The following steps show qualifications for Cisco UCS B460-M4 with 1TB RAM and Intel E7-4890 Processors for SAP HANA.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > Server Pool Policy Qualifications.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualifications
5. Enter <<var_ucs_hana_server_pool_qual_policy>> as the name of the server pool.
6. Optional: Enter a description for the server pool policy qualification.
7. In the Actions panel click Create Memory Qualifications.
8. On Min Cap (MB) choose select button and enter 1048576 (for B260-M4 with 512 GB memory use 524288).

9. Click OK.
10. In the Actions panel click Create CPU/Cores Qualifications.
11. On Min Number of Cores choose select button and enter 60 (for B260-M4 with 2 Socket choose 30).
12. On Min Number of Threads choose select button and enter 120 (for B260-M4 with 2 Socket choose 60).
13. On CPU Speed (MHz) choose select button and enter 2800.
14. Click OK.
15. Click OK.
16. Click OK.

Figure 276 UCS Manager – Create CPU/Cores Qualification




## Server Pool Policy

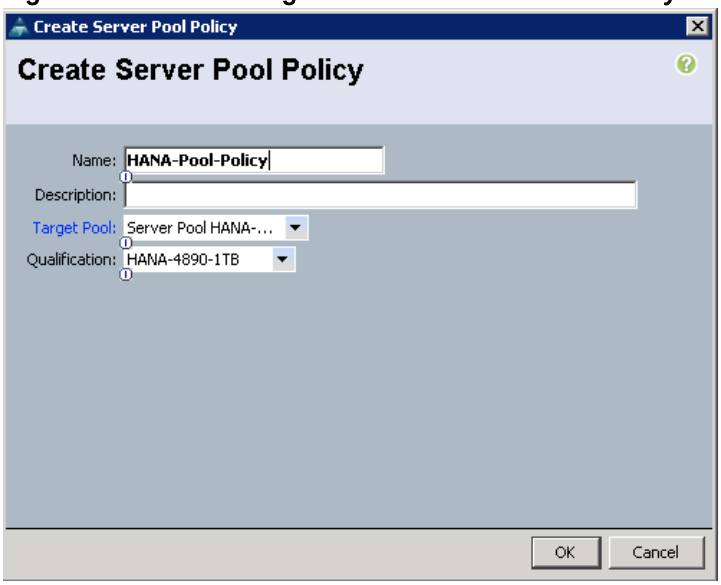
The server pool for the SAP HANA nodes is defined and the qualification policy is also defined. With the Server Pool Policy the two definitions are mapped together.

To create the Server Pool policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > Server Pool Policies.
3. Right-click Server Pool Policy.
4. Select Create Server Pool Policy.
5. Enter <<var_ucs_hana_server_pool_policy>> as the name of the server pool.

6. For Target Pool choose <<var_ucs_hana_server_pool>> Server Pool created from the drop-down menu.
7. For Qualification choose <<var_ucs_hana_server_pool_qual_policy>> Server Pool Policy Qualifications created from the drop-down menu.
8. Click OK.

**Figure 277 UCS Manager – Create Server Pool Policy**




## Create Server Pool for Non-SAP HANA Hosts

For the VMware ESX hosts hosting non-SAP HANA applications, using a server pool simplifies the administrative work.

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:

1. Consider creating unique server pools to achieve the granularity that is required in your environment.
2. In Cisco UCS Manager, click the Servers tab in the navigation pane.
3. Select Pools > root.
4. Right-click Server Pools.
5. Select Create Server Pool.
6. Enter <<var_ucs_non-hana_server_pool>> as the name of the server pool.
7. Optional: Enter a description for the server pool.
8. Click Next.

9. Select All servers you like to use for Non-SAP HANA workloads from the Servers list.
10. Click >>.
11. Click Finish.

### Create Boot Policies

This procedure applies to a Cisco UCS environment in which two vHBA interfaces are configured per service profile.

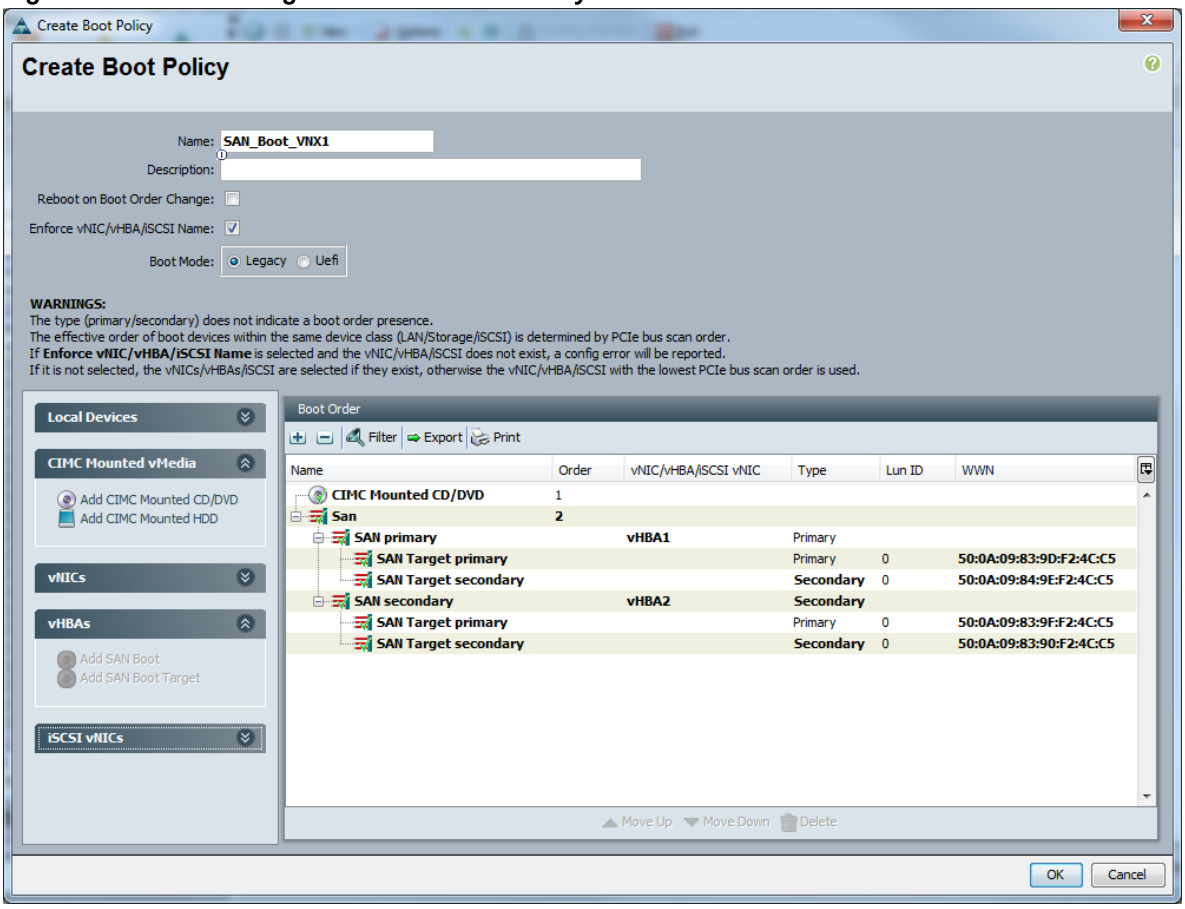
The boot policy is configured in this procedure. This policy configures the primary target to be EMC-VNX-1.

To create boot policies for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter <<var_ucs_san_boot_policy>> as the name of the boot policy.
6. Optional: Enter a description for the boot policy.
7. Keep the Reboot on Boot Order Change option cleared.
8. Expand the CIMC Mounted vMedia drop-down menu and select Add CIMC Mounted CD/DVD.
9. Expand the vHBAs section and select Add SAN Boot.
10. In the Add SAN Boot dialog box, enter <<var_ucs_vhba_1_name>>.
11. Click OK.
12. Select Add SAN Boot Target.
13. In the Boot Target LUN dialog box, enter 0.
14. In the Boot Target WWPN dialog box, enter the WWPN of VNX1-SPA-FC0 (50:0a:09:83:9d:f2:4c:c5).
15. Select Primary as the Type.
16. Click OK.
17. Select Add SAN Boot Target.
18. In the Boot Target LUN dialog box, enter 0.

19. In the Boot Target WWPN dialog box, enter the WWPN of VNX1-SPB-FC0 (50:0a:09:84:9e:f2:4c:c5).
20. Click OK.
21. Select Add SAN Boot.
22. In the Add SAN Boot dialog box, enter <<var_ucs_vhba_2_name>>.
23. Click OK.
24. Select Add SAN Boot Target.
25. In the Boot Target LUN dialog box, enter 0.
26. In the Boot Target WWPN dialog box, enter the WWPN of VNX1-SPA-FC1 (50:0a:09:83:9f:f2:4c:c5).
27. Select Primary as the Type.
28. Click OK.
29. Select Add SAN Boot Target.
30. In the Boot Target LUN dialog box, enter 0.
31. In the Boot Target WWPN dialog box, enter the WWPN of VNX1-SPB-FC1 (50:0a:09:84:90:f2:4c:c5).
32. Click OK.
33. Click OK to save the boot policy. Click OK to close the Boot Policy window.

Figure 278 UCS Manager – Create Boot Policy




## Configure Server Ports

Server ports are all ports where a Cisco UCS Chassis, FEX for Cisco UCS C-Series connection, or a Cisco UCS C-Series is connected.

To enable server ports, complete the following steps:

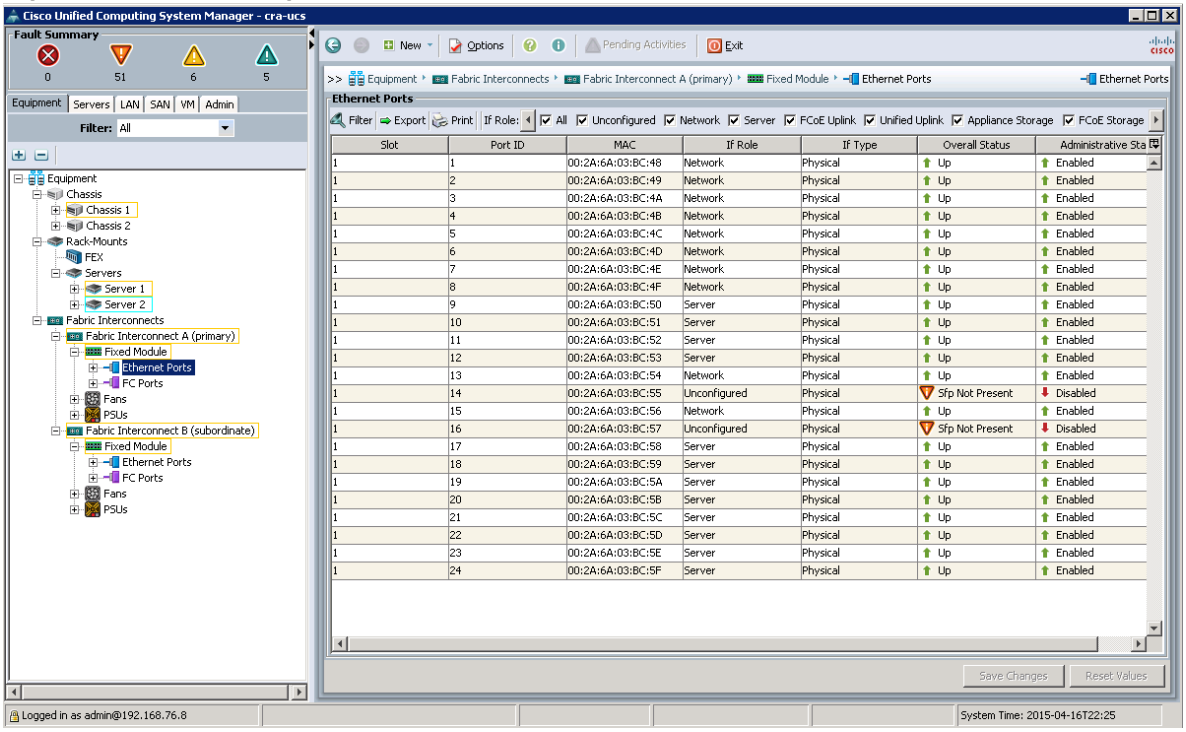
1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Click Ethernet Ports.
4. Select the ports that are connected to the chassis and / or to the Cisco C-Series Server, right-click them, and select Configure as Server Port.
5. Click Yes to confirm server ports and click OK.
6. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
7. Click Ethernet Ports.

8. Select the ports that are connected to the chassis and / or to the Cisco C-Series Server, right-click them, and select Configure as Server Port.

9. Click Yes to confirm server ports and click OK.

10. Verify that the ports connected to the chassis and / or to the Cisco C-Series Server are now configured as server ports.

**Figure 279 UCS Manager – List of Ethernet Ports on Fabric Interconnect A**




After the Server ports are configured, the Cisco UCS Manager will start the chassis and server discovery. This can take a while, especially if the firmware on the IO-Modules is not the same version as the Cisco UCS Manager version, and the Cisco UCS Manager has to run a firmware upgrade or downgrade.

## Configure the Service Profile Templates to Run VMware ESXi

This section details creating the Service Profile template in Cisco UCS that is used as the foundation for all VMware ESXi hosts deployed in this architecture.

Table 32 lists the required information for the Service Profile Template setup in Cisco UCS.

**Table 32 Information to Setup Cisco UCS in the Reference Architecture**

| Name | Variable |
|---|---|
| Name of the Service Profile Template for Vmware ESX | <<var_ucs_esx_template_name>> |

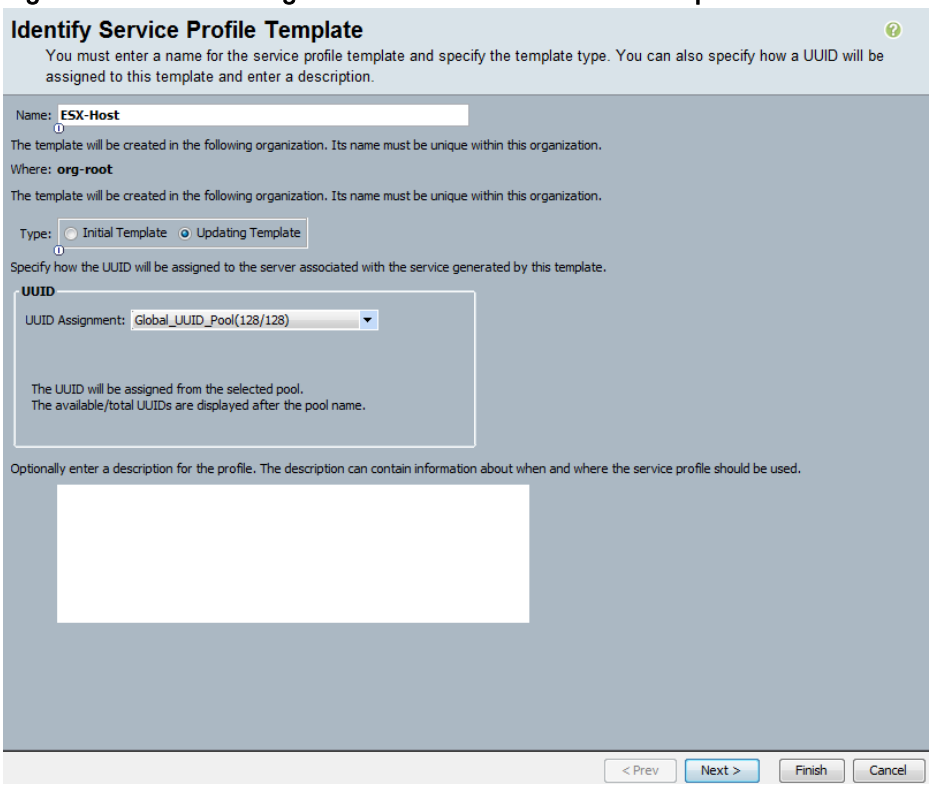
| Name | Variable |
|---|---|
| Name of the global UUID Pool | <<var_ucs_uuid_pool_name>> |
| Name of the LAN Connection Policy for ESX server | <<var_ucs_esx_lan_connect_policy_name>>. |
| Name of the SAN Connection Policy for ESX | <<var_ucs_esx_san_connect_policy_name>> |
| Name of the first vHBA in a Service Profile | <<var_ucs_vhba_1_name>> |
| Name of the second vHBA in a Service Profile | <<var_ucs_vhba_2_name>> |
| Name of the Boot Policy for SAN Boot | <<var_ucs_san_boot_policy>> |
| Name of the BIOS Policy for VMware ESX | <<var_ucs_esx_bios_policy_name>>. |
| Name of the IPMI Policy | <<var_ucs_ipmi_policy>> |
| Name of the Serial Over LAN Profile | <<var_ucs_sol_profile>> |

The Service Profile Template created for virtualized SAP HANA and other Applications which can be used for all Cisco UCS Managed B-Series and Cisco UCS C-Series servers with FC boot for VMware ESXi.

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the service profile template:
    a. Enter <<var_ucs_esx_template_name>> as the name of the service profile template.
    b. Select the Updating Template option.
    c. Under UUID, select <<var_ucs_uuid_pool_name>> as the UUID pool.
    d. Click Next.

Figure 280 UCS Manager – Create Service Profile Template




6. Configure the networking options:

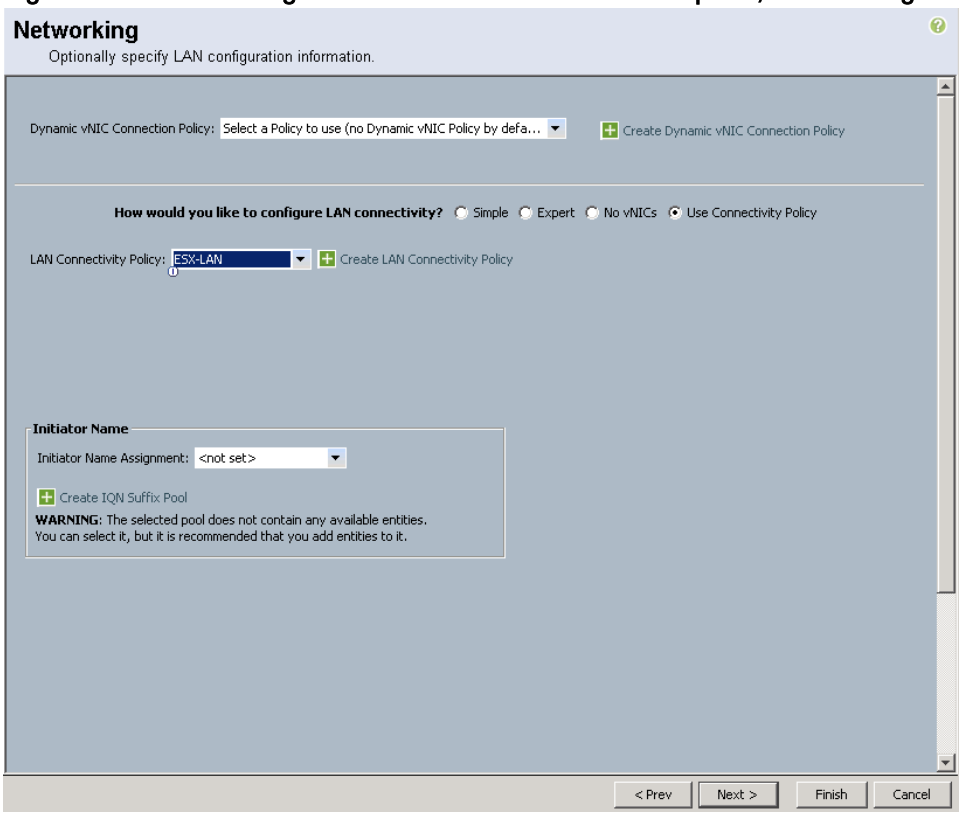
   a. Keep the default setting for Dynamic vNIC Connection Policy.

   b. Select the Use Connectivity Policy option to configure the LAN connectivity.

   c. In the LAN Connectivity Policy list, select <<var_ucs_esx_lan_connect_policy_name>>.

   d. Click Next.

**Figure 281 UCS Manager – Create Service Profile Template, Networking**




7. Configure the storage options:

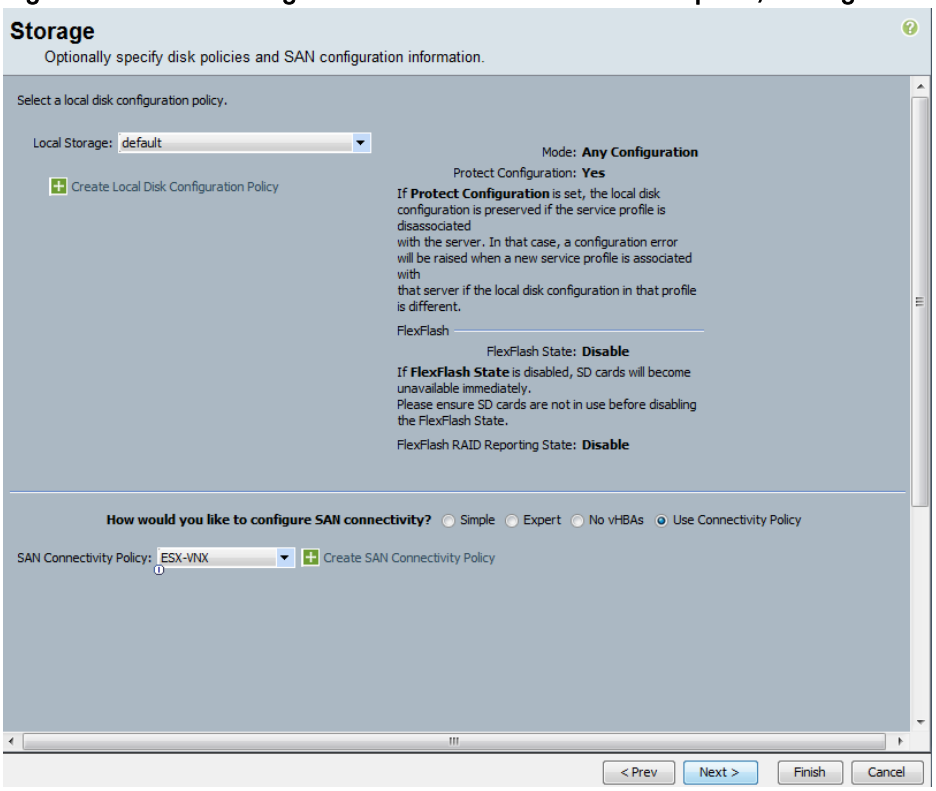
   a. In the Local Storage list, select default.

   b. Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.

   c. In the SAN Connectivity Policy list, select <<var_ucs_esx_san_connect_policy_name>>.

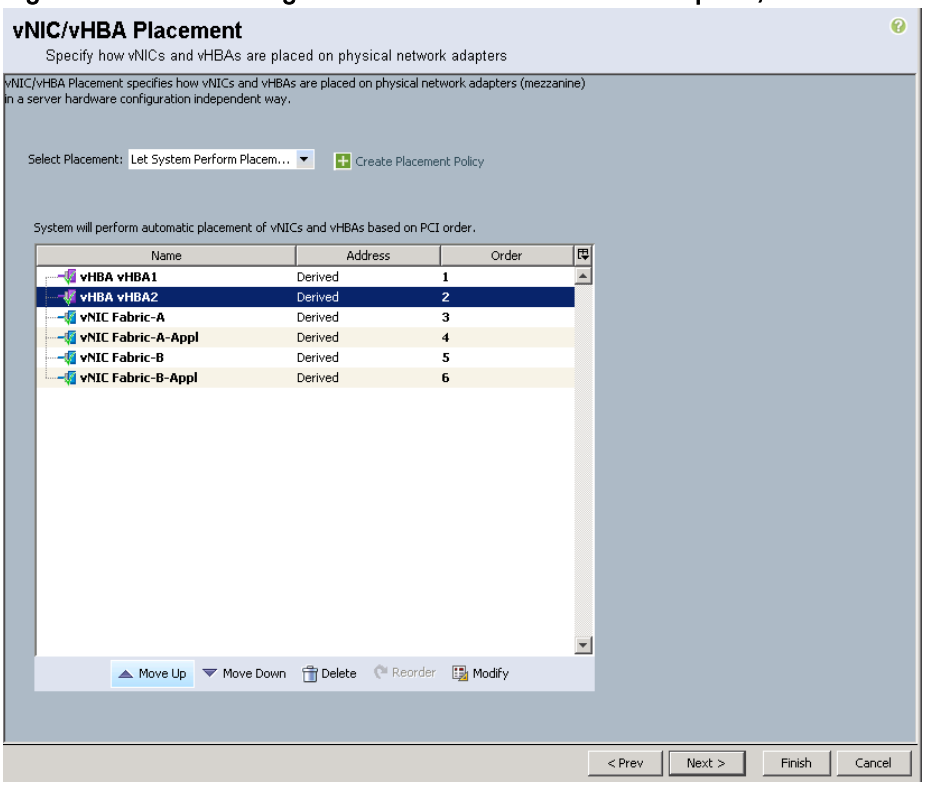
   d. Click Next.

Figure 282 UCS Manager – Create Service Profile Template, Storage



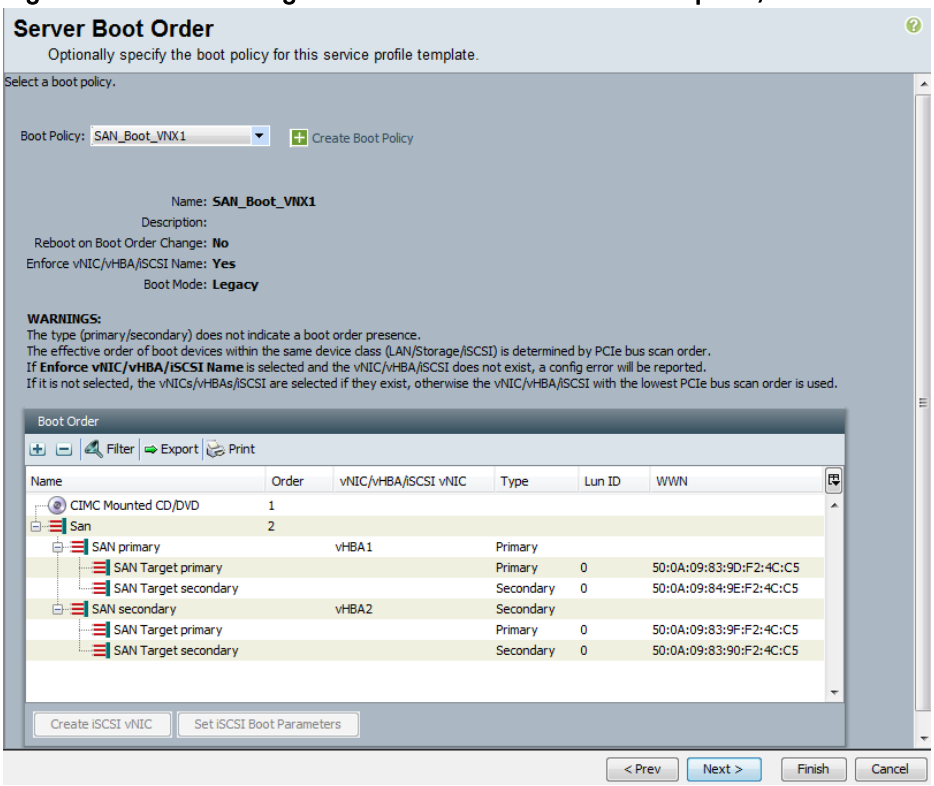

8. Set no Zoning options and click Next.
9. Set the vNIC/vHBA placement options:
   a. In the Select Placement list, select Let System Perform Placement.
   b. Move <<var_ucs_vhba_1_name>> and <<var_ucs_vhba_2_name>> as order 1 and 2.
   c. Click Next.

Figure 283 UCS Manager – Create Service Profile Template, vNIC/vHBA Placement




10. Click Next on vMedia Policy.
11. Set the server boot order:
    a. Select <<var_ucs_san_boot_policy>> for Boot Policy.
    b. In the Boot Order pane, check that the correct WWNs are listed.
    c. Click Next.

Figure 284 UCS Manager – Create Service Profile Template, Server Boot Order

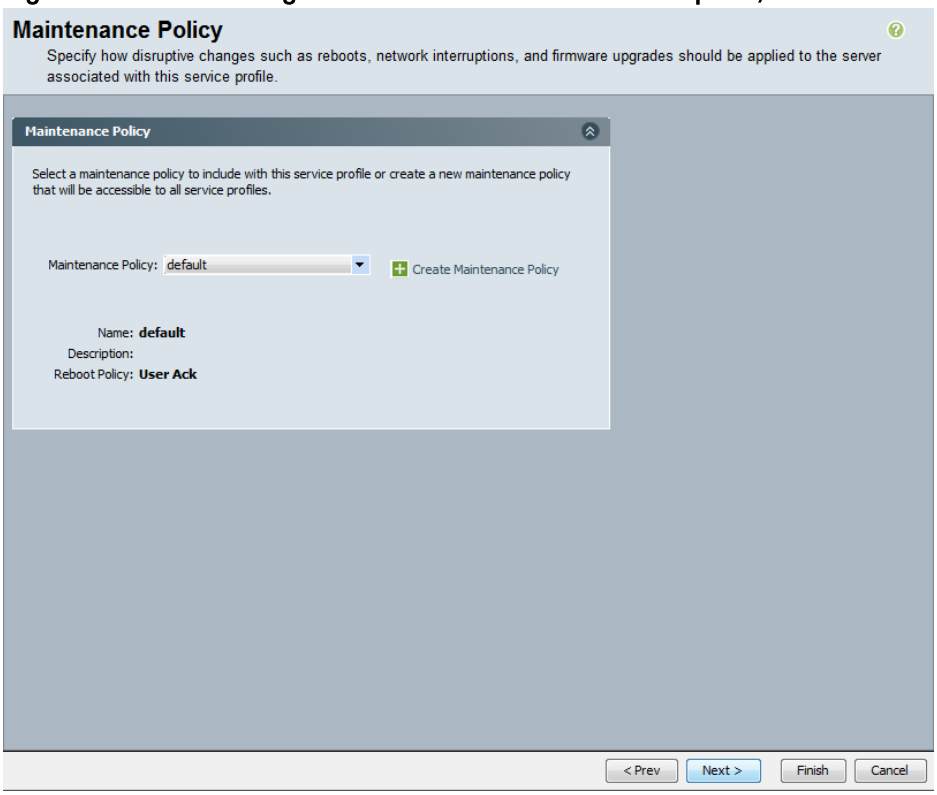



12. Add a maintenance policy:

    a. Select the default Maintenance Policy.

    b. Click Next.

Figure 285 UCS Manager – Create Service Profile Template, Maintenance Policy




13. Click Next on Server Assignment.

14. Add operational policies:

    a. In the BIOS Policy list, select <<var_ucs_esx_bios_policy_name>>.

    b. Expand External IPMI Management Configuration.

    c. Select <<var_ucs_ipmi_policy>> as the IPMI Access Profile.

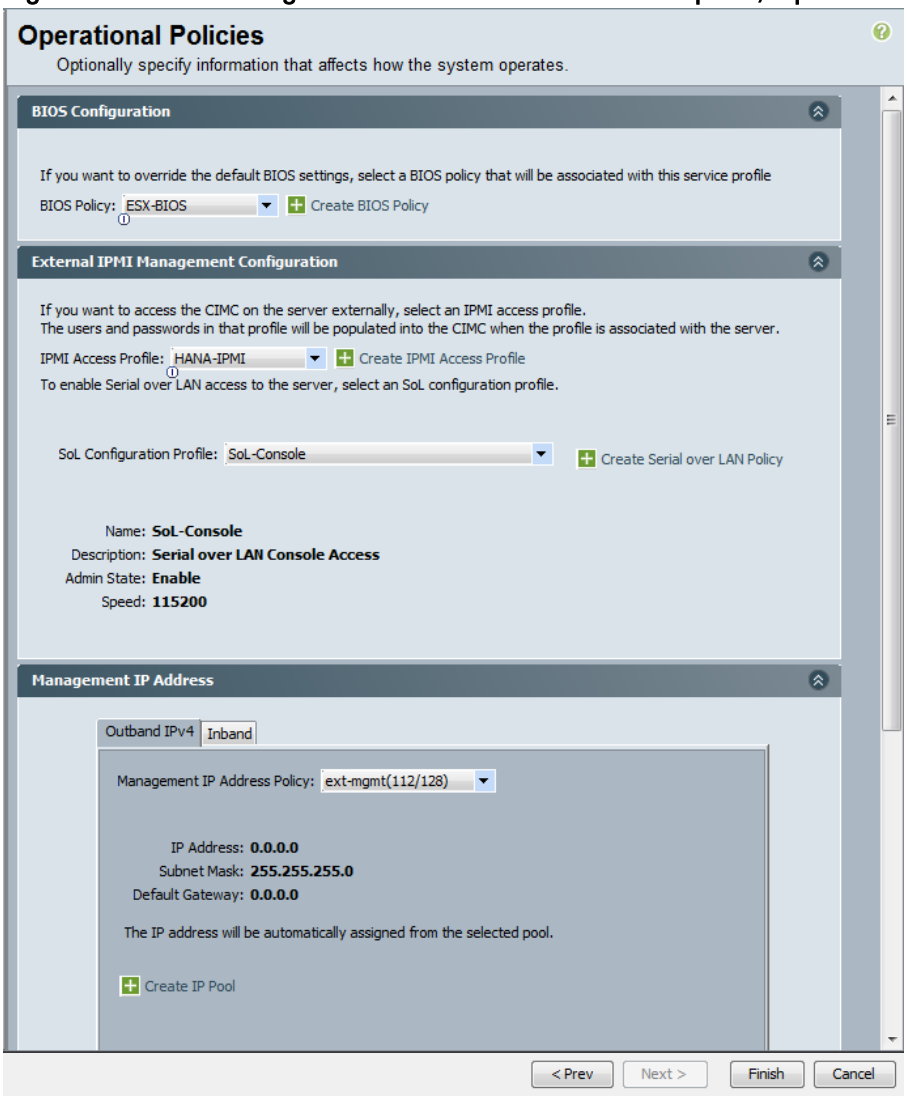
    d. Select <<var_ucs_sol_profile>> as the SoL Configuration Profile.

    e. Expand Management IP Address.

    f. Click Outband IPv4 tab.

    g. Select ext-mgmt as the Management IP Address Policy.

Figure 286 UCS Manager – Create Service Profile Template, Operational Policies




15. Click Finish to create the service profile template.

16. Click OK in the confirmation message.

## Instantiate Service Profiles for VMware ESX

With the created Service Profile Template, creating the Service Profiles for VMware ESX is a simple task.

Table 33 lists the required information to instantiate the Service Profiles for VMware ESX.

Table 33 Information to Setup Cisco UCS in the Reference Architecture

| Name | Variable |
|---|---|
| Name of the UCS Sub-Organization for ESX hosts | <<var_ucs_esx_sub-org>> |

| Name | Variable |
|---|---|
| Name of the Service Profile Template for Vmware ESX | <<var_ucs_esx_template_name>> |

To instantiate the service profiles, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organizations > <<var_ucs_esx_sub-org>>.
3. Click Create Service Profiles from Template to open the Create Service Profile wizard.
4. Enter ESX-Host as the Naming Prefix.
5. Enter 01 as the Name Suffix Starting Number.
6. Enter 10 as the Number of Instances.
7. Select Service Template <<var_ucs_esx_template_name>> as the Service Profile Template.
8. Click OK.
9. Click OK.

Figure 287 UCS Manager – Create Service Profiles From Template

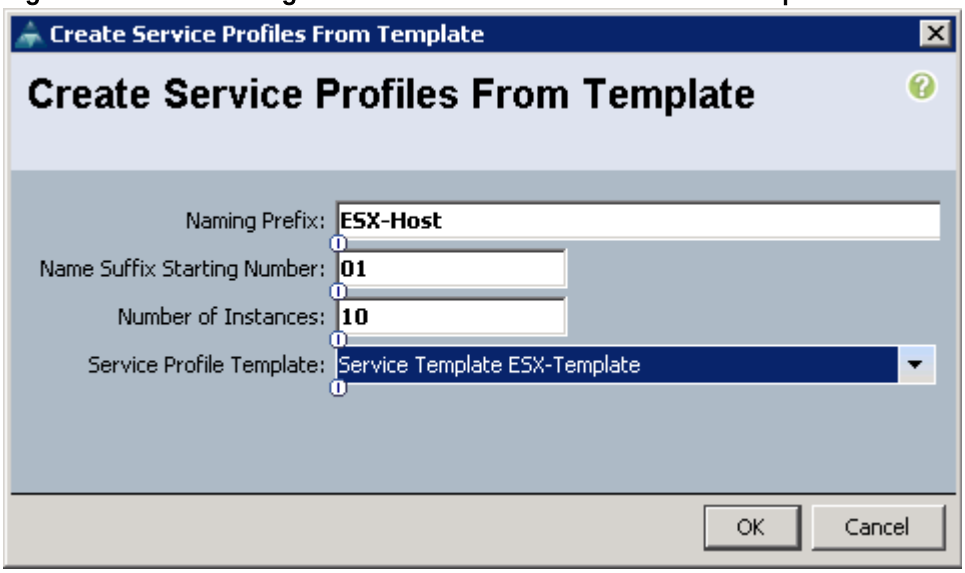
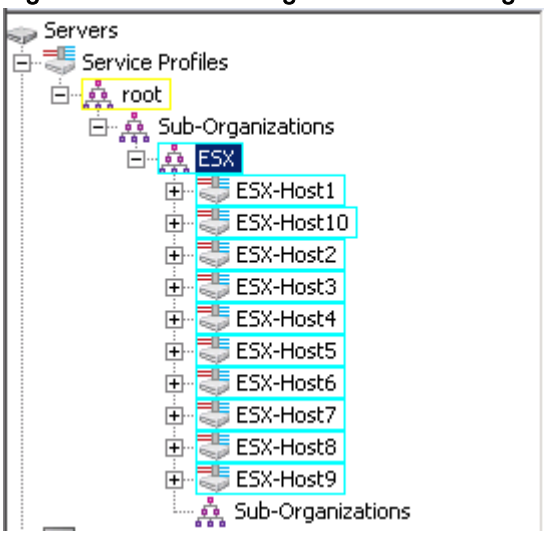


**Figure 288 UCS Manager – List of configured Service Profiles**



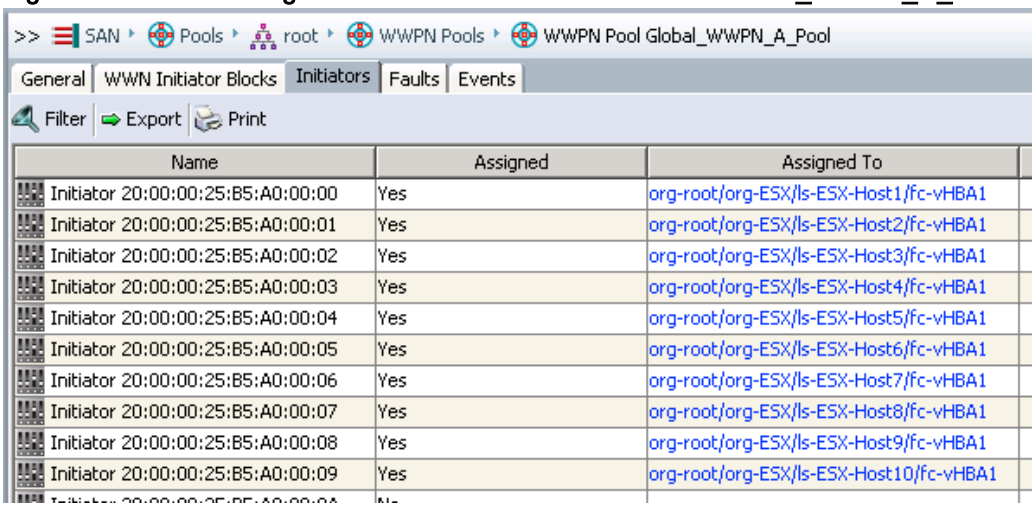

## Create SAN Zones on the MDS Switches

The first Service Profiles are defined. To access the EMC VNX storage, the zones on the Cisco MDS switches must be defined. Based on EMC support requirements, it is necessary to define a single initiator zoning. This means that in each zone there is only one HBA and multiple storages, and storage ports are allowed.

To configure the zones the used WWPNs must be known. To create the SAN zones, complete the following steps:

1. In Cisco UCS Manager, click SAN tab in the navigation pane.
2. Select Pools > root > WWPN Pools > WWPN Pool <<var_ucs_global_wwpn_a_pool_name>>.
3. In the right side click the Initiators tab.

**Figure 289 UCS Manager – List of used WWPNs in Pool Global_WWPN_A_Pool**

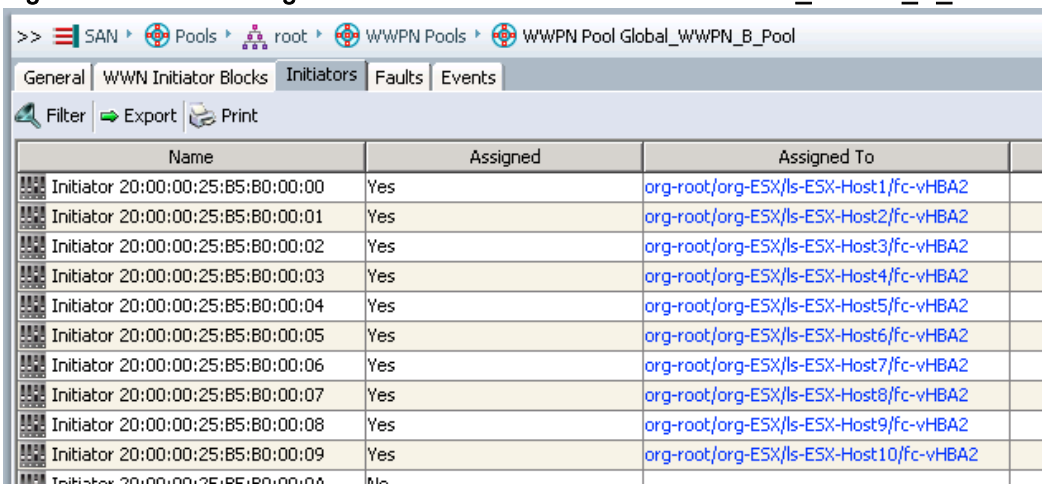



| Name | Assigned | Assigned To |
|---|---|---|
| Initiator 20:00:00:25:B5:A0:00:00 | Yes | org-root/org-ESX/ls-ESX-Host1/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:01 | Yes | org-root/org-ESX/ls-ESX-Host2/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:02 | Yes | org-root/org-ESX/ls-ESX-Host3/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:03 | Yes | org-root/org-ESX/ls-ESX-Host4/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:04 | Yes | org-root/org-ESX/ls-ESX-Host5/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:05 | Yes | org-root/org-ESX/ls-ESX-Host6/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:06 | Yes | org-root/org-ESX/ls-ESX-Host7/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:07 | Yes | org-root/org-ESX/ls-ESX-Host8/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:08 | Yes | org-root/org-ESX/ls-ESX-Host9/fc-vHBA1 |
| Initiator 20:00:00:25:B5:A0:00:09 | Yes | org-root/org-ESX/ls-ESX-Host10/fc-vHBA1 |

4. Select Pools > root > WWPN Pools > WWPN Pool <<var_ucs_global_wwpn_b_pool_name>>.

5. In the right side click the Initiators tab.

**Figure 290 UCS Manager – List of used WWPNs in Pool Global_WWPN_B_Pool**




| Name | Assigned | Assigned To |
|---|---|---|
| Initiator 20:00:00:25:B5:B0:00:00 | Yes | org-root/org-ESX/ls-ESX-Host1/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:01 | Yes | org-root/org-ESX/ls-ESX-Host2/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:02 | Yes | org-root/org-ESX/ls-ESX-Host3/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:03 | Yes | org-root/org-ESX/ls-ESX-Host4/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:04 | Yes | org-root/org-ESX/ls-ESX-Host5/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:05 | Yes | org-root/org-ESX/ls-ESX-Host6/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:06 | Yes | org-root/org-ESX/ls-ESX-Host7/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:07 | Yes | org-root/org-ESX/ls-ESX-Host8/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:08 | Yes | org-root/org-ESX/ls-ESX-Host9/fc-vHBA2 |
| Initiator 20:00:00:25:B5:B0:00:09 | Yes | org-root/org-ESX/ls-ESX-Host10/fc-vHBA2 |

## Cisco MDS 9148 A

Use the following commands to verify the systems are logged into the switch:

```
CRA-EMC-A# show flogi data

--------------------------------------------------------------------------------

INTERFACE        VSAN    FCID           PORT NAME               NODE NAME

--------------------------------------------------------------------------------

fc1/25           10     0xb40700  50:06:01:60:36:60:17:b4 50:06:01:60:b6:60:17:b4

fc1/26           10     0xb40000  50:06:01:68:36:60:17:b4 50:06:01:60:b6:60:17:b4
```

```
fc1/27           10    0xb40100  50:06:01:61:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/28           10    0xb40200  50:06:01:69:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/29           10    0xb40300  50:06:01:62:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/30           10    0xb40400  50:06:01:6a:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/31           10    0xb40500  50:06:01:63:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/32           10    0xb40600  50:06:01:6b:36:60:17:b4 50:06:01:60:b6:60:17:b4
port-channel110  10    0xb41000  24:6e:00:2a:6a:03:bc:40 20:0a:00:2a:6a:03:bc:41
port-channel110  10    0xb41001  20:00:00:25:b5:a0:00:00 20:00:00:25:b5:33:00:00
port-channel110  10    0xb41002  20:00:00:25:b5:a0:00:01 20:00:00:25:b5:33:00:01

Total number of flogi = 11.
```

Make sure the WWPNs match with the WWPNs from Cisco UCS Manager: <<var_global_wwpn_a_pool>>.

On MDS 9148 A enter configuration mode:

```
config terminal
```

Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path zone_esx-host1 vsan 10
zone name zone_esx-host1 vsan 10
   member pwwn 20:00:00:25:b5:a0:00:00
   exit

zoneset name CRA-EMC-A vsan 10
member zone_esx-host1
exit
```

Repeat these steps for all defined ESX-Hosts and activate the updated zoneset:

```
zoneset activate name CRA-EMC-A vsan 10
```

Verify the configuration with the following commands:

```
CRA-EMC-A# show zone
```

```
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_esx-host1 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:00

zone name zone_esx-host2 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:01

zone name zone_esx-host3 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:02

zone name zone_esx-host4 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:03

zone name zone_esx-host5 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
```

```
  pwwn 20:00:00:25:b5:a0:00:04

zone name zone_esx-host6 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:05

zone name zone_esx-host7 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:06

zone name zone_esx-host8 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:07

zone name zone_esx-host9 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:08

zone name zone_esx-host10 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:09
CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
```

```
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
CRA-EMC#
```

## Cisco MDS 9148 B

Use the following commands to verify the systems logged into the switch:

```
CRA-EMC-B# show flogi data
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/25           20    0x4a0200  50:06:01:64:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/26           20    0x4a0300  50:06:01:6c:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/27           20    0x4a0400  50:06:01:65:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/28           20    0x4a0500  50:06:01:6d:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/29           20    0x4a0600  50:06:01:66:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/30           20    0x4a0700  50:06:01:6e:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/31           20    0x4a0800  50:06:01:67:36:60:17:b4 50:06:01:60:b6:60:17:b4
fc1/32           20    0x4a0900  50:06:01:6f:36:60:17:b4 50:06:01:60:b6:60:17:b4
port-channel120  20    0x4a1000  24:78:00:2a:6a:03:ee:c0 20:14:00:2a:6a:03:ee:c1
port-channel120  20    0x4a1001  20:00:00:25:b5:b0:00:00 20:00:00:25:b5:33:00:00
port-channel120  20    0x4a1002  20:00:00:25:b5:b0:00:01 20:00:00:25:b5:33:00:01

Total number of flogi = 11.
```

Make sure the WWPNs match with the WWPNs from Cisco UCS Manager <<var_global_wwpn_b_pool>>.

On MDS 9148 B enter configuration mode:

```
config terminal
```

Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path zone_esx-host1 vsan 20
```

```
zone name zone_esx-host1 vsan 20
   member pwwn 20:00:00:25:b5:b0:00:00
   exit

zoneset name CRA-EMC-B vsan 20
member zone_esx-host1
exit
```

Repeat these steps for all defined ESX-Hosts and activate the updated zoneset.

```
zoneset activate name CRA-EMC-B vsan 20
```

Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_temp_1path vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host1 vsan 20
  pwwn 20:00:00:25:b5:b0:00:00
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
```

```
zone name zone_esx-host2 vsan 20
  pwwn 20:00:00:25:b5:b0:00:01
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host3 vsan 20
  pwwn 20:00:00:25:b5:b0:00:02
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host4 vsan 20
  pwwn 20:00:00:25:b5:b0:00:03
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host5 vsan 20
  pwwn 20:00:00:25:b5:b0:00:04
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host6 vsan 20
  pwwn 20:00:00:25:b5:b0:00:05
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host7 vsan 20
  pwwn 20:00:00:25:b5:b0:00:06
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host8 vsan 20
  pwwn 20:00:00:25:b5:b0:00:07
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78

zone name zone_esx-host9 vsan 20
  pwwn 20:00:00:25:b5:b0:00:08
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
```

```
zone name zone_esx-host10 vsan 20
  pwwn 20:00:00:25:b5:b0:00:09
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
CRA-EMC-B#
```

## EMC VNX Storage Configuration



The basic installation and configuration of the EMC VNX storage is done by the EMC service technician at delivery time. Make sure to provide this CVD to the service technician.

### Initial Storage Setup

Initial setup of the base VNX is done using the VNX Installation Assistant for File/Unified (VIA). Initial setup of the expansion arrays (block only) is performed using the Unisphere Storage System Initialization Wizard. Additionally Unisphere CLI is required. Both tools are available for download from the tools section on EMC's Online Support Website https://support.emc.com/.



These tools are only available to EMC personnel and EMC's Authorized Service Providers. The initialization wizards are in the latest toolkit and Unisphere CLI is separate.

Refer to EMC's documentation "Getting Started with VNX Installation Assistant for File/Unified" and "EMC VNX VNX[5400|8000] Block Installation Guide" for more detailed information.

With VIA, the IP addresses of the EMC VNX Control Station as well as the storage processors will be specified for just the Base array. Please note that the IP addresses must be in the IP range of the management network and each EMC VNX array within a multi-array solution must have its own dedicated IP addresses as per Table 34 .

Table 34 lists the required information for VIA to setup the EMC VNX arrays in this Cisco UCS Integrated Infrastructure for SAP HANA with EMC VNX Storage.

**Table 34 Information to Setup EMC VNX**

| Name | Variable |
|---|---|
| Name of the first VNX in the Solution | <<var_vnx1_name>> |
| IP Address of the Control Station | <<var_vnx1_cs1_ip>> |
| Hostname of the Control Station | <<var_vnx1_cs1_hostname>> |
| IP Address of the Storage Processor A | <<var_vnx1_spa_ip>> |
| Hostname of the Storage Processor A** | <<var_vnx1_spa_hostname>> |
| IP Address of the Storage Processor B | <<var_vnx1_spb_ip>> |
| Hostname of the Storage Processor B** | <<var_vnx1_spb_hostname>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| DNS domain name | <<var_mgmt_dns_domain_name>> |
| Global default administrative password | <<var_mgmt_passwd>> |

** Setting up the SP hostnames is not part of the VIA process. The hostnames can be specified later within the Unisphere GUI.

In order to run VIA and the Unisphere Storage System Initialization Wizard, a service laptop running Windows needs to be connected to the management LAN.

When the VIA configuration process has completed, it cannot be run again.

0 through Figure 299 show the VIA pre-configuration setup procedure. Use the passwords specified in the worksheet in the pre-installation section of this document.

Figure 291 VIA Setup the Control Station for Accessing the Network

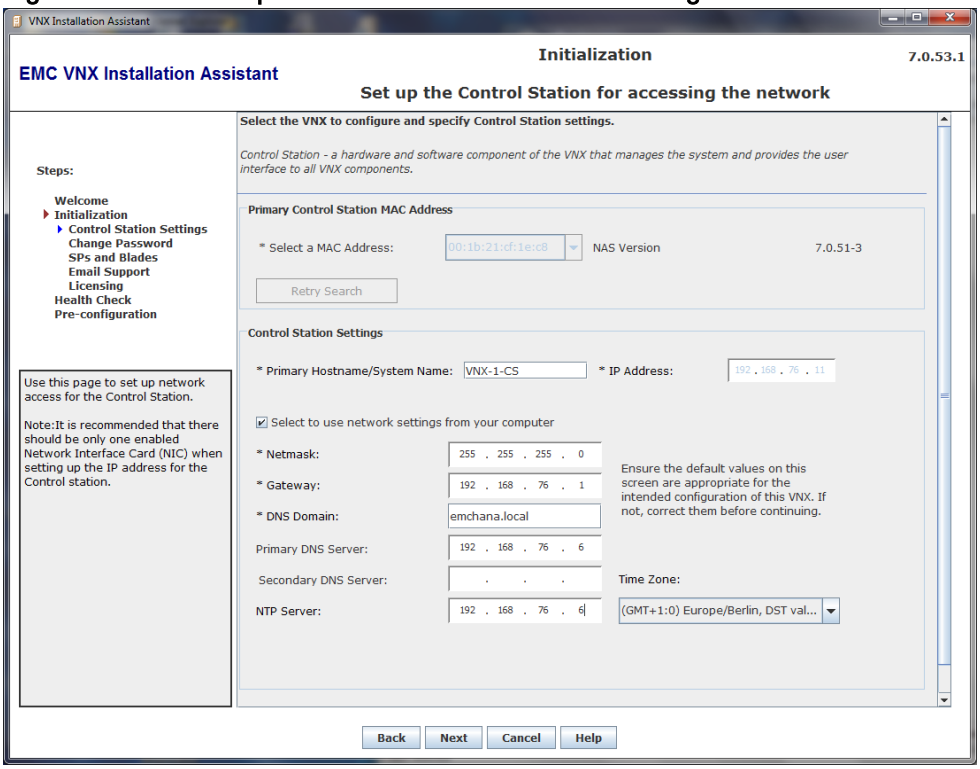



Figure 292 VIA Change the Default Passwords

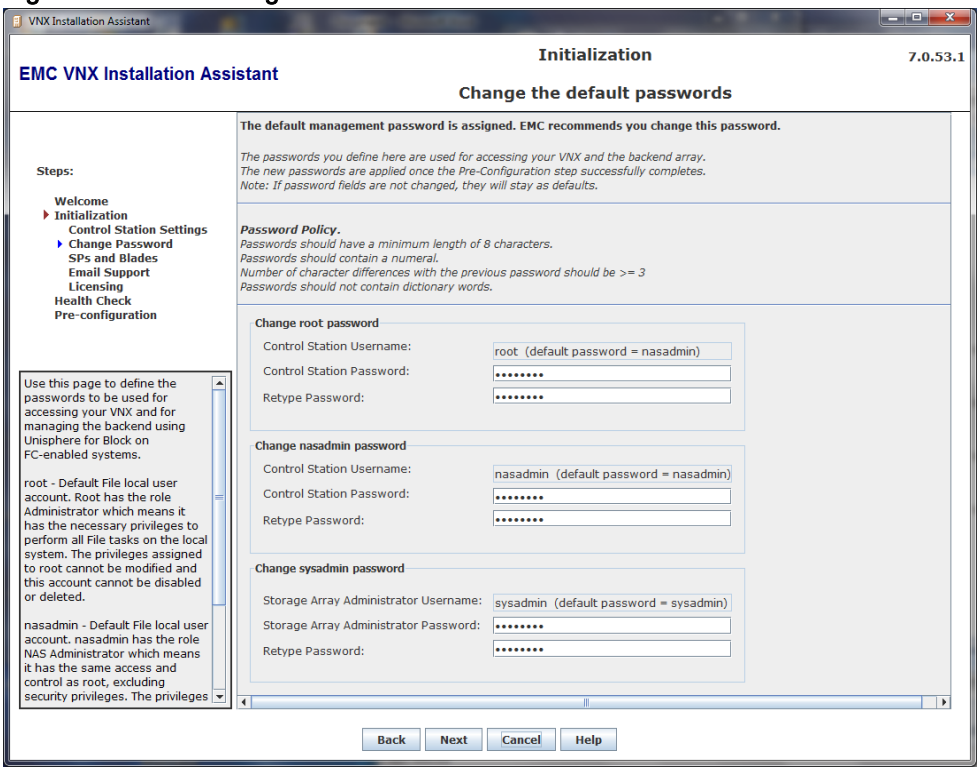


Figure 293 VIA Setting up the Blades and Storage Processors

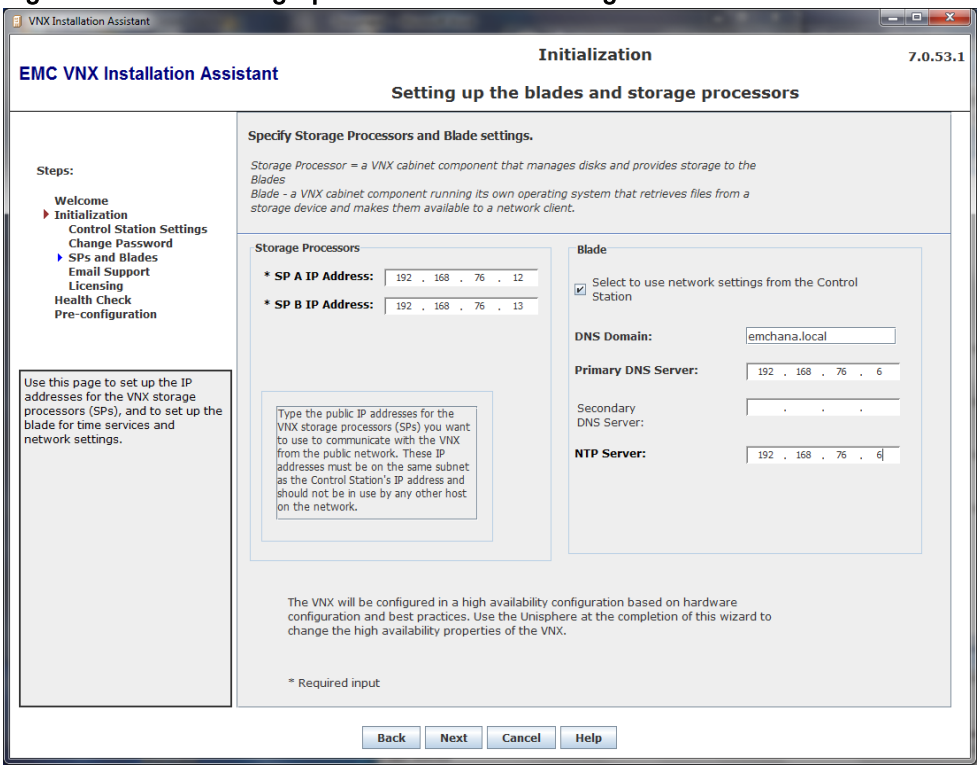



Figure 294 Configuring Email Support and Customer Information

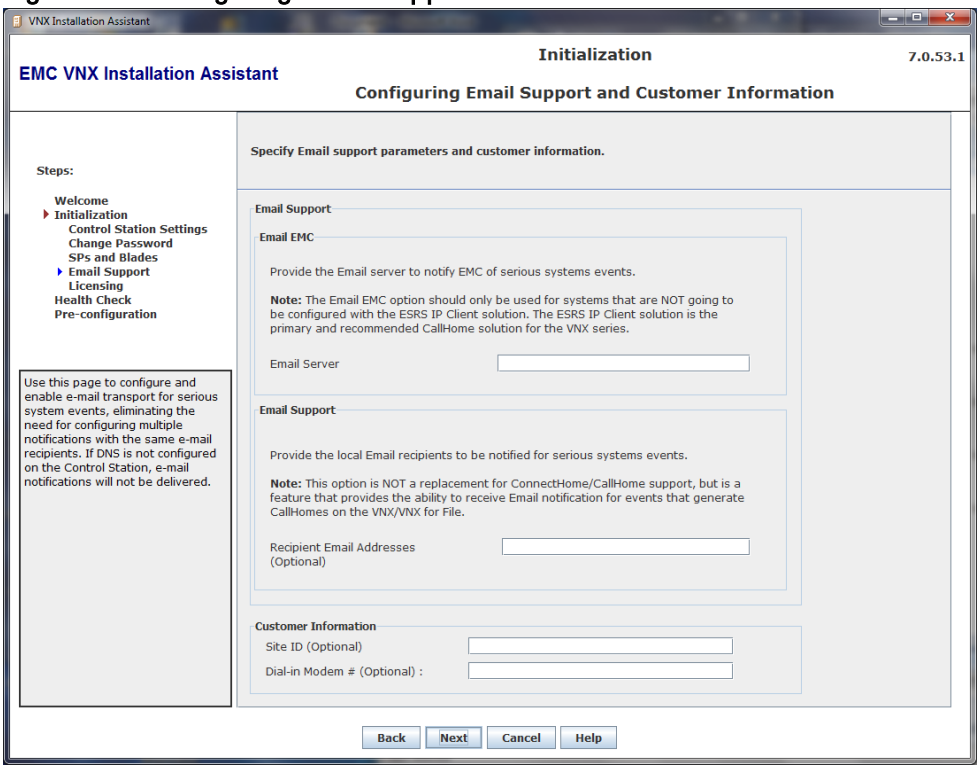


Figure 295 VIA Collecting License Information

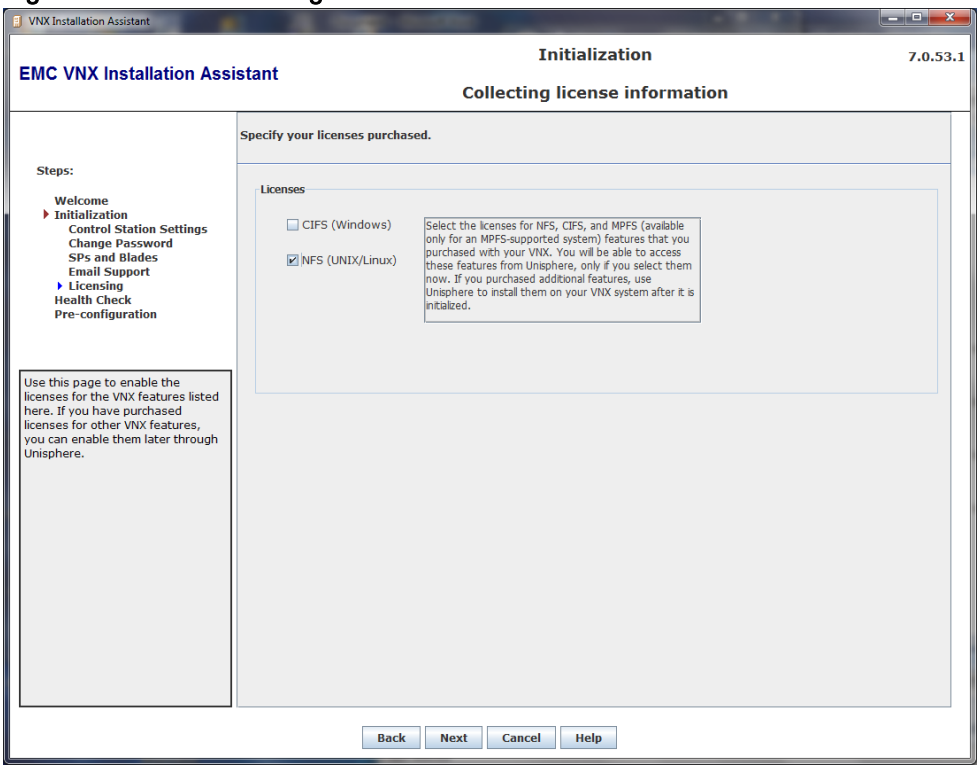



Figure 296 VIA Health Check

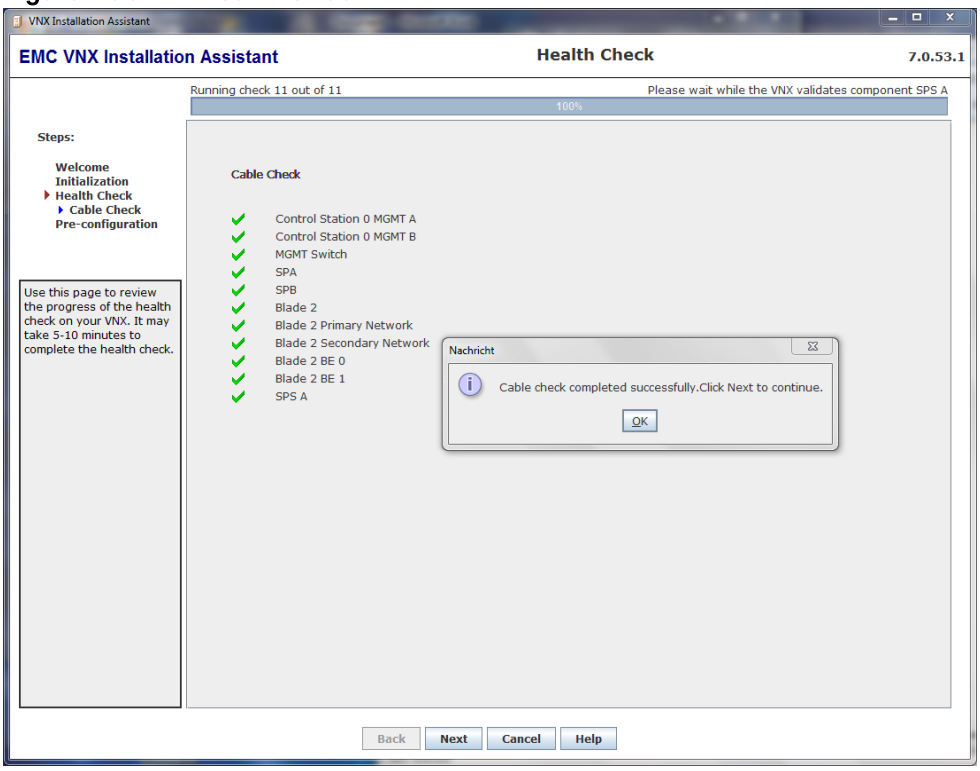


Figure 297 VIA Pre-configuration

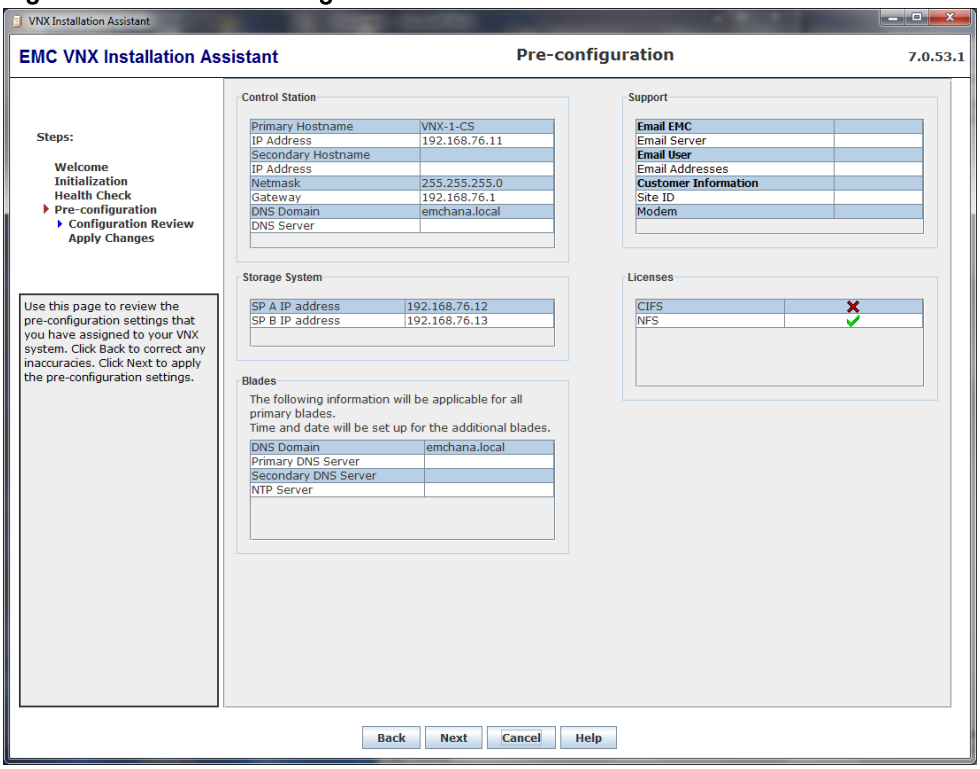



Figure 298 VIA Applying the Specified Configuration Changes

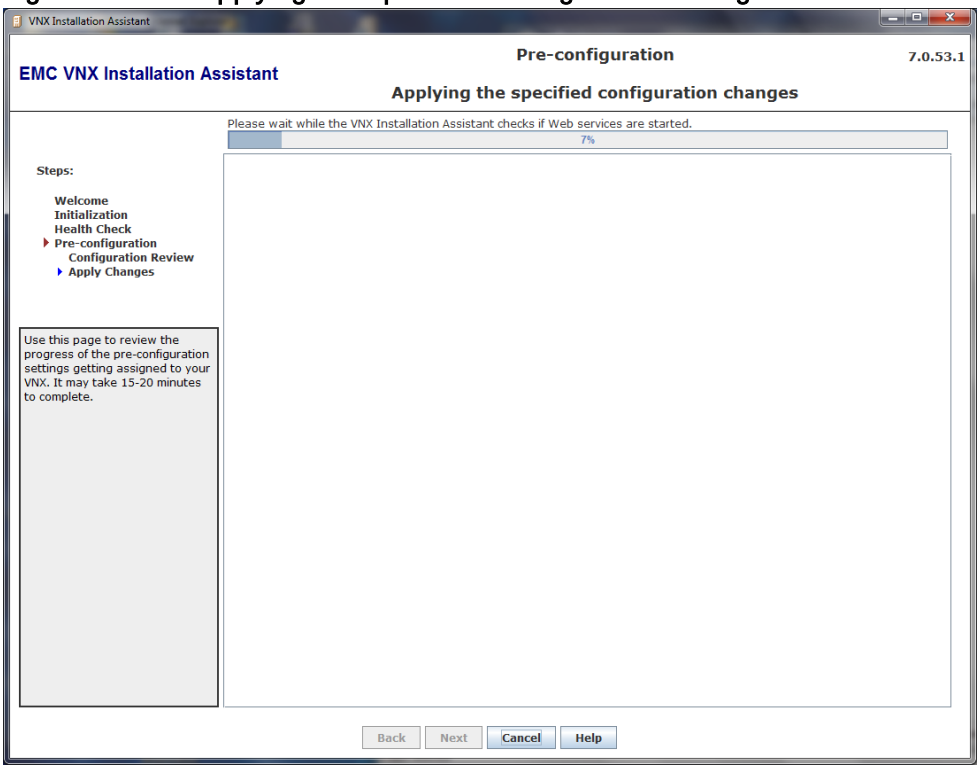
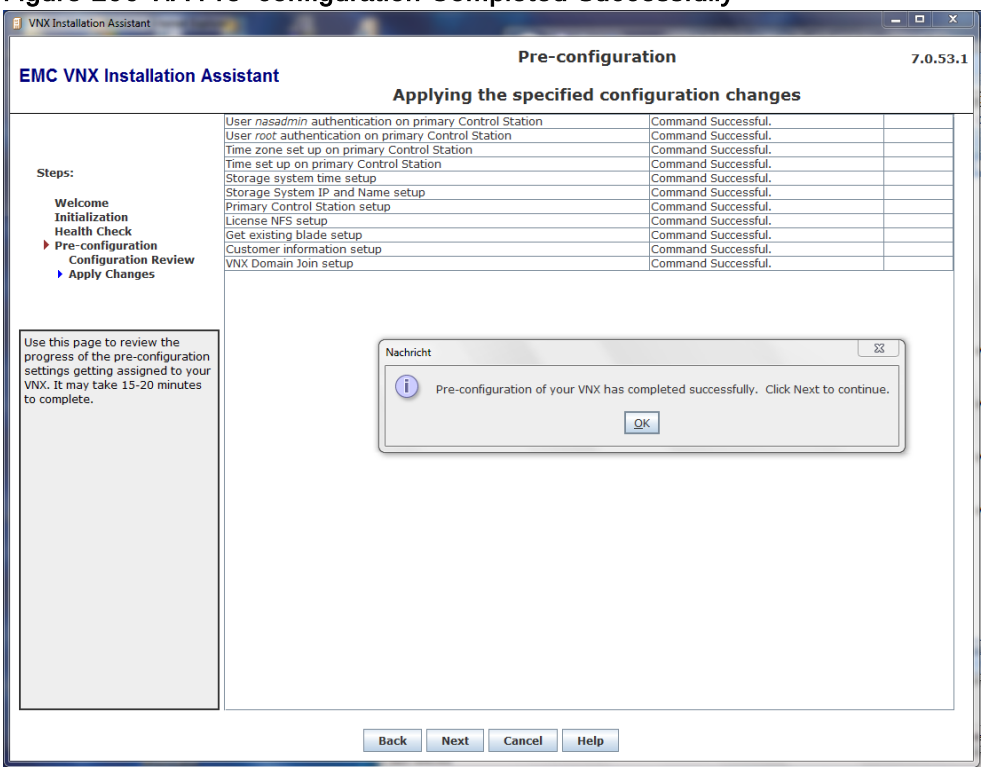


Figure 299 VIA Pre-configuration Completed Successfully




VIA does not work for block-only arrays. These arrays must be initialized using the Unisphere Storage System Initialization Wizard. Refer to the EMC documentation “EMC VNX Block Installation Guide” for information about how to download and run this tool.

The Storage is now manageable through EMC Unisphere over the network.

## Configure Storage Pool for Operating Systems and Non-SAP HANA Applications

Table 34 lists the required information to setup the EMC VNX arrays in this Cisco UCS Integrated Infrastructure for SAP HANA with EMC VNX Storage.

Table 35 Information to configure the EMC VNX

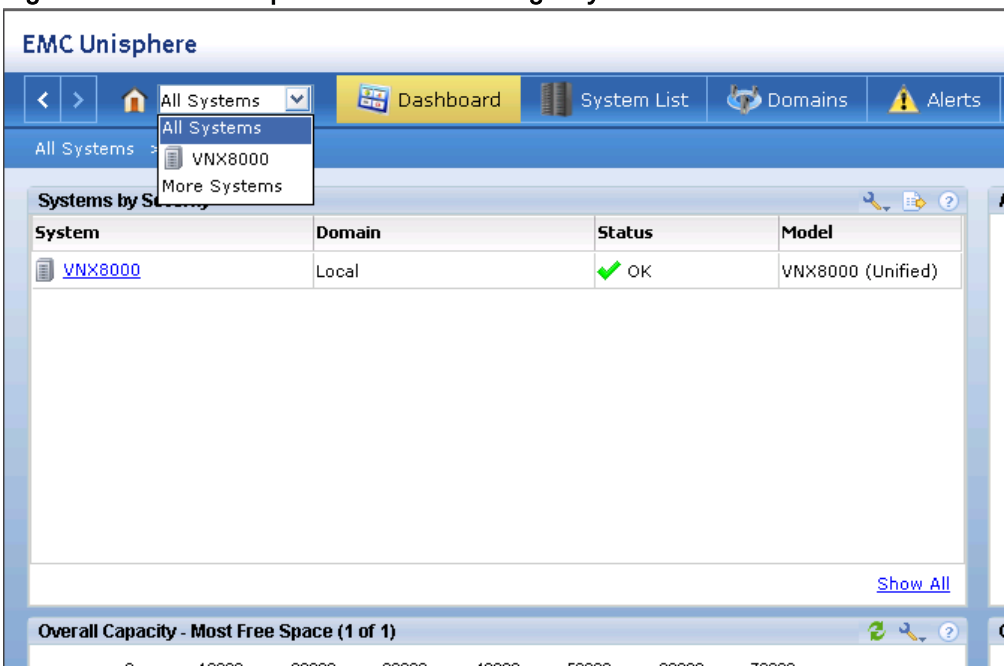
| Name | Variable |
|---|---|
| Name of the first VNX in the Solution | <<var_vnx1_name>> |
| Name of the first Storage pool on VNX1 - for Non-HANA usage | <<var_vnx1_pool1_name>> |
| Name of the Global World Wide Port Name Pool on Fabric A | <<var_ucs_global_wwpn_a_pool_name>> |
| Name of the first Storage pool for File on VNX1 - | <<var_vnx1_fs-pool1_name>> |

| Name | Variable |
|---|---|
| for Non-HANA usage | |
| NTP server IP address | <<var_global_ntp_server_ip>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| DNS server 2 IP Address | <<var_nameserver2_ip>> |
| Name of the LACP Device for NFS traffic | <<var_vnx1_lacp_dev_name>> |
| IP Address of Datamover2 on the NFS Network | <<var_vnx1_dm2_nfs_ip>> |
| Netmask of the NFS network | <<var_nfs_netmask>> |
| VMware ESX Storage access Network VLAN ID | <<var_esx_nfs_vlan_id>> |
| Name of the first File System on VNX1 | <<var_vnx1_fs1_name>> |
| Size of the Filesystem in Megabyte | <<var_vnx1_fs1_size>> |
| Global default administrative password | <<var_mgmt_passwd>> |
| Name of the CIFS Workgroup if required | <<var_vnx1_cifs_workgroup>> |
| NetBIOS Name of VNX1 | <<var_vnx1_netbios_name>> |
| Name of the CIFS share for File System 1 | <<var_vnx1_cifs_share1_name>> |
| IP Address of Datamover2 on the Management Network | <<var_vnx1_dm2_mgmt_ip>> |
| Name of the Interface for the Management Network | <<var_vnx1_dm2_mgmt_name>> |
| Name of the NFS share for the first File System | <<var_vnx1_nfs1_name>> |

To create storage pools and carve boot LUNs on a per server basis, complete the following steps:

1. Open a Web Browser and connect to EMC VNX Unisphere.
2. From the Drop-down Menu select the VNX <<var_vnx1_name>>.

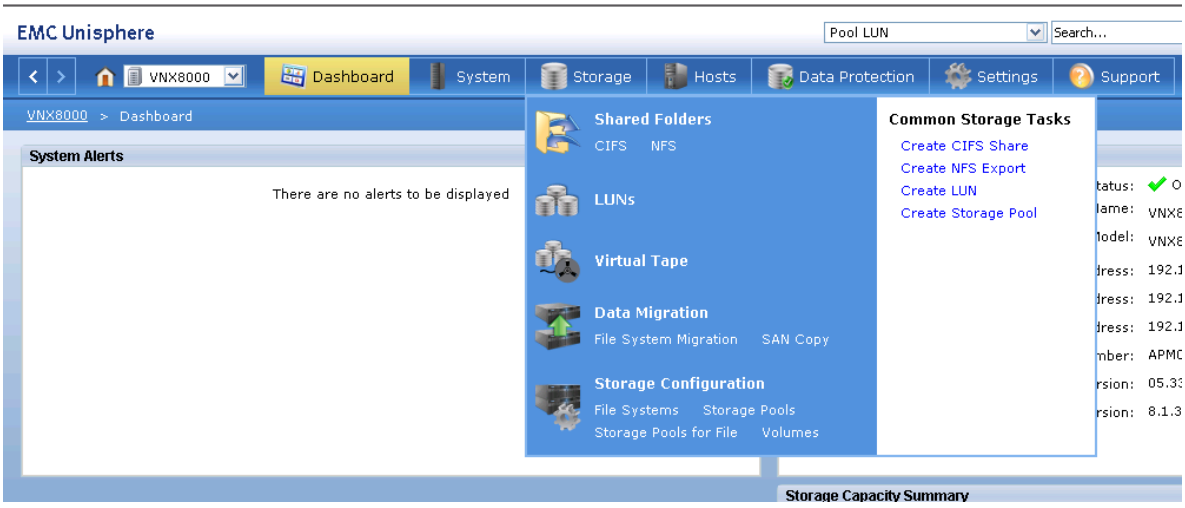
Figure 300 EMC Unisphere – Select Storage System




3. Click the Storage tab on the top.

4. Select Storage Configuration > Storage Pools.

Figure 301 EMC Unisphere – Storage Pools



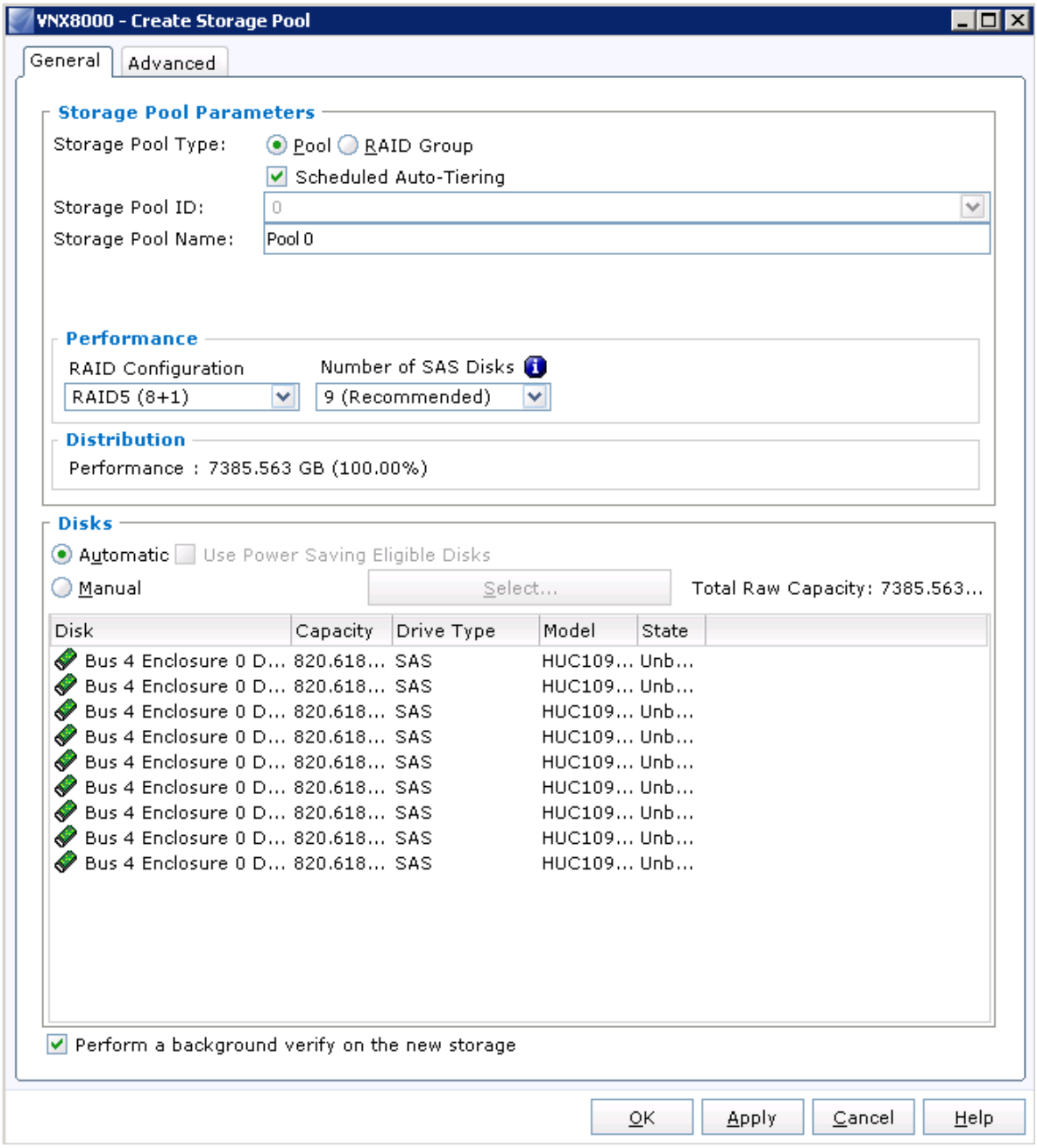

5. Click Create.

6. Keep Pool selected as the Storage Pool Type.

7. Enter <<var_vnx1_pool1_name>> as the Storage Pool Name.

8. Choose RAID5 (8 + 1) as the RAID Configuration.
9. Choose 9 (Recommended) as the Number of SAS Disks.
10. In the Disks Section keep Automatic selected, the Configuration wizard will select 9 SAS disks to create the storage pool.
11. Click OK.
12. Click Yes to Initiate the Pool creation.

Figure 302 EMC Unisphere – Create Storage Pool




13. Click Yes to accept the Auto-Tiering Warning.

14. Click OK.

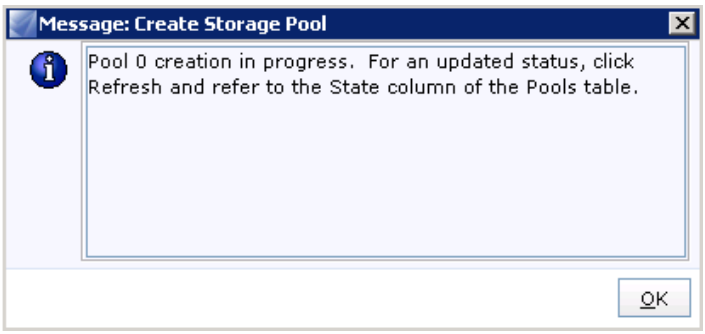
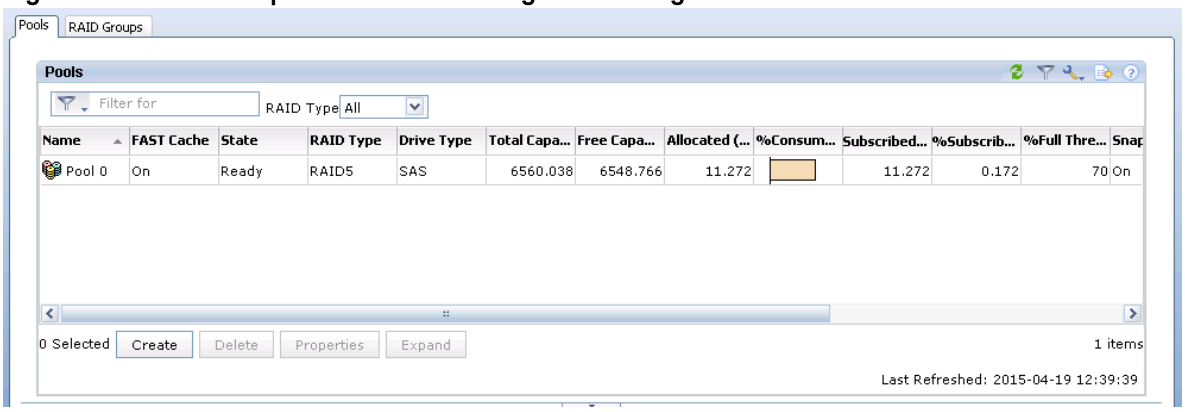



**Figure 303 EMC Unisphere – List of configured Storage Pools**



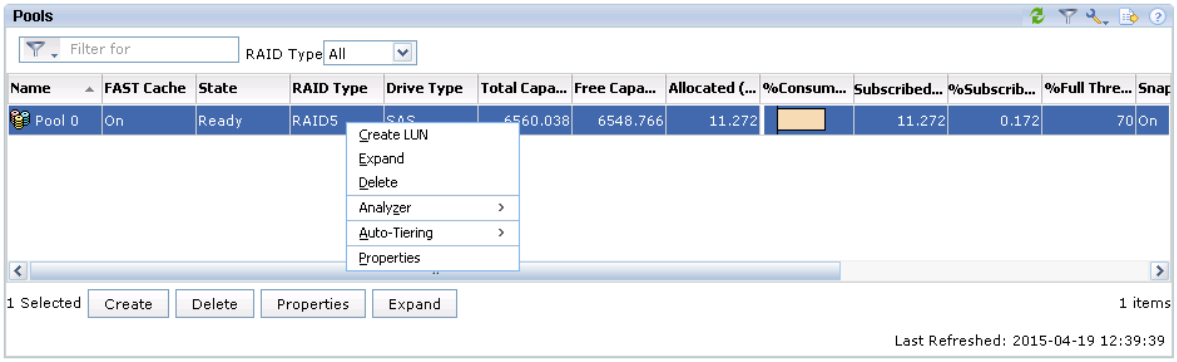

## Configure LUNs for VMware ESX Hosts

The VMware ESX hosts in the Cisco UCS Integrated Infrastructure booting through SAN from the VNX storage. ESX host one LUN to host the hypervisor OS is required. In step 10, LUNs are created to boot 10 ESX hosts.

To configure LUNs for VMware ESX Hosts, complete the following steps:

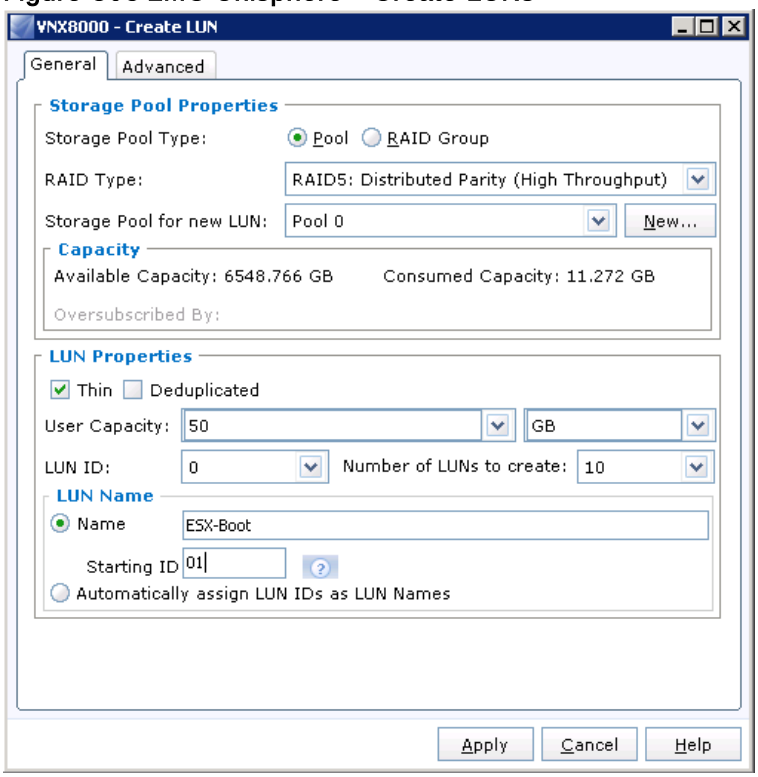
1. Right-Click the created Storage Pool.
2. Click Create LUN.

**Figure 304 EMC Unisphere – Storage Pool Action Menu**



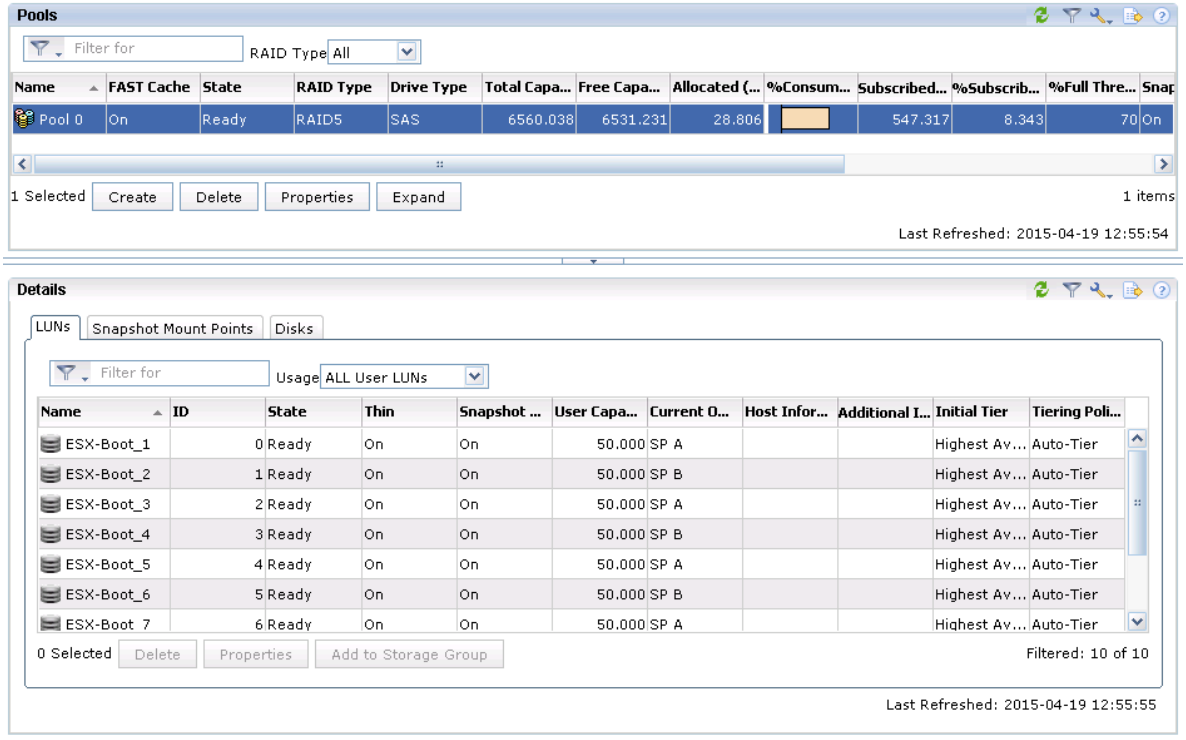
3. Review the Storage Pool Properties.
4. In the LUN Properties Section  Keep the Check-Box for Thin selected.
5. Enter 50 as the User Capacity and select GB as the unit.
6. Enter 10 as the Number of LUNs to create.
7. Click the Radio-Button left of Name.
8. Enter ESX-Boot in the Name field.
9. Enter 01 as the Starting ID.
10. Click Apply.

**Figure 305 EMC Unisphere – Create LUNs**



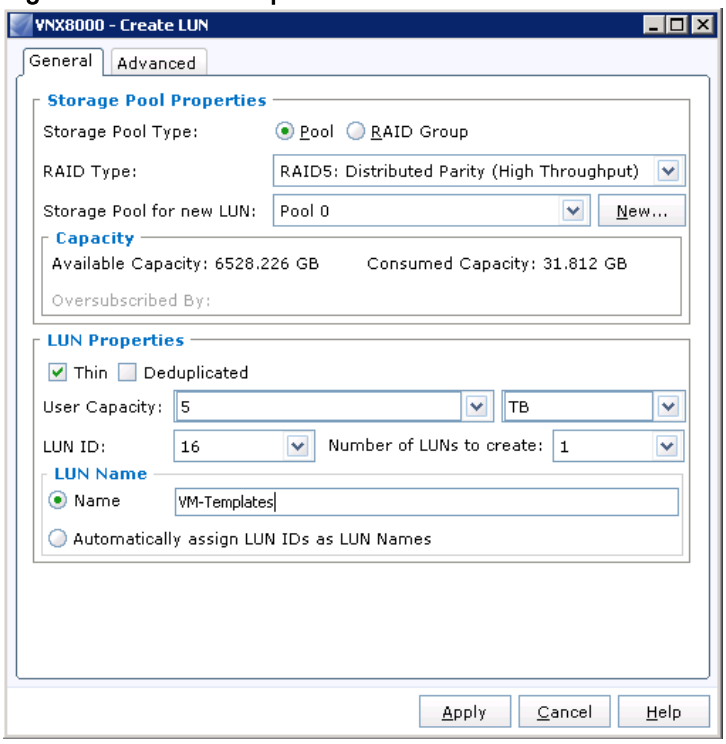

11. Click Yes.
12. Click OK.
13. Click Cancel.

Figure 306 EMC Unisphere – List of configured LUNs for a Storage Pool




14. Right-Click the created Storage Pool.
15. Click Create LUN.
16. For the User Capacity, enter 5 and select TB from the drop-down menu.
17. Select the Radio-Button for Name.
18. Enter VM-Templates as the Name.
19. Click Apply.
20. Click Yes.
21. Click OK.
22. Click Cancel.

Figure 307 EMC Unisphere – Create LUN



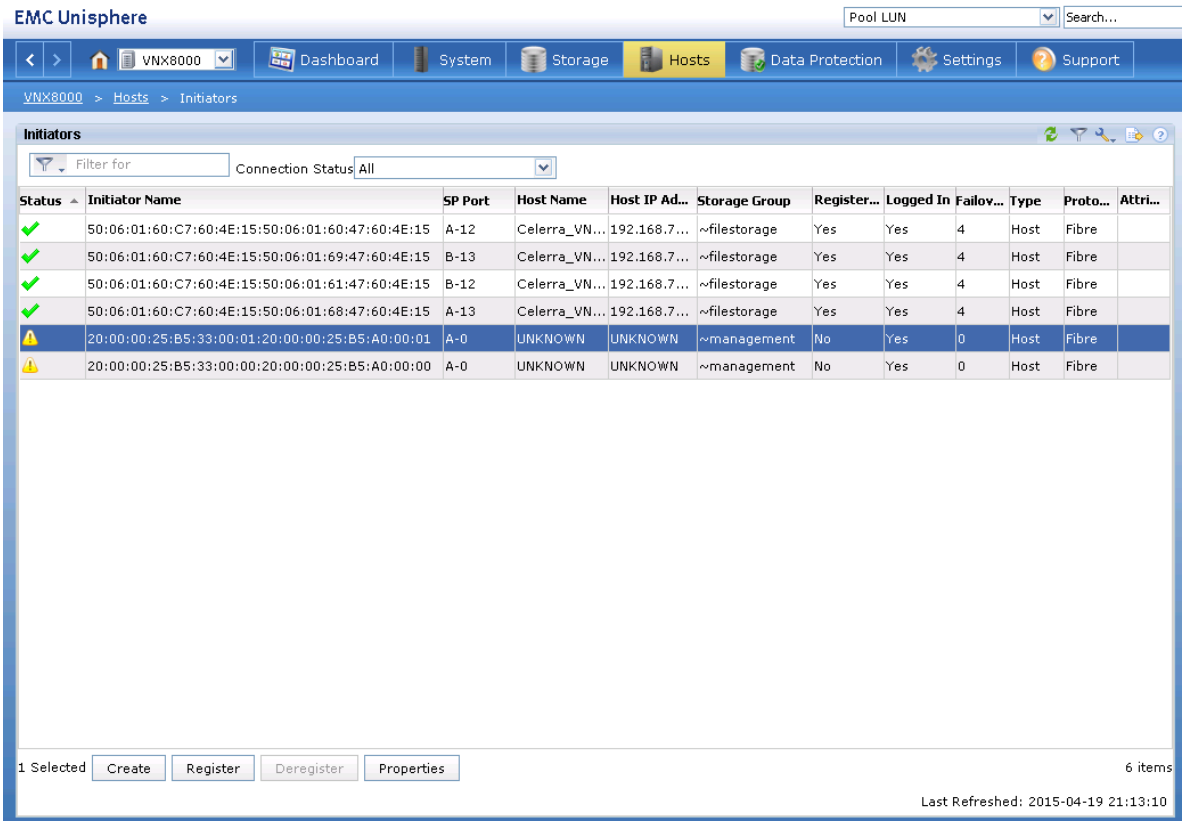

## Register Hosts and Configure Storage Groups

### Register Hosts

When the service profiles are associated in Cisco UCS Manager, the vHBAs will perform a fibre channel login (flogi) in the network and the SAN initiators are identified by the VNX storage array. To register the hosts identified by the WWPN of the server, complete the following steps:

1. On Unisphere GUI, click Hosts at the top.
2. Click the Initiators.
3. Select the first unregistered initiator and click Register.

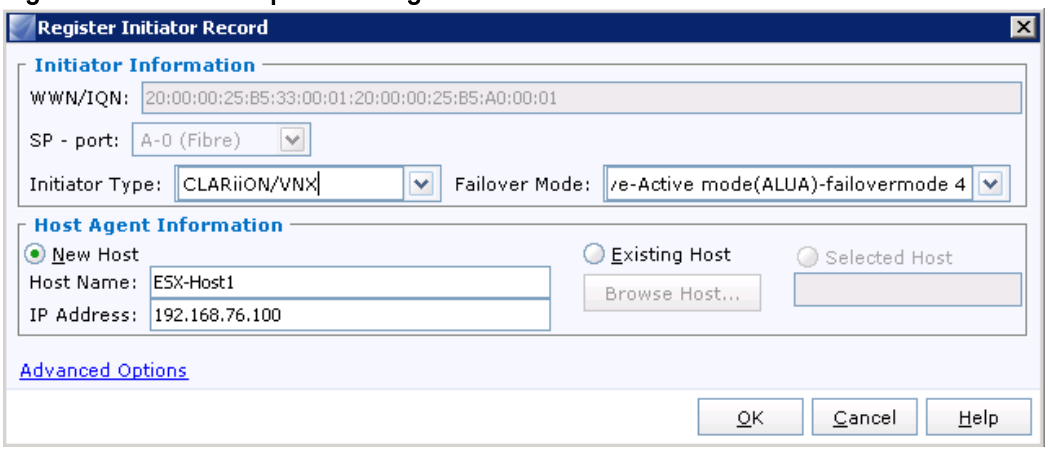
Figure 308 EMC Unisphere – List of Initiators




4. In Cisco UCS Manager, click SAN tab in the navigation pane.
5. Select Pools > root > WWPN Pools > WWPN Pool <<var_ucs_global_wwpn_a_pool_name>>.
6. In the right side click the Initiators tab.
7. This would list the WWPN identifies of all hosts. Using these IDs, you can associate WWPN to the server.
8. Back in the Unisphere GUI, on the Register Initiator Record" wizard, popped up by the action taken in step 1.
9. Select Initiator Type as CLARiiON/VNX.
10. Select Failover Mode as ...failovermode 4 from the drop-down menu.
11. Click the New Host radio button.
12. Provide the hostname.
13. Enter the management IP address of the host.

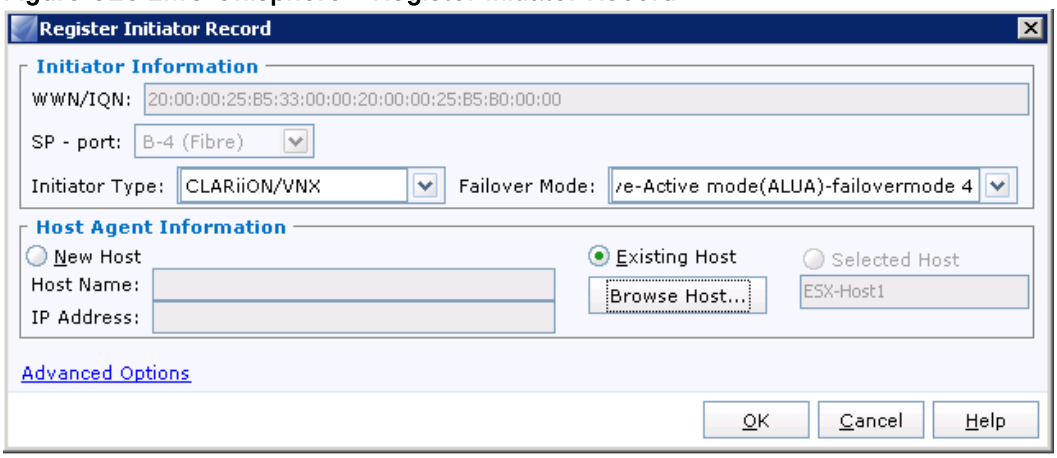
14. Click OK.
15. Click Yes in the Pop-Up window.
16. Click OK in the Pop-Up window.
17. Click OK.

Figure 309 EMC Unisphere – Register Initiator Record



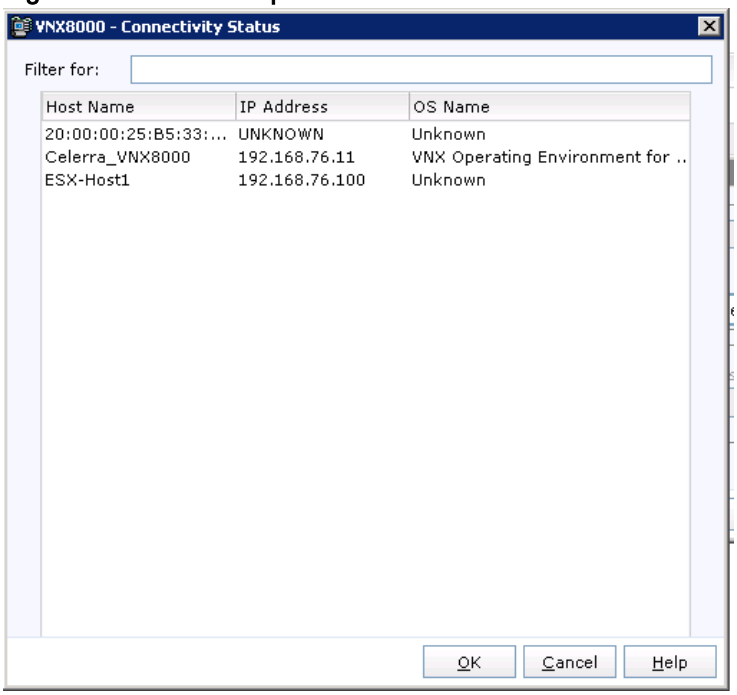

18. Select the second vHBAs WWPN from the same server.
19. Click the Register.
20. Click the Existing Host radio button.
21. Click Browse Host to select the host.

Figure 310 EMC Unisphere – Register Initiator Record



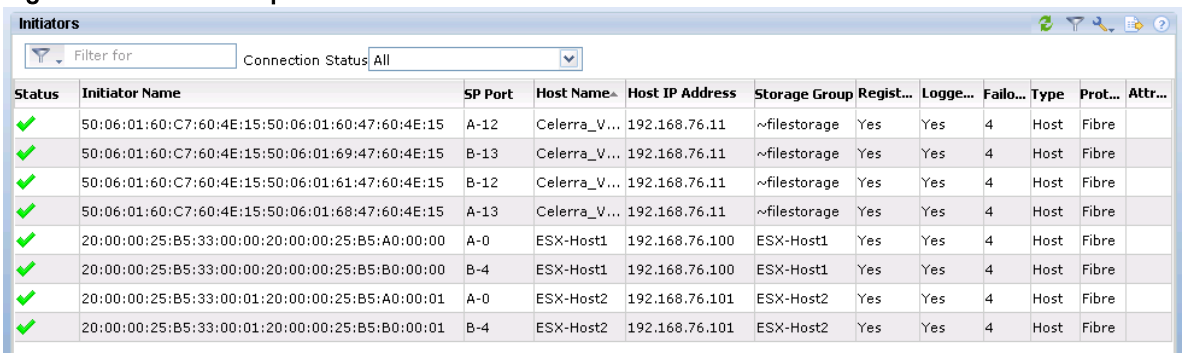

22. Select the previously registered host, and click OK.

**Figure 311 EMC Unisphere – Select Host**




23. Repeat these steps for all the servers in the group. The result will look like the screen shot below:

**Figure 312 EMC Unisphere – List of Initiators**



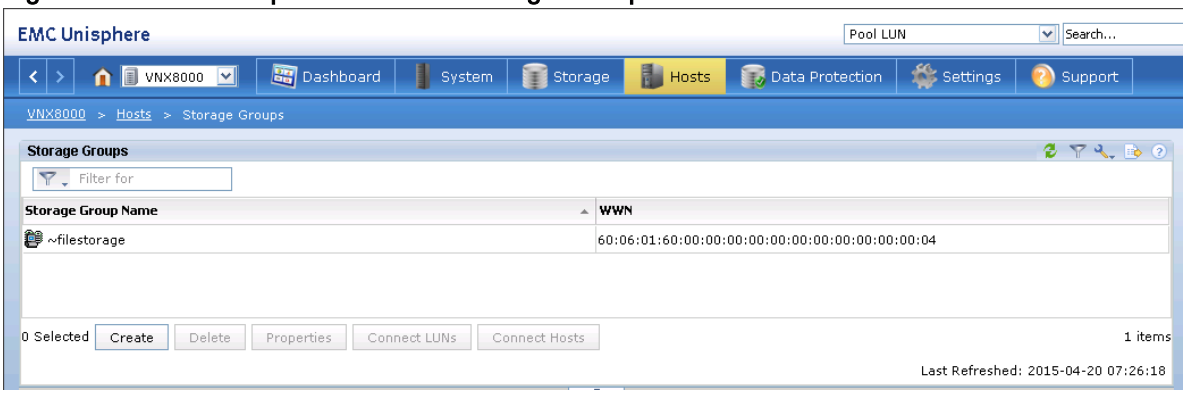

| Status | Initiator Name | SP Port | Host Name | Host IP Address | Storage Group | Regist... | Logge... | Failo... | Type | Prot... | Attr... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:60:47:60:4E:15 | A-12 | Celerra_V... | 192.168.76.11 | ~filestorage | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:69:47:60:4E:15 | B-13 | Celerra_V... | 192.168.76.11 | ~filestorage | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:61:47:60:4E:15 | B-12 | Celerra_V... | 192.168.76.11 | ~filestorage | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:68:47:60:4E:15 | A-13 | Celerra_V... | 192.168.76.11 | ~filestorage | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:00:20:00:00:25:B5:A0:00:00 | A-0 | ESX-Host1 | 192.168.76.100 | ESX-Host1 | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:00:20:00:00:25:B5:B0:00:00 | B-4 | ESX-Host1 | 192.168.76.100 | ESX-Host1 | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:01:20:00:00:25:B5:A0:00:01 | A-0 | ESX-Host2 | 192.168.76.101 | ESX-Host2 | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:01:20:00:00:25:B5:B0:00:01 | B-4 | ESX-Host2 | 192.168.76.101 | ESX-Host2 | Yes | Yes | 4 | Host | Fibre | |

## Configure Storage Groups

Now that the hosts as well as the LUNs are created on the VNX storage array, you need to create storage groups to assign access to LUNs for various hosts. The boot LUN will be dedicated to a specific server. To configure storage groups, complete the following steps:

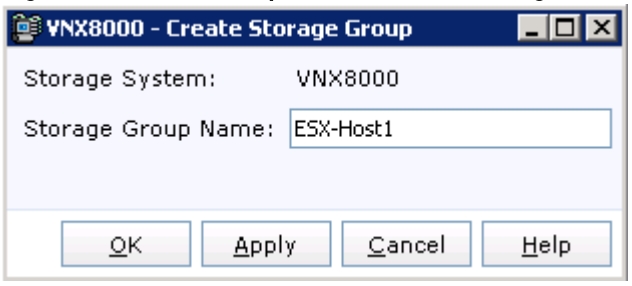
1. Click Hosts in EMC VNX Unisphere GUI.
2. Click Storage Groups.
3. Click Create to create a new storage group.

Figure 313 EMC Unisphere – List of Storage Groups



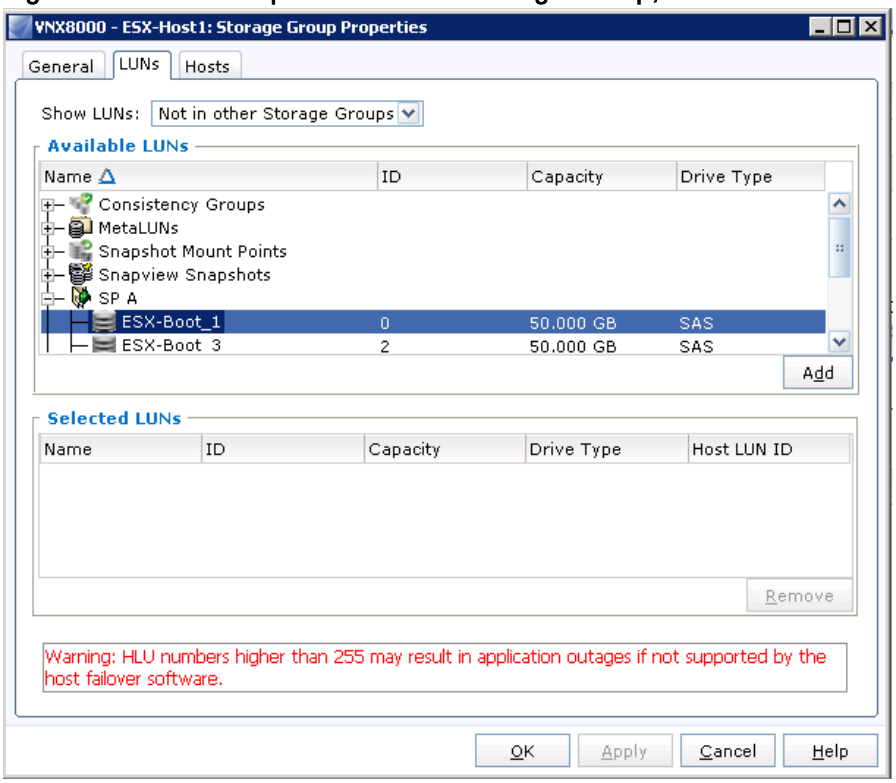

4. Provide a name to the storage group.
5. Click OK.
6. Click Yes.

Figure 314 EMC Unisphere – Create Storage Group



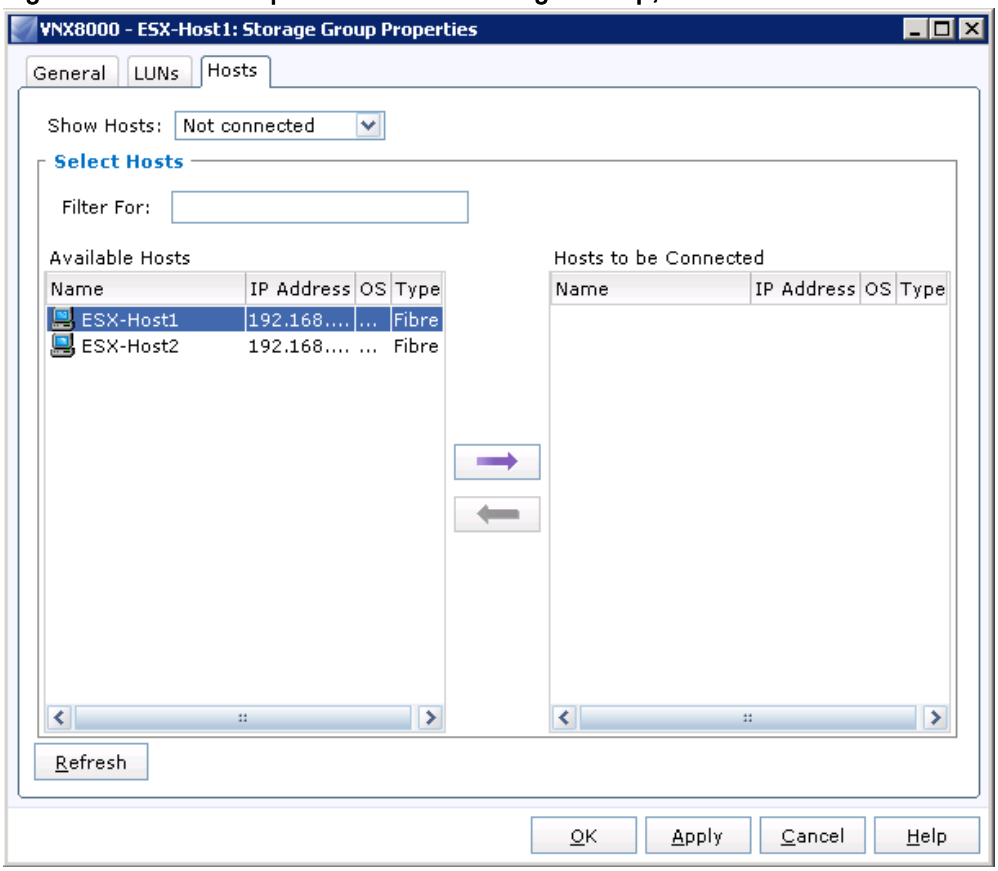

7. The success message appears. The system will prompt you to create LUNs and connect hosts.
8. Click Yes.
9. From the LUNs tab of the popped up wizard, select a single LUN and click Add.

Figure 315 EMC Unisphere – Create Storage Group, Select LUNs




10. Click Hosts tab.
11. Select a single server to add on the storage group.
12. Click OK to deploy the storage group.

Figure 316 EMC Unisphere – Create Storage Group, Select Host

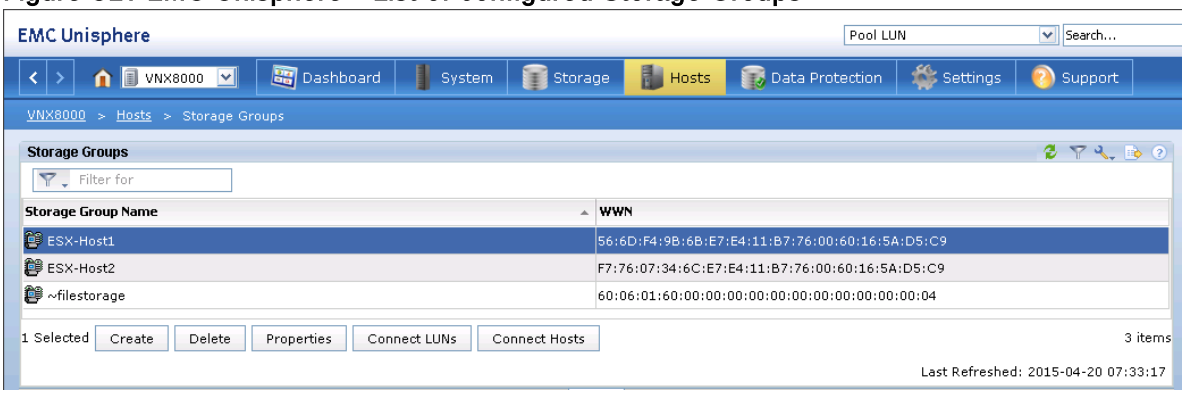



13. Click Yes.

14. Click OK.

15. Repeat these steps for all five servers. The result will look like the screen shot below:

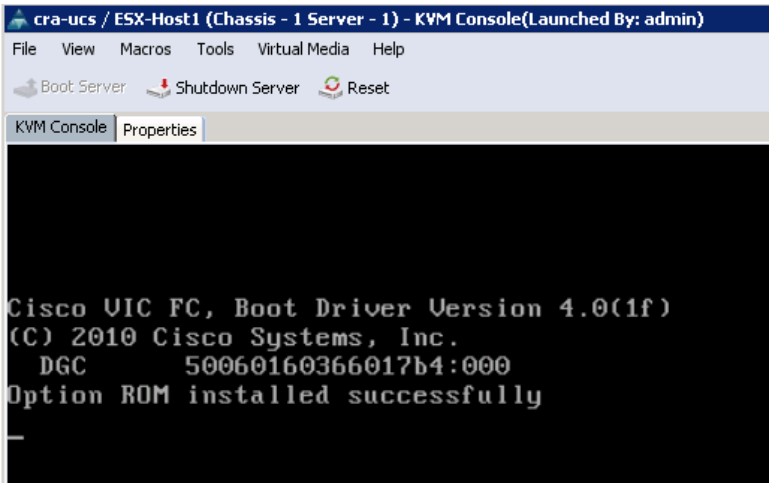
Figure 317 EMC Unisphere – List of configured Storage Groups




Now there is end-to-end FC storage access from the servers in Cisco UCS to the specific boot LUN on the VNX storage devices. Next, install the ESXi images on the server.

To verify that the storage group was created, complete the following steps:

1. Log in to Cisco UCS Manager and open the KVM of ESX-Host1.
2. Boot the server and verify the Cisco VIC FC adapter message. If all is configured correctly, you will see a line with the LUN (DGC 5006....) for both vHBAs.

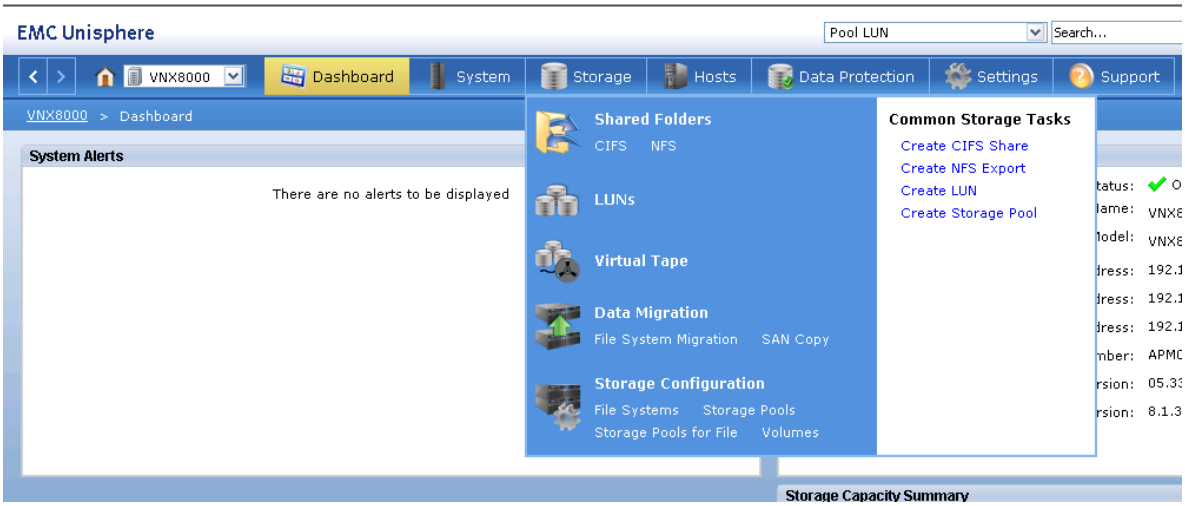



## Configure Storage Pools for File

To configure Storage Pools for File, complete the following steps:

1. Click the Storage tab.
2. Select Storage Configuration > Storage Pools.

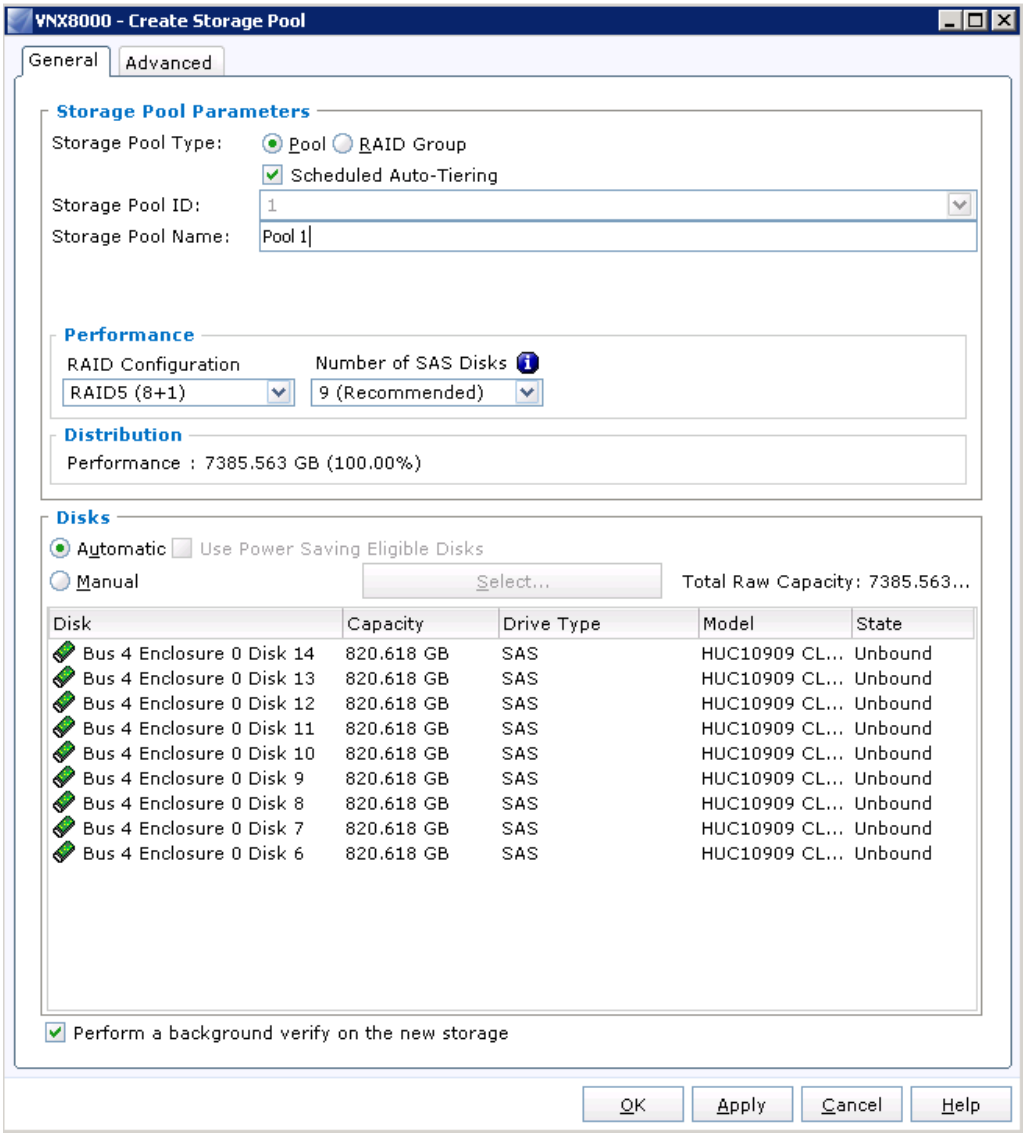
**Figure 318 EMC Unisphere – Select Storage Pool for File**




3. Click Create.

4. Keep Pool selected as the Storage Pool Type.
5. Enter <<var_vnx1_fs-pool1_name>> as the Storage Pool Name.
6. Choose RAID5 (8 + 1) as the RAID Configuration.
7. Choose 9 (Recommended) as the Number of SAS Disks.
8. In the Disks Section keep Automatic selected, the Configuration wizard will select 9 SAS disks to create the storage pool.
9. Click OK.
10. Click Yes to Initiate the Pool creation.

Figure 319 EMC Unisphere – Create Storage Pool




11. Click Yes to accept the Auto-Tiering Warning.

12. Click OK.

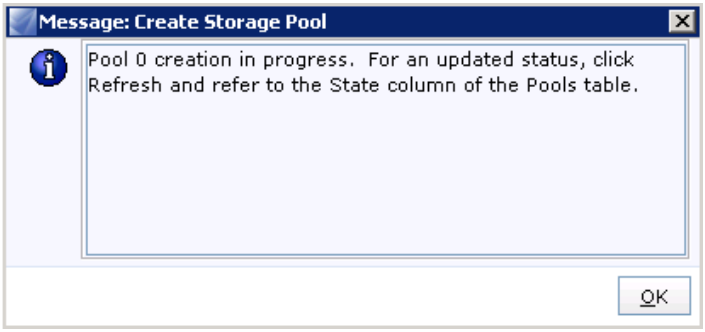
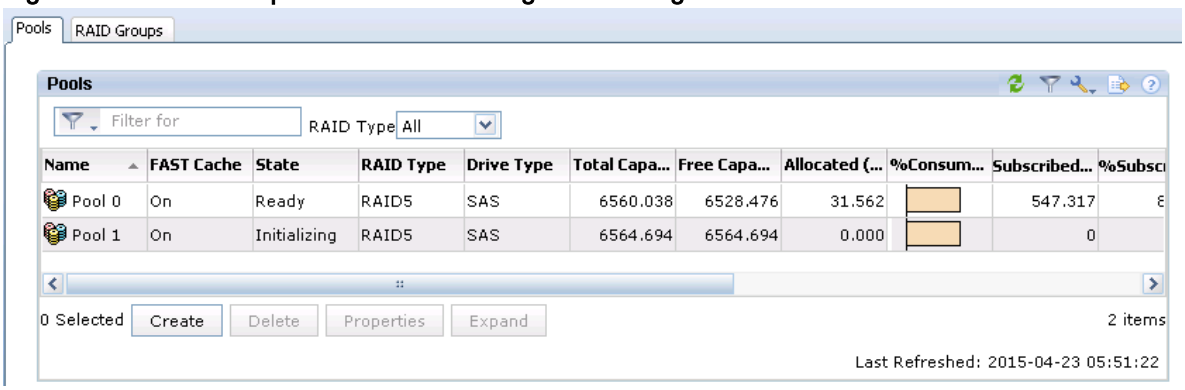
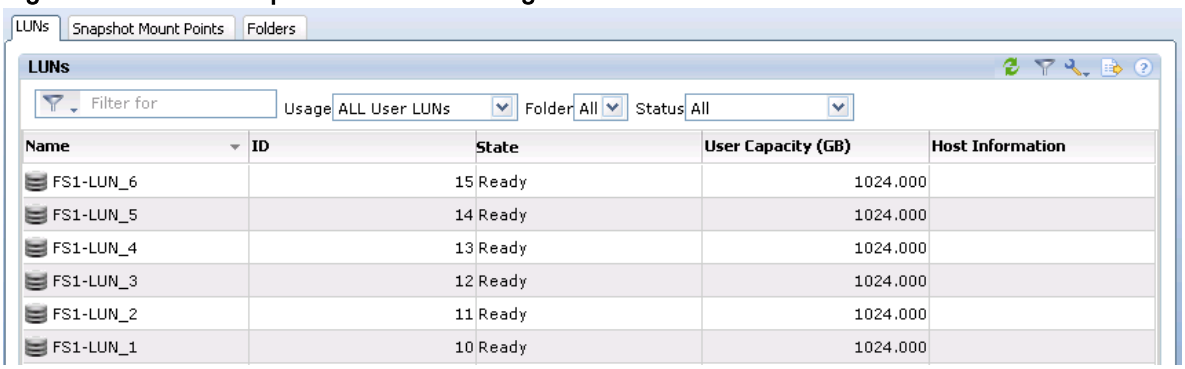


**Figure 320 EMC Unisphere – List of configured Storage Pools**




13. Click Storage > LUNs.
14. Click Create.
15. Select Pool 1 as the Storage Pool for new LUN.
16. Clear the Check-Box for Thin.
17. Enter 1 and TB as the User Capacity.
18. Enter 6 as Number of LUNs to create.
19. Click the Radio-Button for Name.
20. Enter FS1-LUN as the name.
21. Enter 1 as the Starting ID.
22. Click Apply.
23. Click Yes.
24. Click OK.
25. Click Cancel.

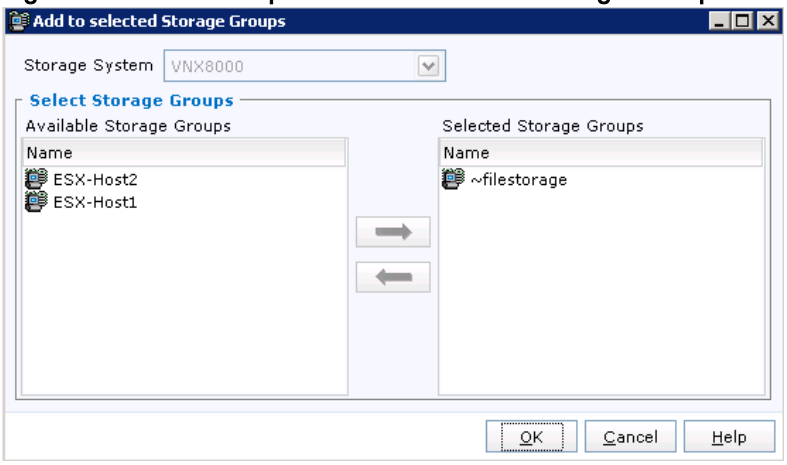
Figure 321 EMC Unisphere – List of configured LUNs




26. Select all created LUNs, click Add to Storage Group.

27. Select ~filestorage, click → button, click OK.

Figure 322 EMC Unisphere – Add Hosts to Storge Group

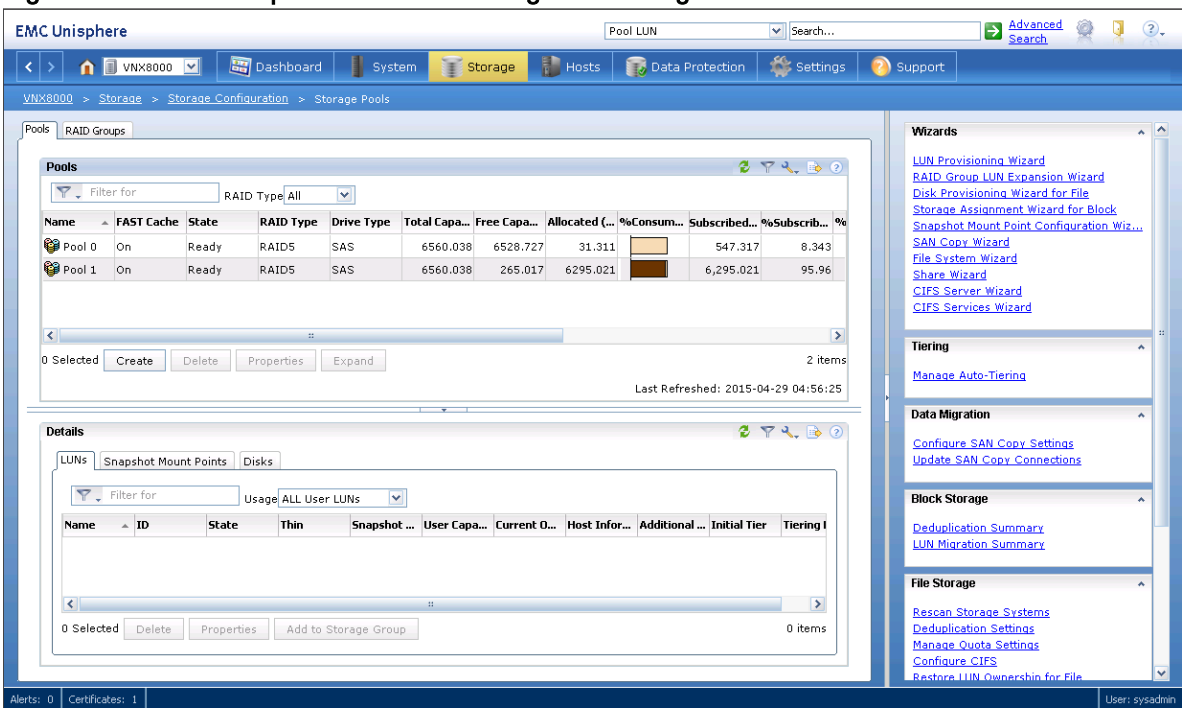



28. Click Yes.

29. Click OK.

30. Click Rescan storage systems on right hand side as shown below. Rescan may take a few minutes.

**Figure 323 EMC Unisphere – List of Configured Storage Pools**



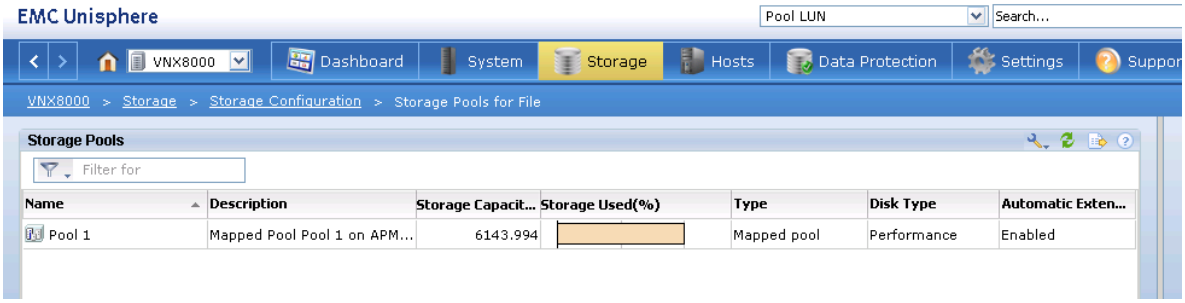

31. When the rescan successfully finishes (track the progress at “Background task for files” page under System menu > Monitoring and Alerts).

32. Click the Storage tab.

33. Select Storage Configuration > Storage Pools for File.

34. Click Refresh-button if the newly created storage pool is not visible on the left side of the window as shown below:

**Figure 324 EMC Unisphere – List of Storage Pool for File**

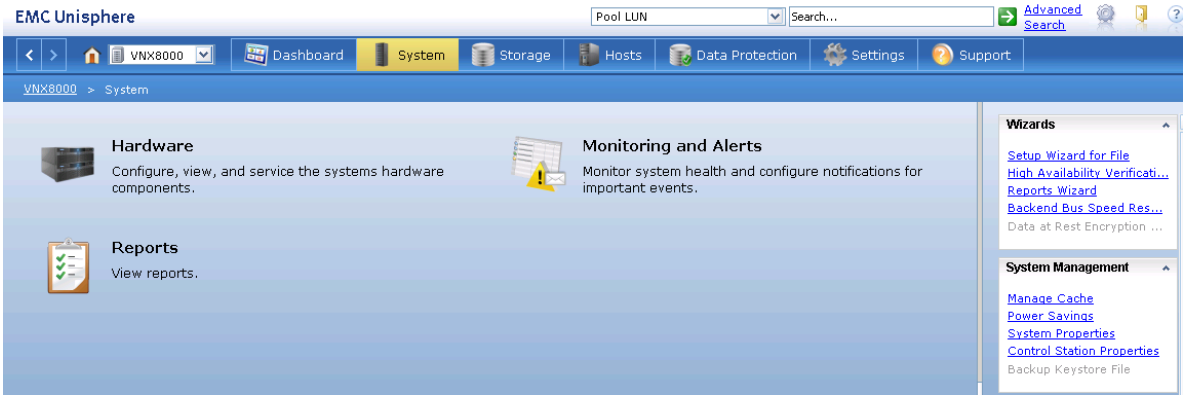



## Configure Network and File Service

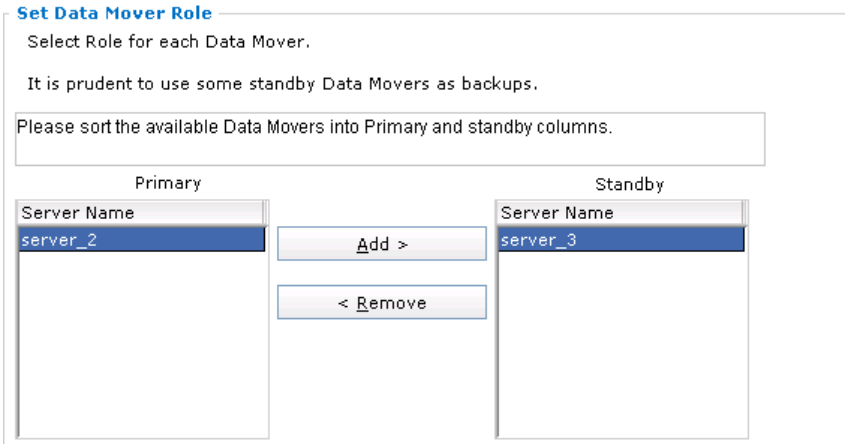
Now create a highly available network access for the NFS volume. To create LACP interfaces, complete the following steps:

1. In EMC Unisphere GUI, click System.
2. In the Wizards section, click Setup Wizard for File.

**Figure 325 EMC Unisphere – System Settings Menu**



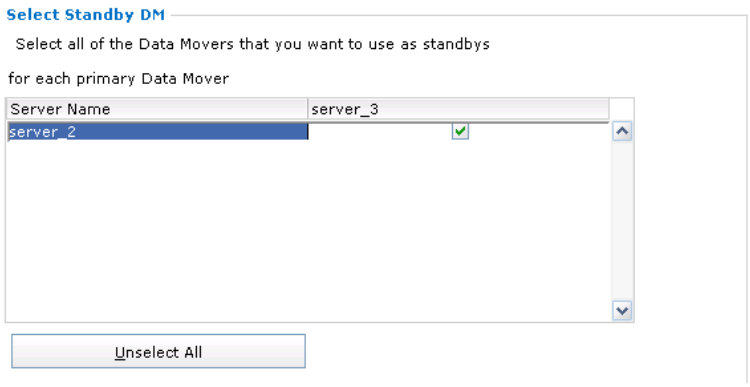

3. Begin Setup page, click Next.
4. Setup Data Mover page, click Next.
5. Setup Data Mover Role, click Next.
6. Select server_2 as Primary and server_3 as Standby, click Next.




7. Overview / Results page, click Next.
8. Waiting for Data Movers page, click Next.
9. Unicode Enabled page, click Next.
10. Select Standby DM page
11. Select server_3 as standby.

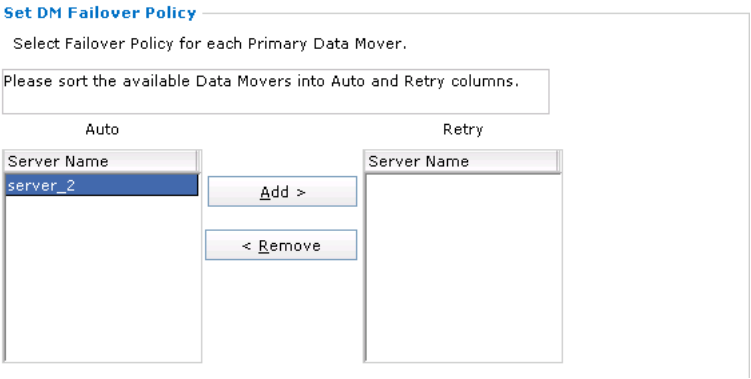
12. Click the checkbox.

13. Click Next.



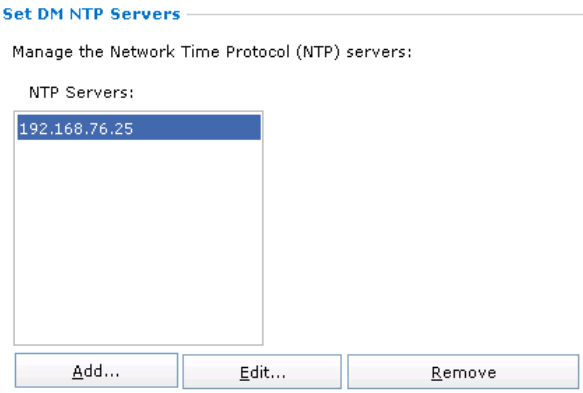

14. Set DM Failover Policy page and select server_2 as Auto.

15. Click Next.

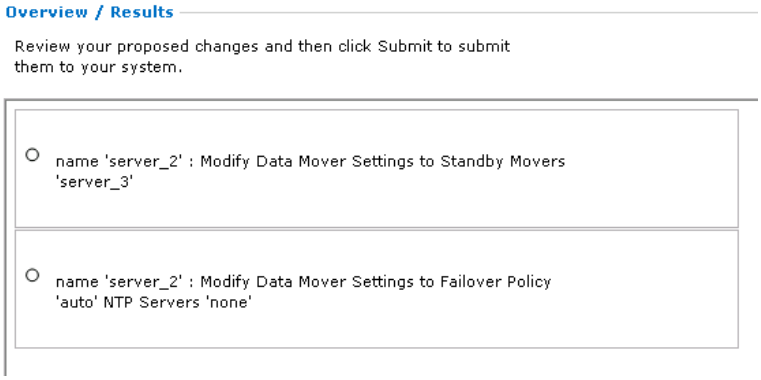



16. Set DM NTP Servers page and add <<var_global_ntp_server_ip>> as the available NTP server.

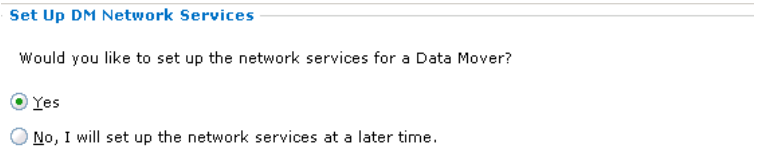
17. Click Next.



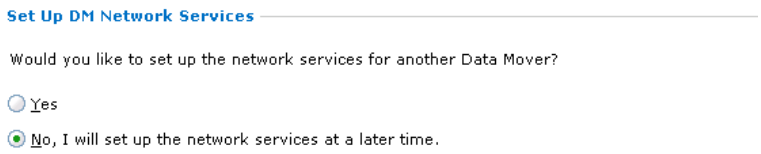

18. Overview / Results page, click Submit.



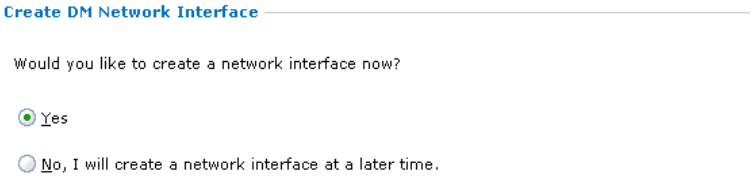

19. After all the changes have completed successfully, click Next.
20. Set Up DM Network Services page, click Next.




21. Select a Data Mover page, select server_2 from the drop-down menu, click Next.
22. DM DNS Settings page, add <<var_nameserver_ip>> and <<var_nameserver2_ip>> as the DNS server, click Next.
23. DM NIS Settings page, click Next.
24. Overview / Results page, click Submit.
25. After all changes are completed successfully, click Next.
26. Set Up DM Network Services page, select No, then click Next.

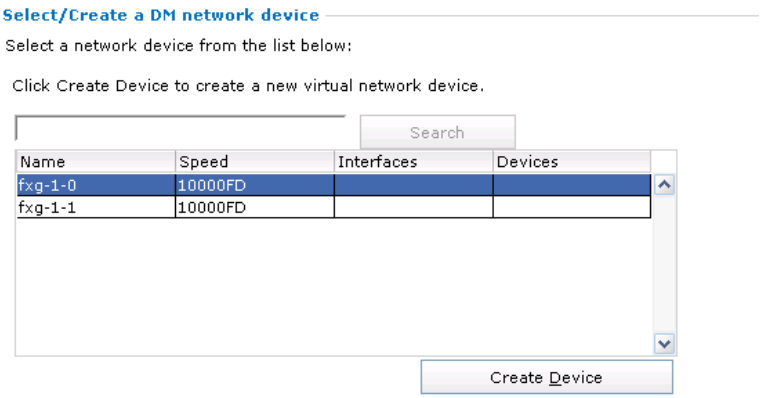



27. Create DM Network Interface page, click Next.



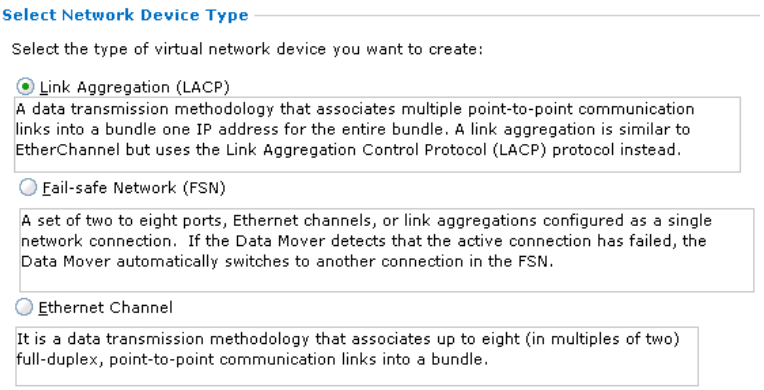

28. Select Data Mover page, select server_2 from the Drop-down menu, click Next.

29. Select / Create a DM network device page, click Create Device.



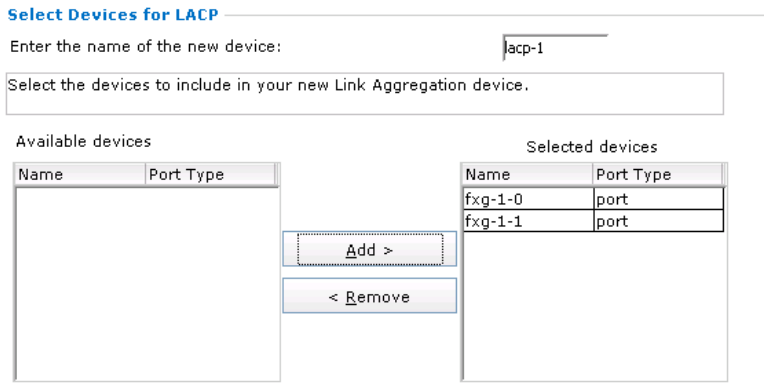

30. Select server_2, click Next.

31. Select Link Aggregation (LACP), click Next.




32. Enter <<var_vnx1_lacp_dev_name>> as the name of the new device.

33. Add fxg-1-0 and fxg-1-1 to the selected devices, click Next.

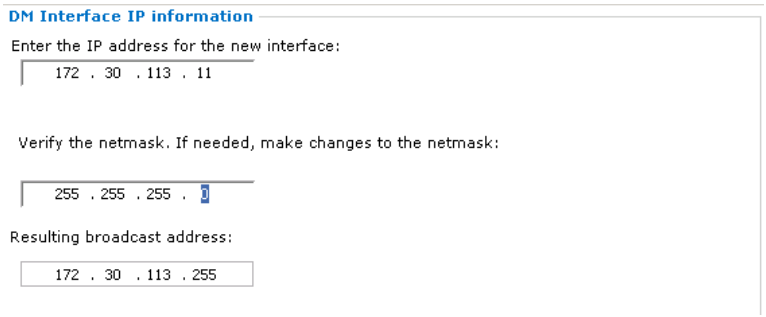



34. Click Submit.

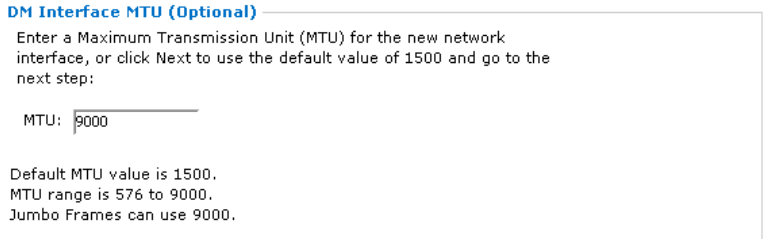
35. After all changes are completed successfully, click Next.

36. Select <<var_vnx1_lacp_dev_name>> , click Next.

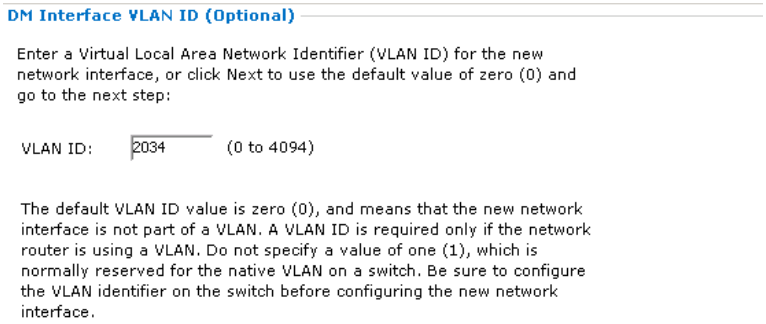
37. Enter <<var_vnx1_dm2_nfs_ip>> and <<var_nfs_netmask>>, click Next.



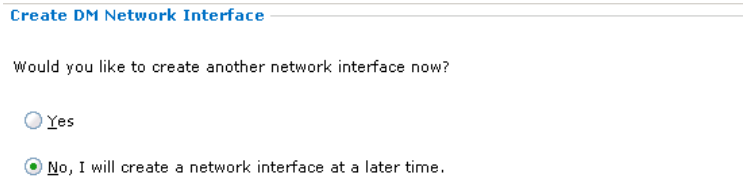

38. Enter 9000 as MTU, click Next.



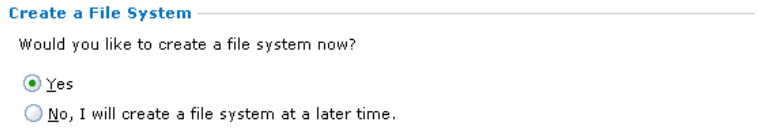

39. Enter <<var_esx_nfs_vlan_id>>, click Next.



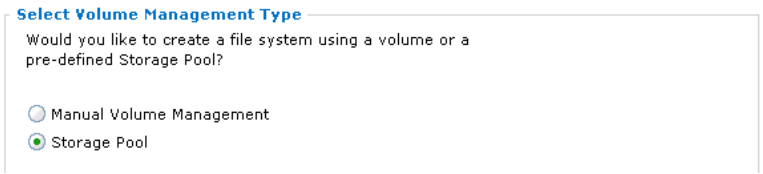

40. Overview / Results page, click Submit.
41. Overview / Results page, click Next.
42. Test the New Route page, click Next.
43. Create DM Network Interface page, select No, I will ..., click Next.




44. Create a File System page, select Yes, click Next.

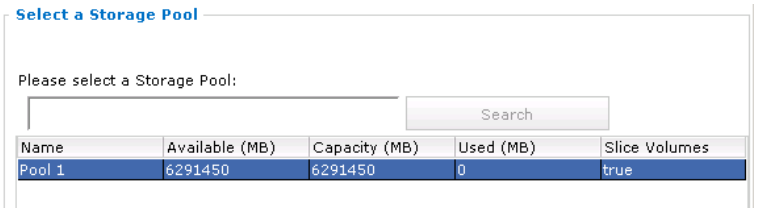



45. Select Data Mover page, select server_2, click Next.
46. Select Volume Management Type, select Storage Pool, click Next.
47. Click Create Volume.
48. Select Meta, Click Next.




49. Select <<var_vnx1_fs-pool1_name>> .

50. Click Next.

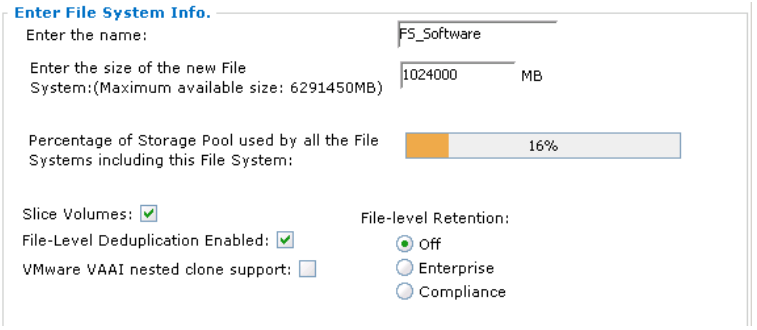



51. Enter <<var_vnx1_fs1_name>> as the name.

52. Enter <<var_vnx1_fs1_size>> as the size.

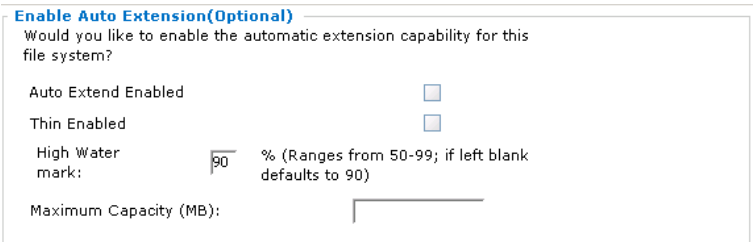
53. Click the checkbox for File-Level Deduplication if the license is available.

54. Click Next.



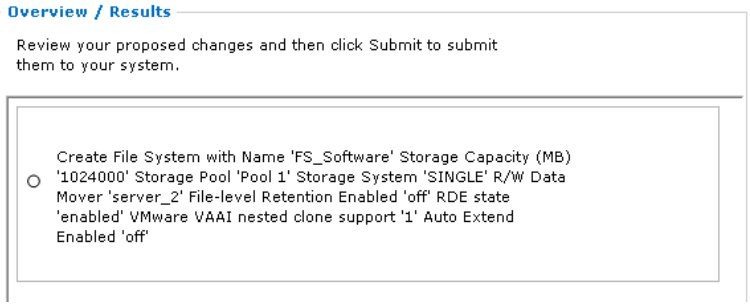

55. Enable Auto Extend and define the Maximum Capacity.

56. Click Next.




57. Default Quota Page, select No and click Next.

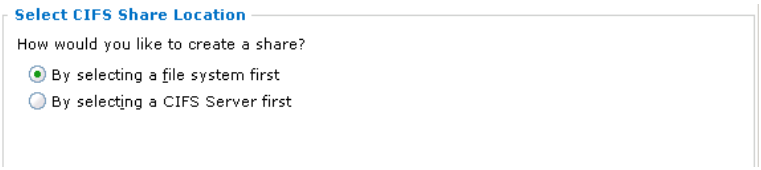
58. Review the information and click Submit.




59. Click Next.

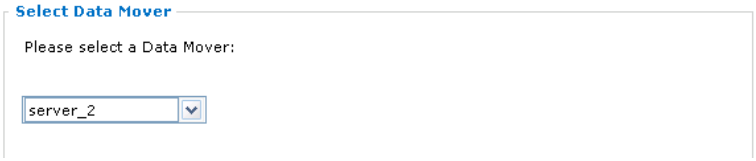
60. Create File System page, select No and click Next.

61. Create a CIFS Share page, select Yes and click Next.




62. Select server_2 from the drop-down menu.

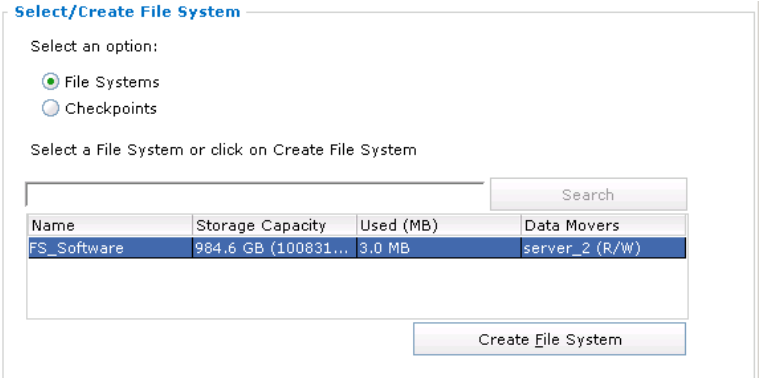
63. Click Next.



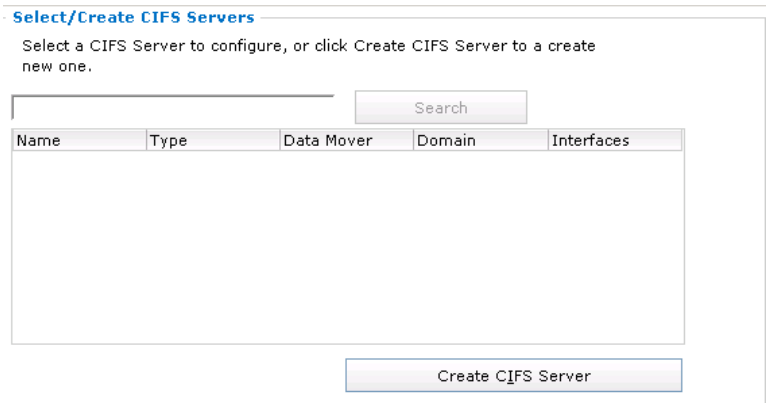

64. Select File Systems.

65. Select <<var_vnx1_fs1_name>>.

66. Click Next.

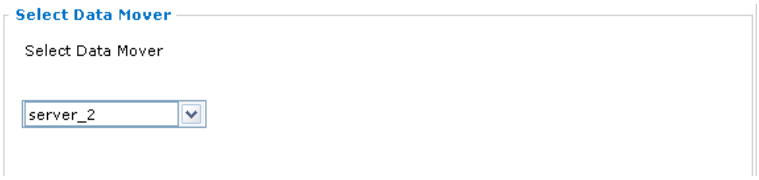



67. Click Create CIFS Server.



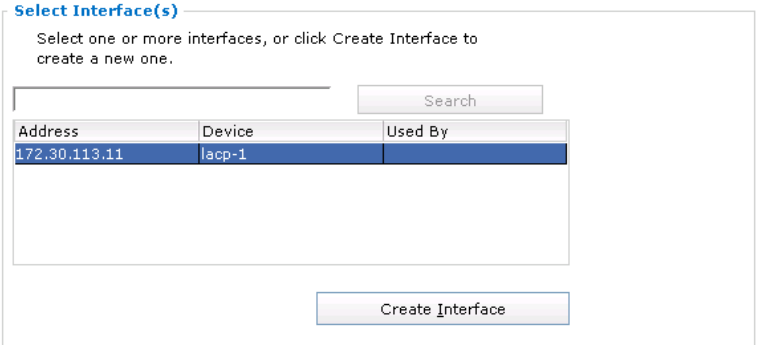

68. Select server_2 from the drop-down menu.

69. Click Next.



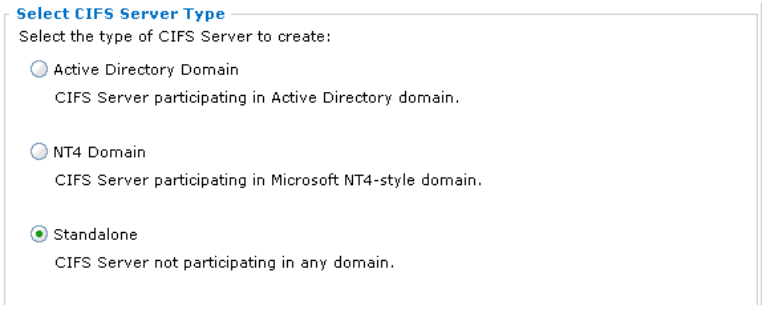

70. Select <<var_vnx1_lacp_dev_name>> .

71. Click Next.



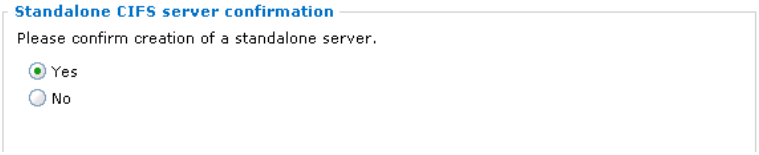

72. Select the CIFS Server type as required. In this solution, Standalone is used.

73. Click Next.

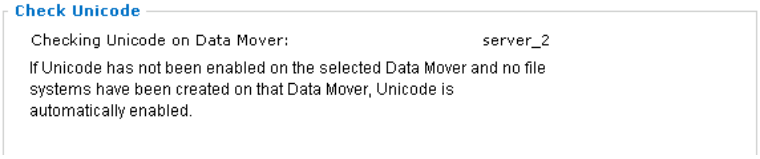



74. Confirm the Standalone CIFS Server configuration.

75. Click Next.

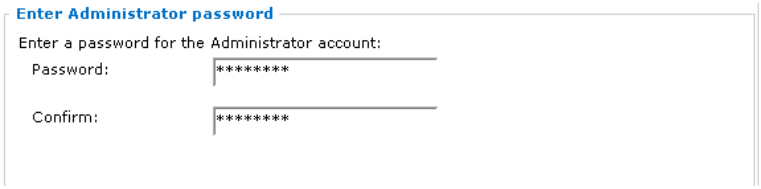



76. Check Unicode Page, click Next.




77. Enter <<var_mgmt_passwd>> and confirm it.

78. Click Next.



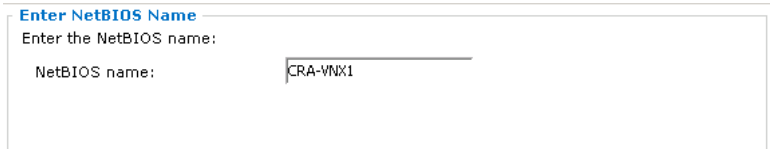

79. Enter <<var_vnx1_cifs_workgroup>> as the Workgroup.

80. Click Next.

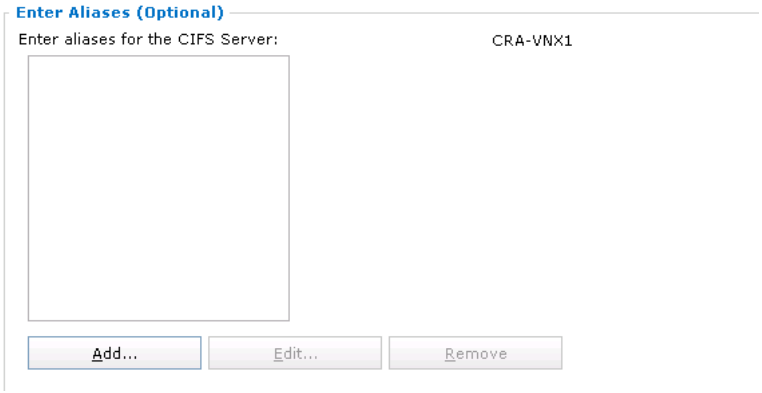



81. Enter <<var_vnx1_netbios_name>> as the NetBios name.

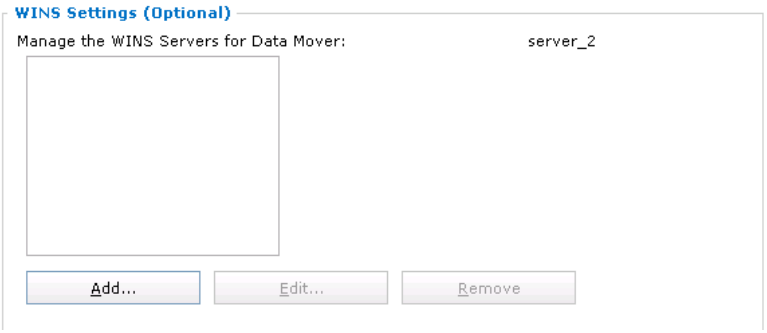
82. Click Next.




83. Enter Aliases page, click Next.

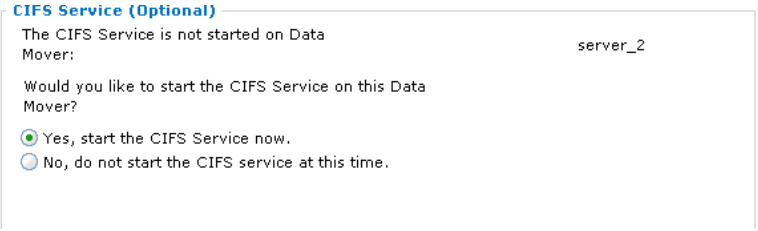



84. WINS Settings page, click Next.




85. Select Yes and start the CIFS Server.

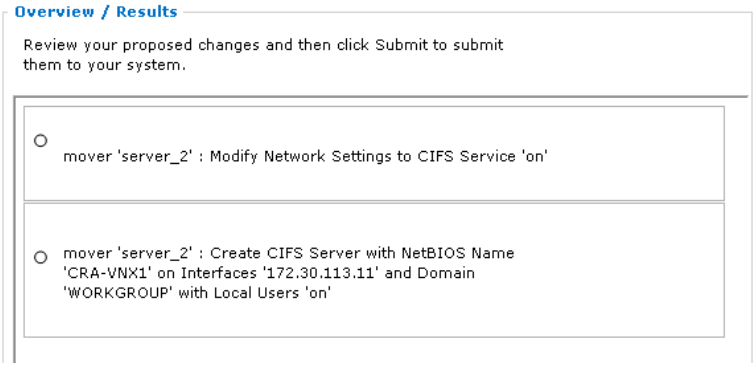
86. Click Next.




87. Review the Information.

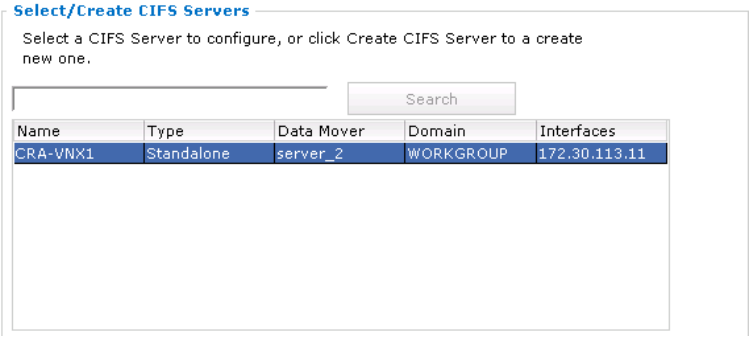
88. Click Submit.

89. Click Next.



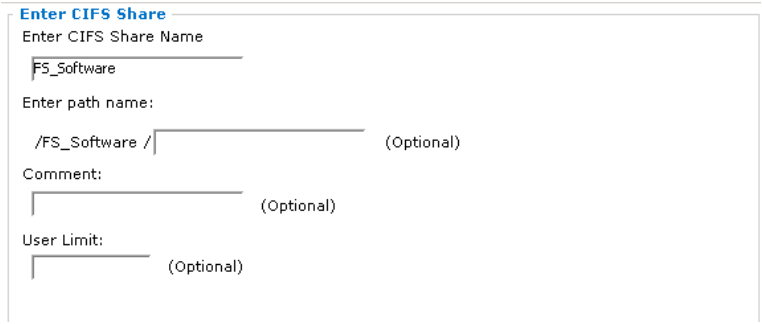

90. Select <<var_vnx1_netbios_name>>.

91. Click Next.




92. Enter <<var_vnx1_cifs_share1_name>> as the name.

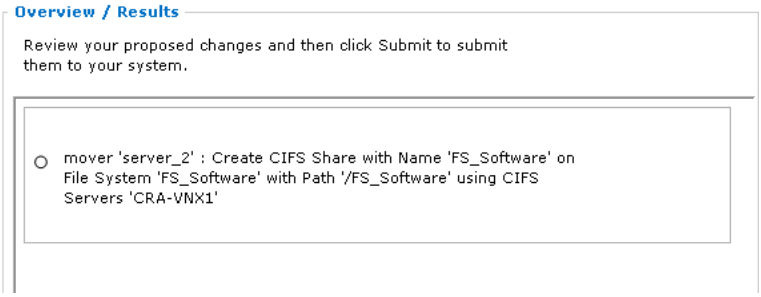
93. Click Next.




94. Review the information.

95. Click Submit.

96. Click Next.

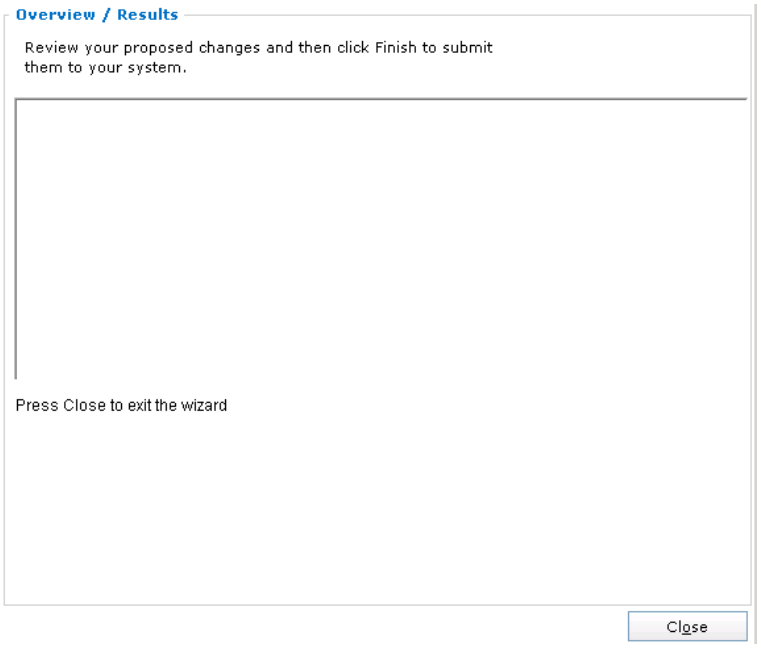



97. Select No.

98. Click Next.




99. On the last Overview page, click Close.

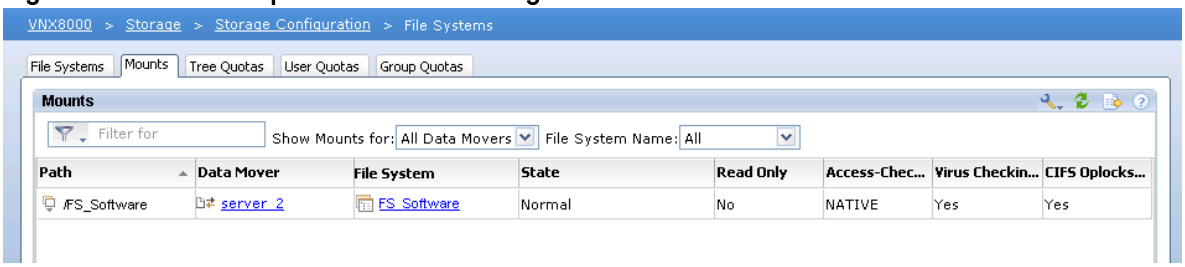



## Enable Direct Writes for all the File Systems

1. Select Storage > Storage Configuration > File Systems.
2. Click Mounts tab.
3. Select the path <<var_vnx1_nfs1_name>>.

4. Click Properties.

**Figure 326 EMC Unisphere – List of Configured Mounts on the Data Movers**

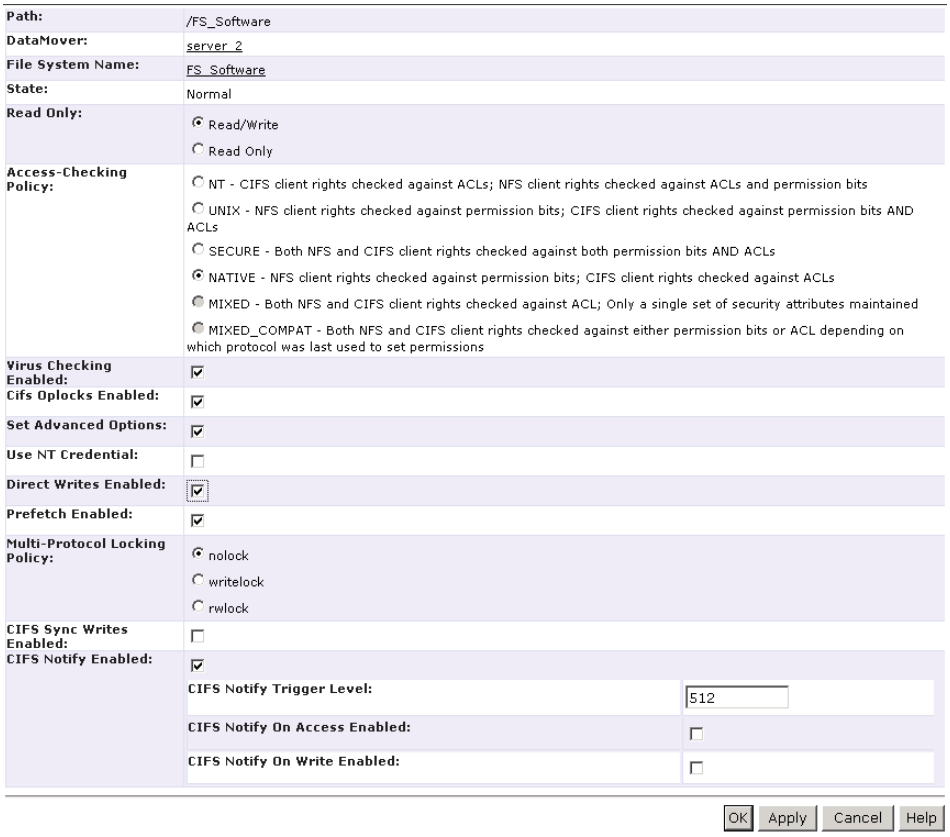



5. From the mount properties. Make sure Read/Write & Native Access policy is selected.

6. Select the Set Advanced Options check box.

7. Check the Direct Writes Enabled check box.

8. Click OK.



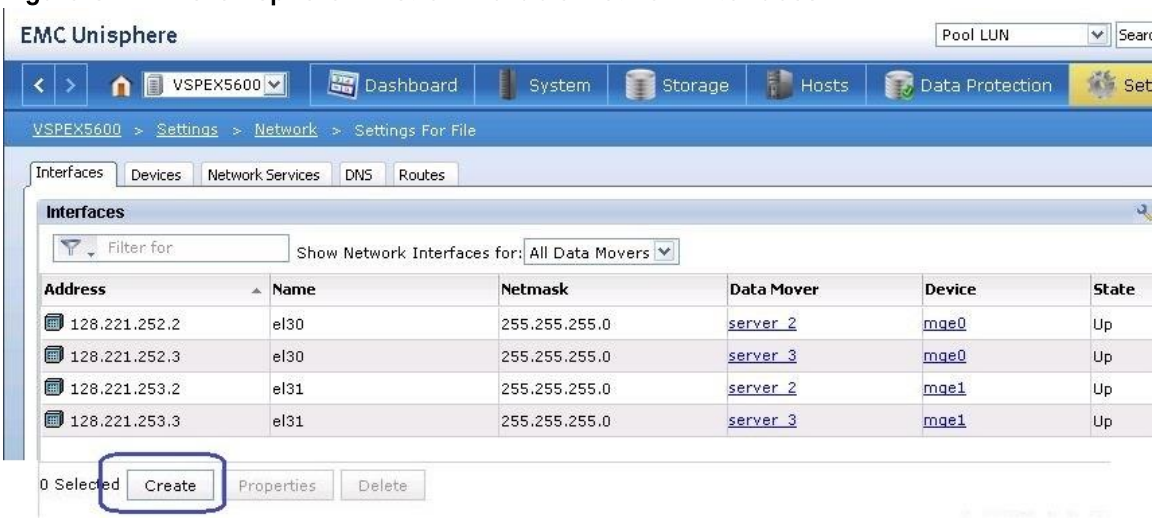

9. Repeat these steps for all File Systems created on the Storage.

## Create Additional Network Settings

To create additional network settings, complete the following steps:

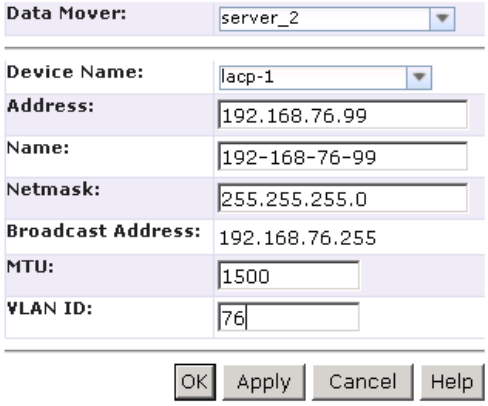
1. Navigate to Settings > Network > Select Settings for File.
2. Click Interfaces tab.

**Figure 327 EMC Unisphere – List of Available Network Interfaces**




3. Select Data Mover as server_2.
4. Choose Device name as lacp-1 from the drop-down list.
5. Specify <<var_vnx1_dm2_mgmt_ip>> as the IP address.
6. Netmask is <<var_mgmt_netmask>>.
7. Interface name as <<var_vnx1_dm2_mgmt_name>>.
8. MTU value as 1500 to allow jumbo frames for the lacp interface.
9. Click OK.

Figure 328 EMC Unisphere – Create a new Network Interface

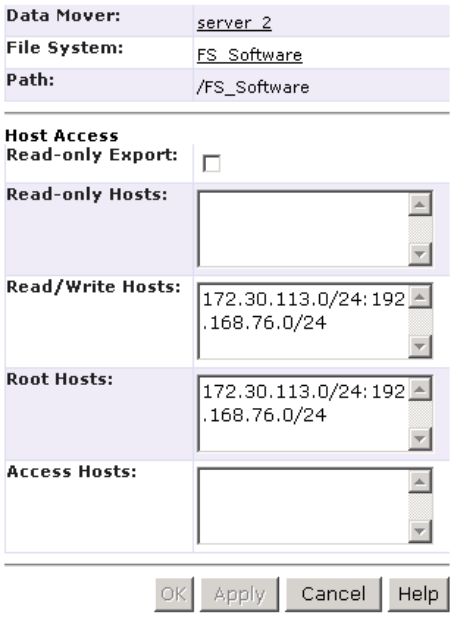



## Create NFS Share

To create a NFS Share, complete the following steps:

1. Select Storage > Shared Folders > NFS.
2. Click Create.
3. Select server_2 from the drop-down menu.
4. Select <<var_vnx1_fs1_name>> from drop-down menu.
5. Enter <<var_vnx1_nfs1_name>> as the Path.
6. Enter <<var_nfs_network>> and <<var_mgmt_network>> with the related netmask to Read/write hosts and Root hosts.
7. Click OK.

Figure 329 EMC Unisphere – Create a new NFS Share




## Software Repository

To have access to all software sources required later in the Datacenter Reference Architecture, such as ISO Images for the Operating systems or Installation files for Applications it is recommended to copy those onto the created FS_Software share. You can mount this share to all VMware ESXi hosts as well as to all Linux hosts and virtual machines as Read-Only to access the ISO images.

# VMware ESXi Host Installation

This section describes the installation and basic configuration of VMware ESXi 5.5, as follows:

- Installation from ISO-Image
- Initial Configuration
- Setup Management Network through KVM
- VMware ESXi configuration with VMware vCenter Client software

Table 34 lists the required information to setup the VMware ESX hosts in this Cisco UCS Integrated Infrastructure for SAP HANA with EMC VNX Storage.

Table 36 Information to Setup VMware ESXi hosts

| Name | Variable |
|---|---|
| Name of the UCS Sub-Organization for ESX hosts | <<var_ucs_esx_sub-org>> |
| Name of the Service Profile for ESX host X | <<var_ucs_esxX_sp_name>> |

| Name | Variable |
|---|---|
| Global default administrative password | <<var_mgmt_passwd>> |
| Infrastructure Management Network VLAN ID | <<var_management_vlan_id>> |
| Management Network IP Address of ESX host X | <<var_esxX_ip>> |
| Management network Netmask | <<var_mgmt_netmask>> |
| Management network default Gateway | <<var_mgmt_gw>> |
| DNS server 1 IP Address | <<var_nameserver_ip>> |
| DNS server 2 IP Address | <<var_nameserver2_ip>> |
| Full Qualified Domain Name of ESX host X | <<var_esxX_fqdn>> |
| Virtual Center Server IP address | <<var_vc_ip_addr>> |
| Name of the Management Network for the VMkernel | <<var_vmkern_mgmt_name>> |
| Name of the Management Network with VM access | <<var_esx_mgmt_network>> |
| Global Administration Network VLAN ID | <<var_admin_vlan_id>> |
| Name of the NFS Network for the VMkernel | <<var_esx_vmkernel_nfs>> |
| VMware ESX Storage access Network VLAN ID | <<var_esx_nfs_vlan_id>> |
| NFS Network IP Address of ESX host 1 | <<var_esx1_nfs_ip>> |
| Netmask of the NFS Network | <<var_nfs_netmask>> |
| Name of the VMotion Network for the VMkernel | <<var_esx_vmkernel_vmotion>> |
| VMware Vmotion Network VLAN ID | <<var_vmotion_vlan_id>> |
| VMotion Network IP Address of ESX host 1 | <<var_esx1_vmotion_ip>> |
| Netmask of the Vmotion Network | <<var_vmotion_netmask>> |
| Port Profile name for Management traffic | <<var_n1k_mgmt_pp-name>> |
| Port Profile name for Client Access traffic | <<var_n1k_client_pp_name>> |
| Port Profile name for NFS traffic | <<var_n1k_nfs_pp_name>> |

The X stands for any number of ESX-Host, like 1 for ESX-Host1 Service Profile, IP address and hostname, 2 for ESX-Host2 Service Profile, IP address and hostname.

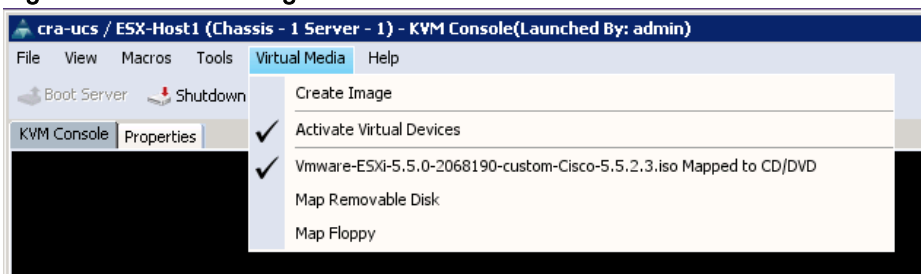
To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organizations > <<var_ucs_esx_sub-org>>.
3. Select <<var_ucs_esx1_sp_name>>.
4. Click KVM Console in the right pane.
5. Open with Java JRE installed.
6. Click Continue in the Pop-Up window.
7. Click the Virtual Media Menu.
8. Click Activate Virtual Devices.
9. If prompted, click Accept this Session and the checkbox to Remember this setting.




10. Click Apply.
11. Click the Virtual Media Menu.
12. Click Map CD/DVD.
13. Browse to the ESXi installer ISO image file and click Open.
14. Please download the latest ESXi-5.5.0-*-Custom-Cisco-5.5.*.iso from the VMware website.
15. Click Map Device.

Figure 330 UCS Manager – Virtual Media Menu




16. Power On or PowerCycle the Server.
17. Use the KVM Window to monitor the server boot.
18. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
19. After the installer is finished loading, press Enter to continue with the installation.
20. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
21. Select the LUN from the EMC VNX Storage which was previously created for ESXi and press Enter to continue with the installation.
22. Select the appropriate keyboard layout and press Enter.
23. Enter <<var_mgmt_passwd>> and confirm the root password and press Enter.
24. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
25. After the installation is complete, clear the Mapped checkbox (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.
26. The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.
27. The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Because the media cannot be ejected and it is read-only, simply click Yes to unmap the image.
28. From the KVM tab, press Enter to reboot the server.

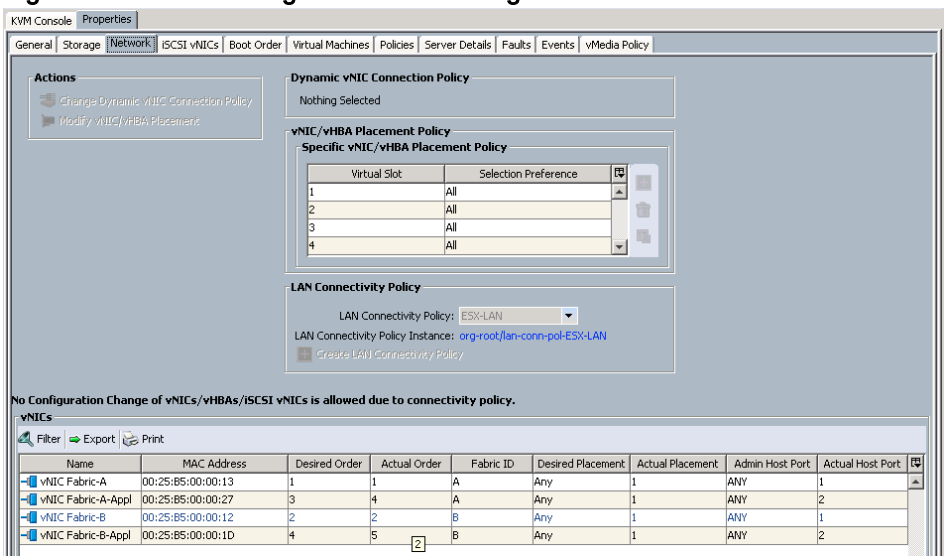
## Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host.

To configure the ESX host with access to the management network, complete the following steps:

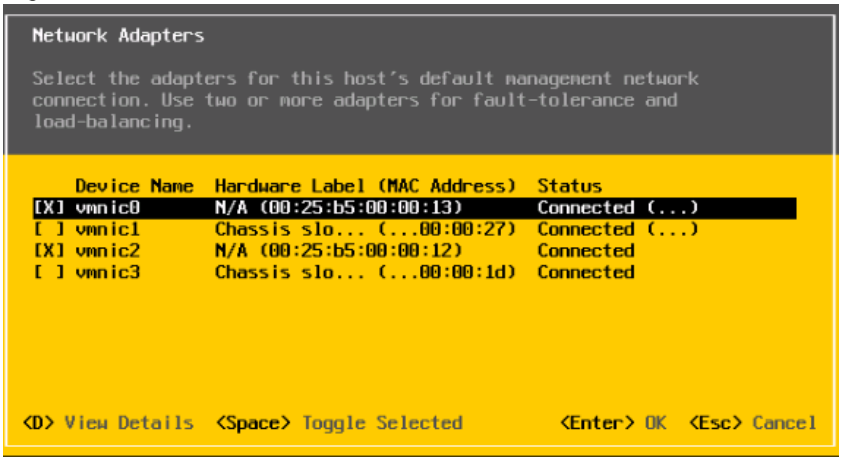
1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter <<var_mgmt_passwd>> as the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. From the Configure Management Network menu, select Network Adapters and press Enter.
5. Select the two devices that are used for Administrative traffic.
6. To identify the right devices the MAC address is the best information.
7. Select Properties Tab > Network.

**Figure 331 UCS Manager – List of Configured vNICs**




8. Compare the MAC address with the address shown in the Network Adapters View of VMware ESXi.

**Figure 332 ESXi – List of available vmnics**



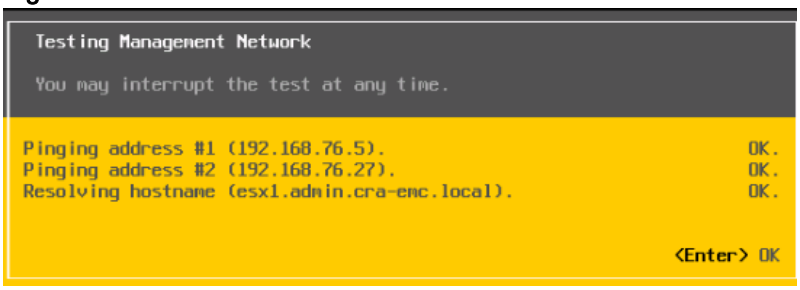
9. Press Enter.
10. Select VLAN (optional), Enter <<var_management_vlan_id>> and press Enter.
11. Select IP Configuration and press Enter.
12. Select the Set Static IP Address and Network Configuration option by using the space bar.
13. Enter the IP address for managing the first ESXi host: <<var_esxX_ip>>.
14. Enter the subnet mask <<var_mgmt_netmask>> for this ESXi host.
15. Enter the default gateway <<var_mgmt_gw>> for this ESXi host.
16. Press Enter to accept the changes to the IP configuration.
17. Select the DNS Configuration option and press Enter.



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

18. Enter the IP address of the primary <<var_nameserver_ip>> DNS server.
19. Optional: Enter the IP address of the secondary <<var_nameserver2_ip>> DNS server.
20. Enter the fully qualified domain name (FQDN) <<var_esx1_fqdn>> for this ESXi host.
21. Press Enter to accept the changes to the DNS configuration.
22. Select the IPv6 Configuration option and press Enter.
23. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
24. Press Esc to exit the Configure Management Network submenu.
25. Press Y to confirm the changes and return to reboot the server.
26. After the server is booted log in to the system.
27. Select Test Management Network to verify that the management network is set up correctly and press Enter.
28. Press Enter to run the test. Confirm results of ping.

**Figure 333 ESXi – Network Test Results**




29. Press Enter to exit the window.

30. Press Esc to log out of the VMware console.

## Register and Configure ESX Hosts with VMware vCenter

If the VMware vCenter Server is deployed as a virtual machine on an ESXi server installed as part of this solution, connect directly to an Infrastructure ESXi server using the vSphere Client. To register and configure ESX hosts with VMware vCenter, complete the following steps:

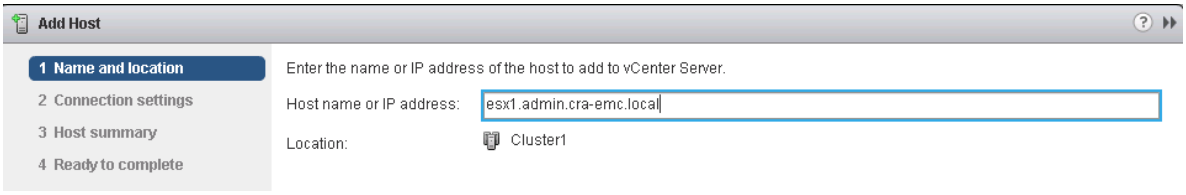
1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.

2. Logon as root and the password <<var_mgmt_passwd>>.

3. Click Hosts and Clusters.

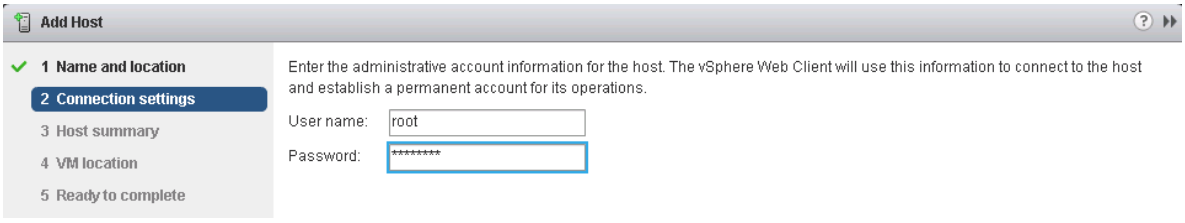
4. Right-Click <<var_vc_cluster1_name>> and select Add Host.

5. Enter <<var_esx1_fqdn>> in the Hostname or IP Address field.



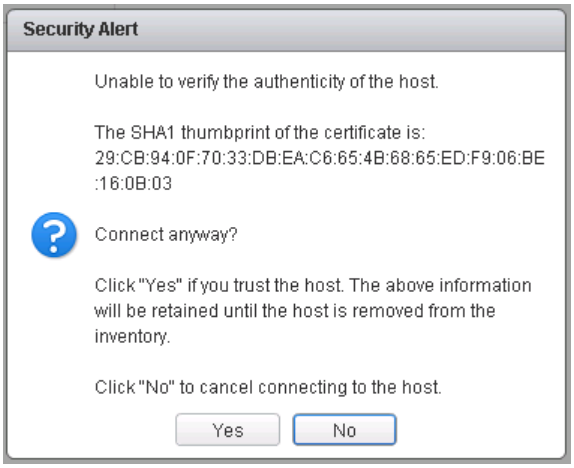

6. Click Next.

7. Enter root as the User name and <<var_mgmt_passwd>> as the Password.

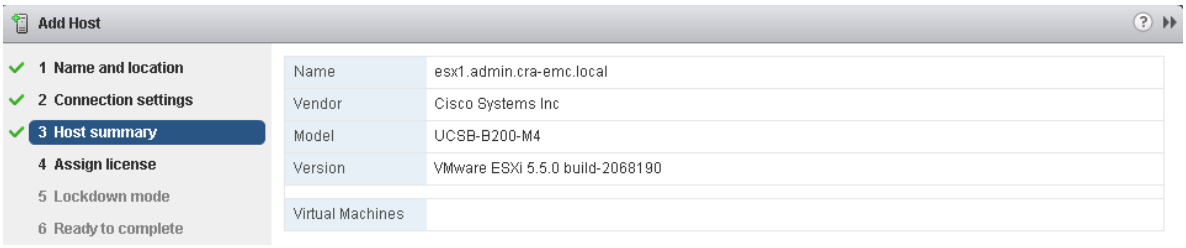



8. Click Next.

9. Click Yes to Accept the Certificate.

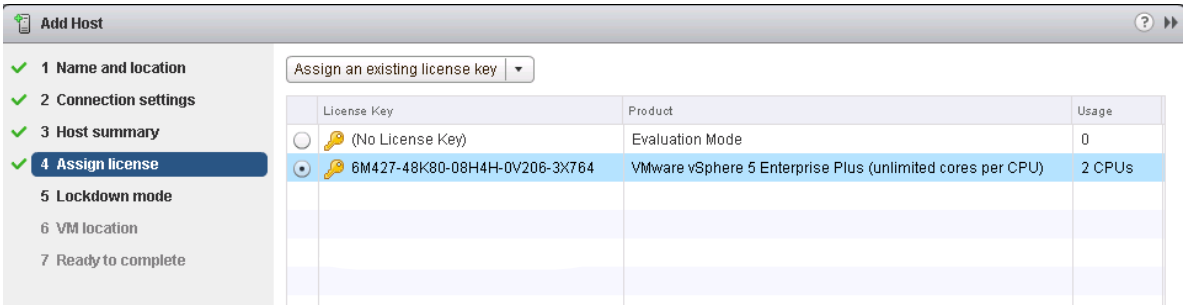



10. Review the Host Summary and click Next.



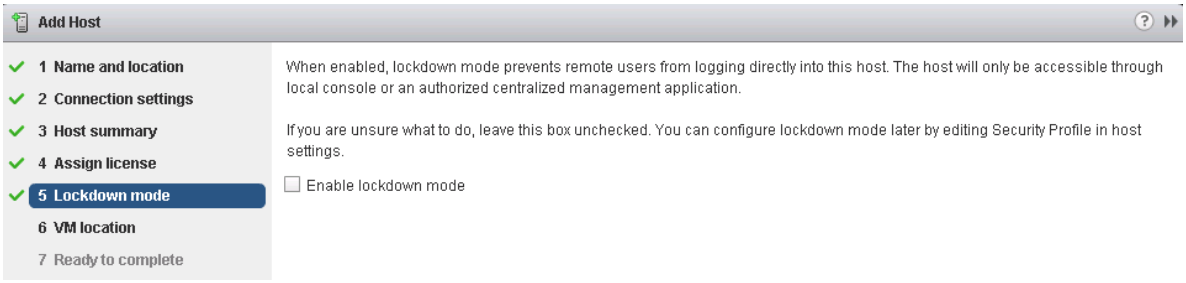

11. Select a License Key to be used by this host.

12. Click Next.



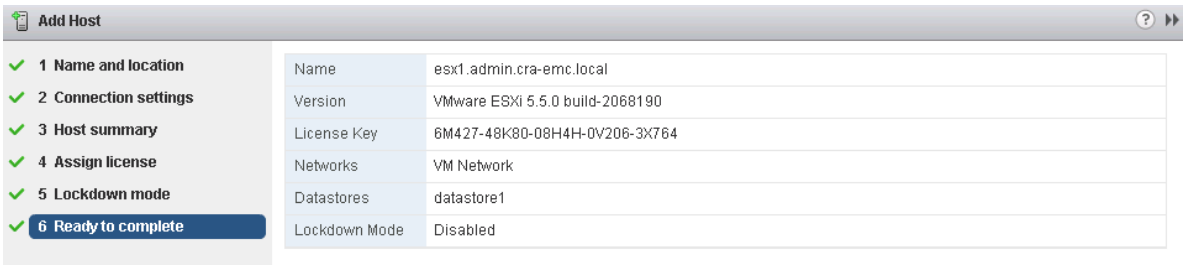

13. Leave the Check-Box for Lockdown Mode unchecked.

14. Click Next.




15. On the VM Location Screen click Next.

16. Review the Information and click Finish.



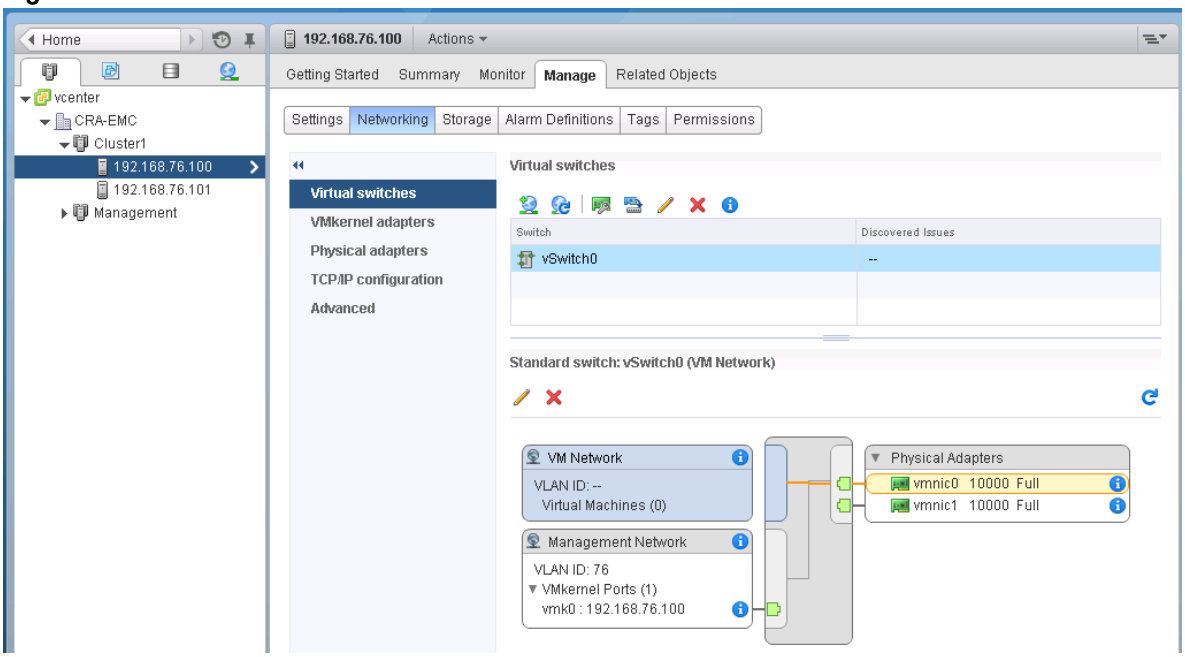

17. Repeat this step with all ESX hosts installed to run in Cluster 1.

## Configure Basic Networking on the ESX Hosts

Only the VMkernel networks for NFS and vMotion traffic must be defined. To configure the basic networking on the ESX hosts, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. In the Home screen, click Hosts and Clusters.
4. Click <<var_esx1_fqdn>> on the left pane.
5. Click Manage tab in the right pane.
6. Click Networking.
7. Click Virtual switches.

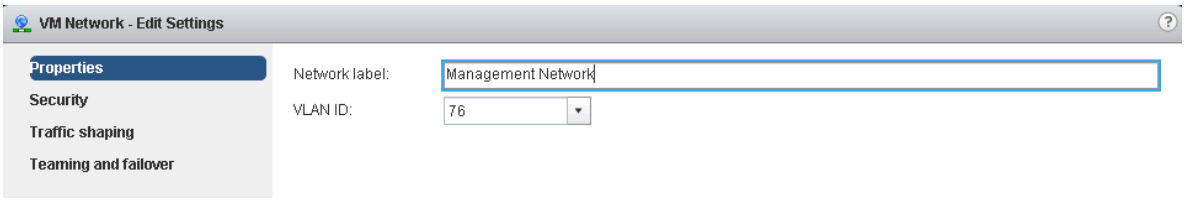
**Figure 334 Virtual Center – Virtual Switches View**




8. Select Management Network.
9. Click the Pencil Icon.
10. Change the Network Label to <<var_vmkern_mgmt_name>>.
11. Click OK.



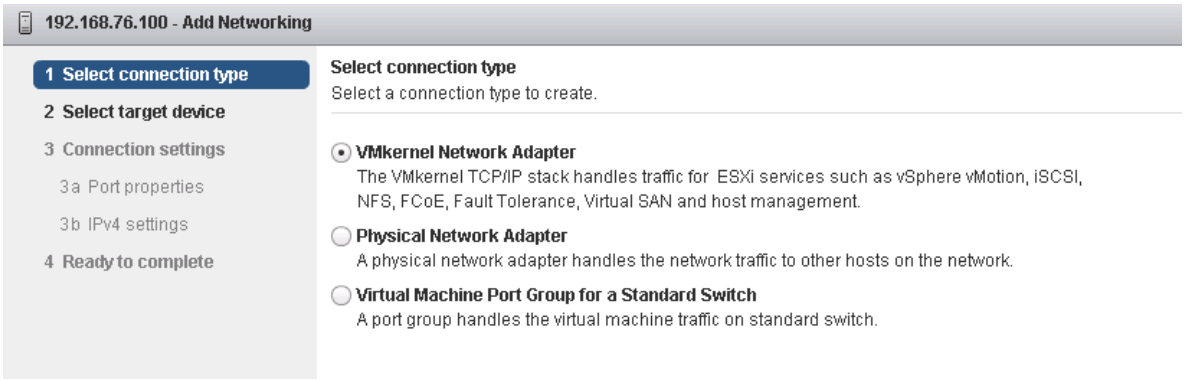

12. Select VM Network.
13. Click the Pencil Icon.
14. Change the Network label to <<var_esx_mgmt_network>>.
15. Change the VLAN ID to <<var_managment_vlan_id>>.
16. Click OK.




17. Click the  Icon.

18. Select VMkernel Network Adapter.

19. Click Next.



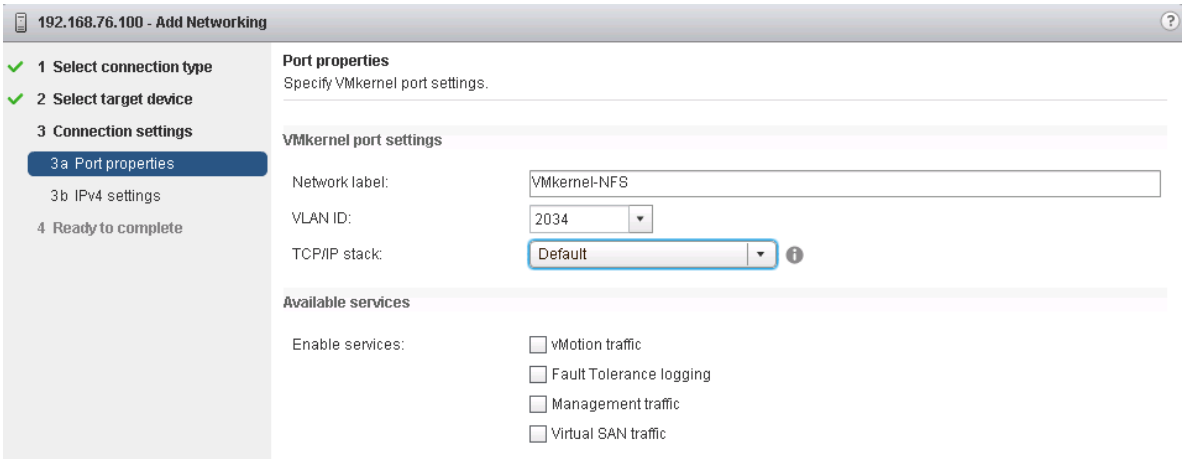

20. On the Select Target Device Screen the use of vSwitch0 should be selected by default.

21. Click Next.

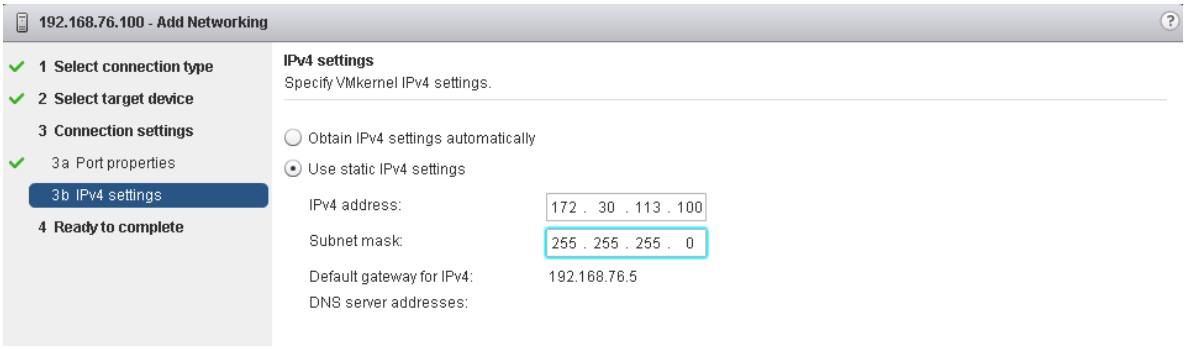
22. Enter <<var_esx_vmkernel_nfs>> as the Network label.

23. Enter <<var_esx_nfs_vlan_id>> as the VLAN ID.

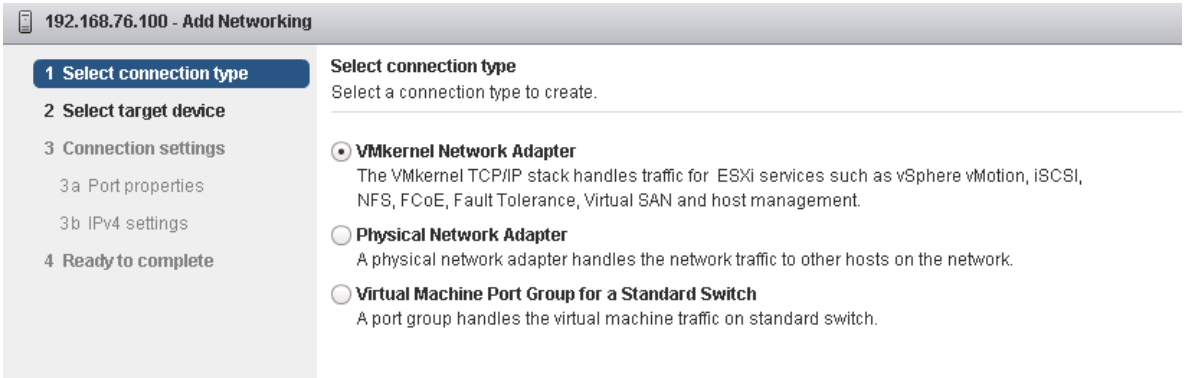
24. Click Next.



25. Select Use Static IP.
26. Enter <<var_esx1_nfs_ip>>.
27. Enter <<var_nfs_netmask>>.
28. Click Next.

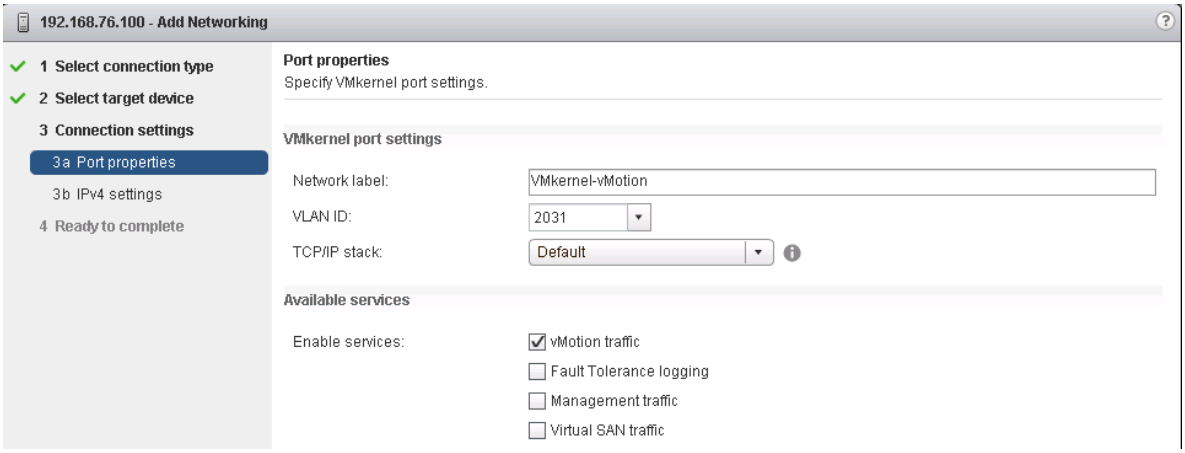



29. Review the Information.
30. Click Finish.
31. Click the  Icon.
32. Select VMkernel Network Adapter.
33. Click Next.




34. On the Select Target Device Screen the use of vSwitch0 should be selected by default.
35. Click Next.
36. Enter <<var_esx_vmkernel_vmotion>> as the Network label.
37. Enter <<var_vmotion_vlan_id>> as the VLAN ID.

38. Click Next.

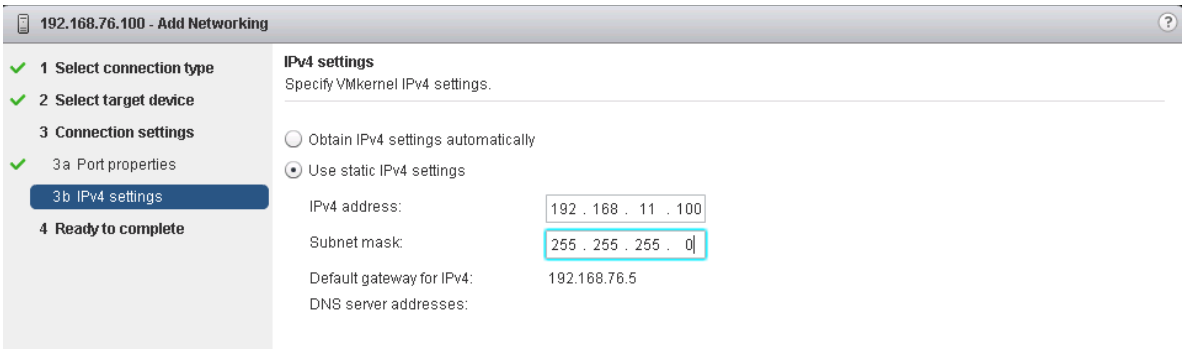



39. Select Use Static IP.

40. Enter <<var_esx1_vmotion_ip>>.

41. Enter <<var_vmotion_netmask>>.

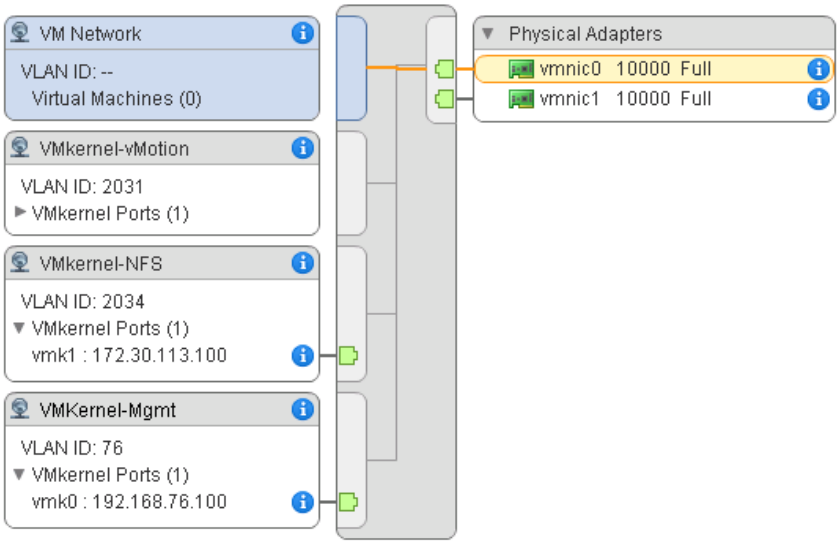
42. Click Next.




43. Review the Information.

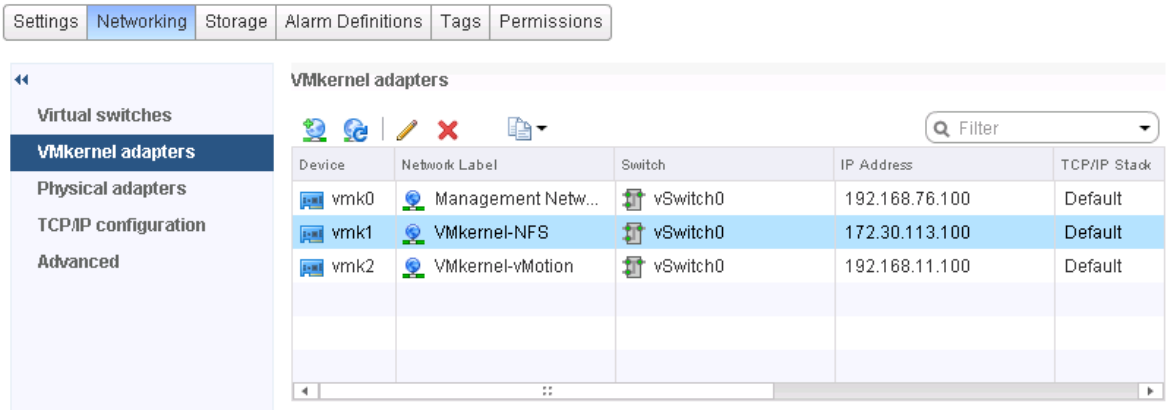
44. Click Finish.

The Virtual Switch Graph should look like the screenshot below:




45. Click VMkernel Adapters.

46. Click vmk1.

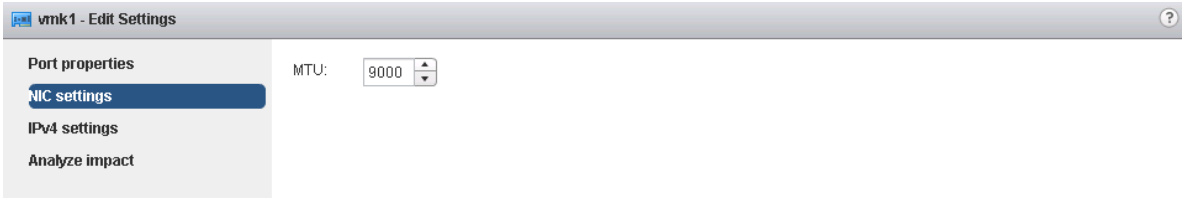



47. Click the Pencil icon.

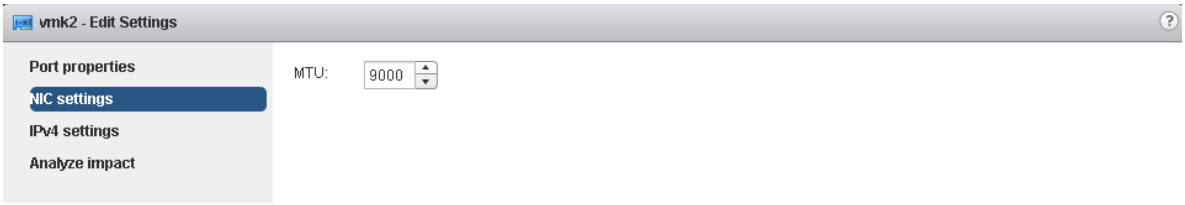
48. Click NIC Settings.

49. Enter 9000 in the MTU field.

50. Click OK.



51. Click vmk2.
52. Click the Pencil icon.
53. Click NIC settings.
54. Enter 9000 in the MTU field.

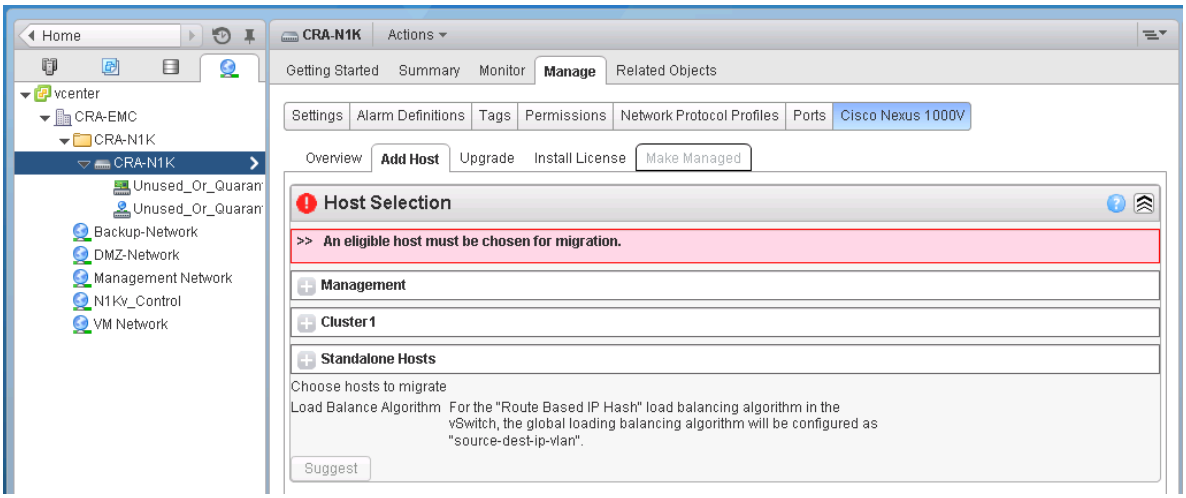



55. Click OK.

## Add Hosts to Cisco Nexus1000V

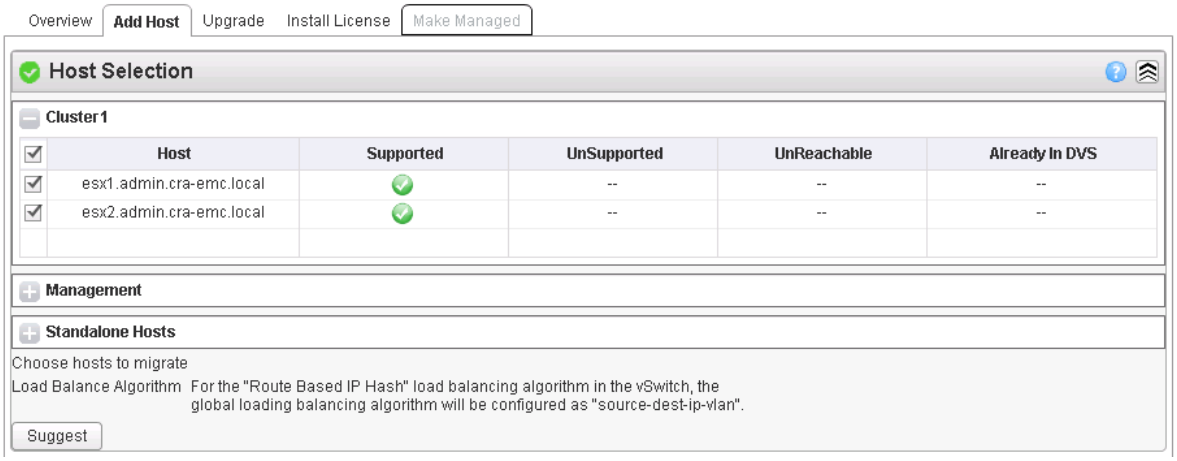
In this section, add the ESX-Hosts to the Cisco Nexus1000V and configure the administrative networks on the VSM using the Cisco Virtual Switch Update Manager. To add hots to Cisco Nexus 1000V, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Log in as root and the password <<var_mgmt_passwd>>.
3. In the Home screen, click Networking.
4. Click the Virtual Distributed Switch <<var_n1k_switch_name>>.
5. Click Cisco Nexus 1000V in the right pane.
6. Click Add Hosts.
7. Click the + Sign left of Cluster 1.




8. In the Host Section, select the hosts.

9. Click Suggest.

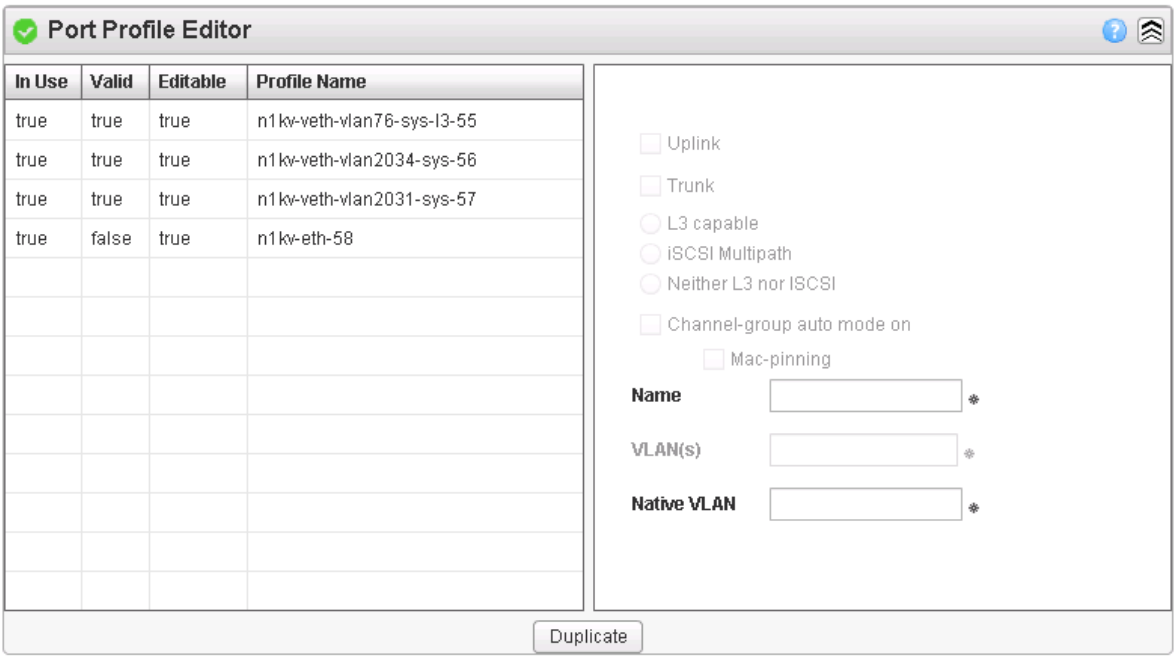



10. In the Port Profile Editor Section all required port-groups must be shown.

---

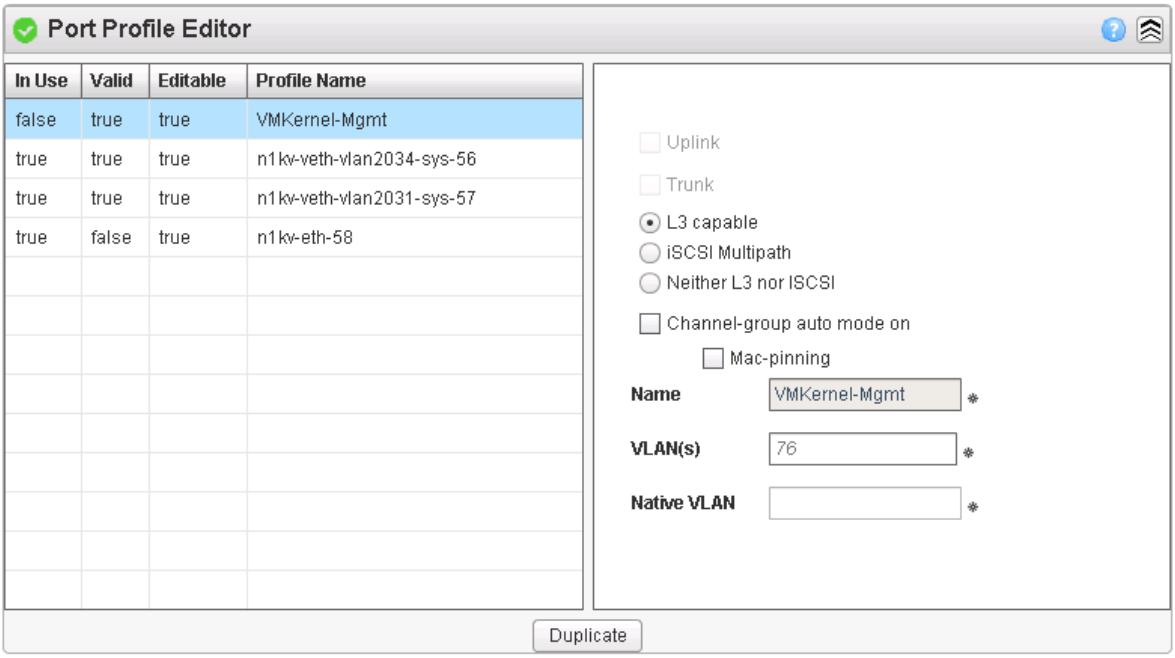
*vlan76* for the VMKernel-Mgmt network, *vlan2034* for the VMKernel-NFS for the NFS network and *vlan2031* for the vMotion network. The *-eth-* is the uplink network.

---



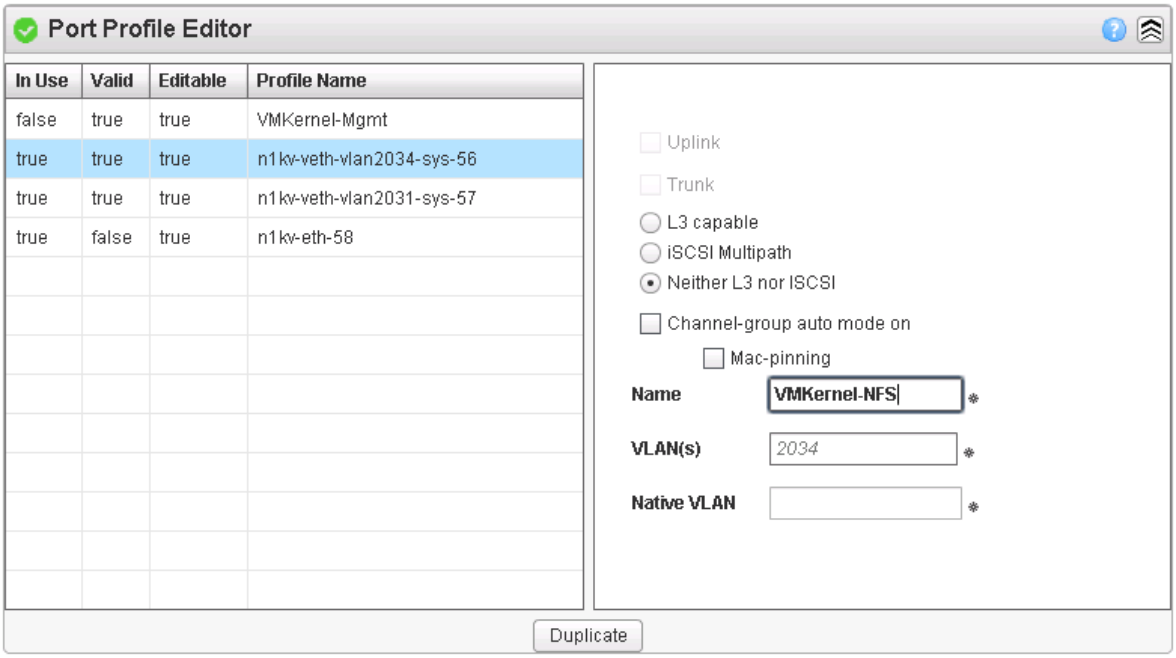

11. Select the line with includes <<var_management_vlan_id>> in the Profile Name.

12. Change the Name to <<var_vmkern_mgmt_name>>.



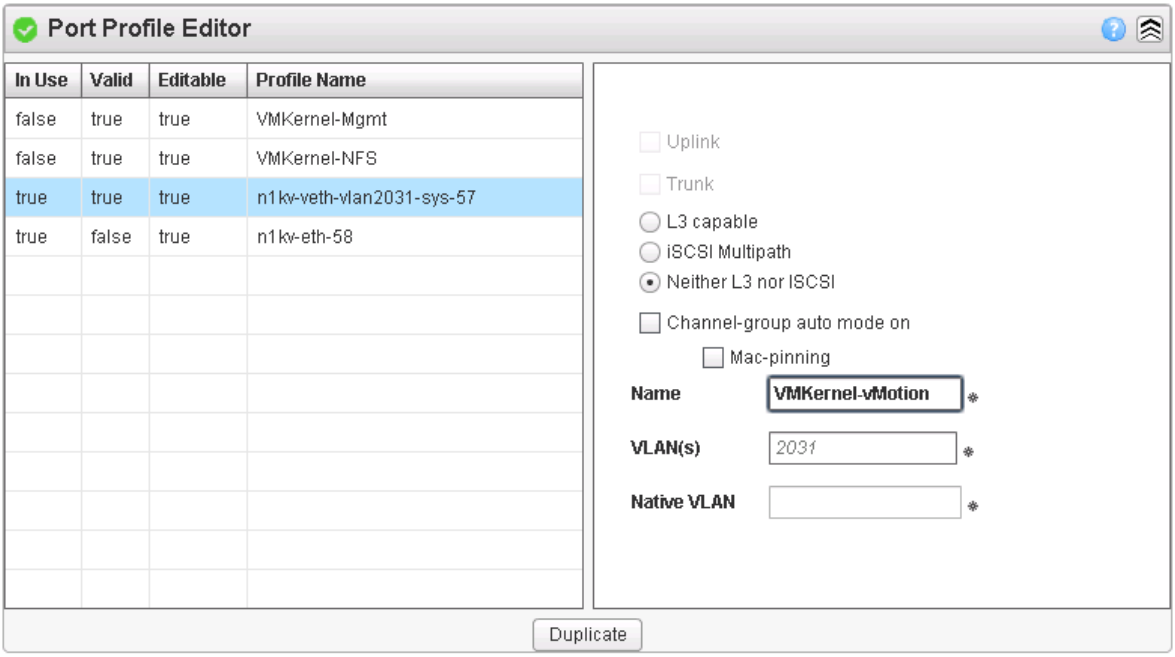

13. Select the line with includes <<var_nfs_vlan_id>> in the Profile Name.

14. Change the Name to <<var_esx_vmkernel_nfs>>.

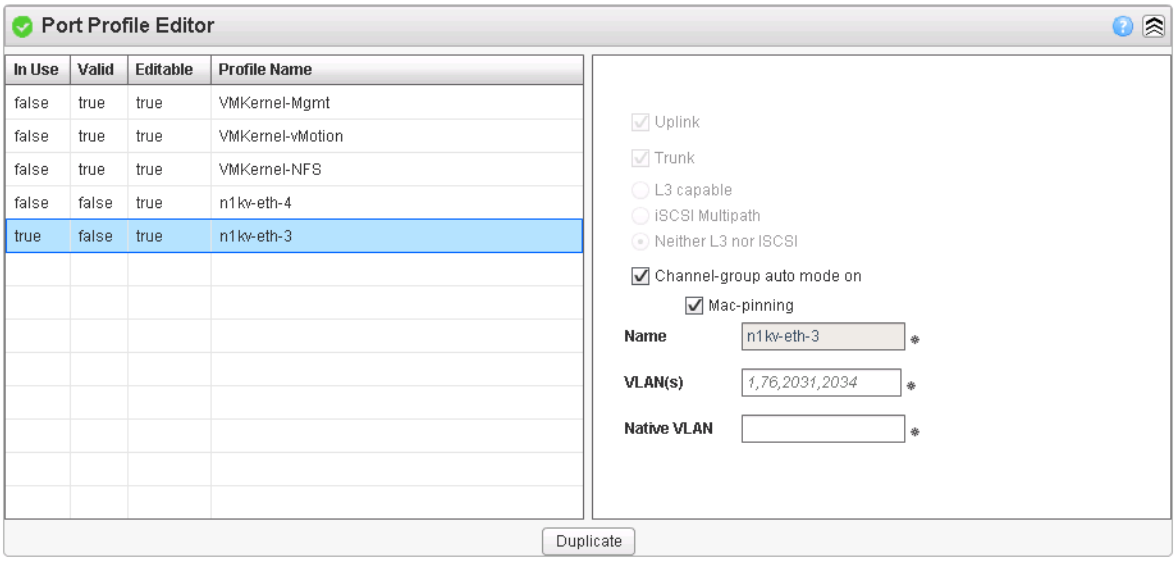



15. Select the line with includes <<var_vmotion_vlan_id>> in the Profile Name.

16. Change the Name to <<var_esx_vmkernel_vmotion>>.




17. Select the line with n1kv- in the Profile Name that is listed as In Use = true.

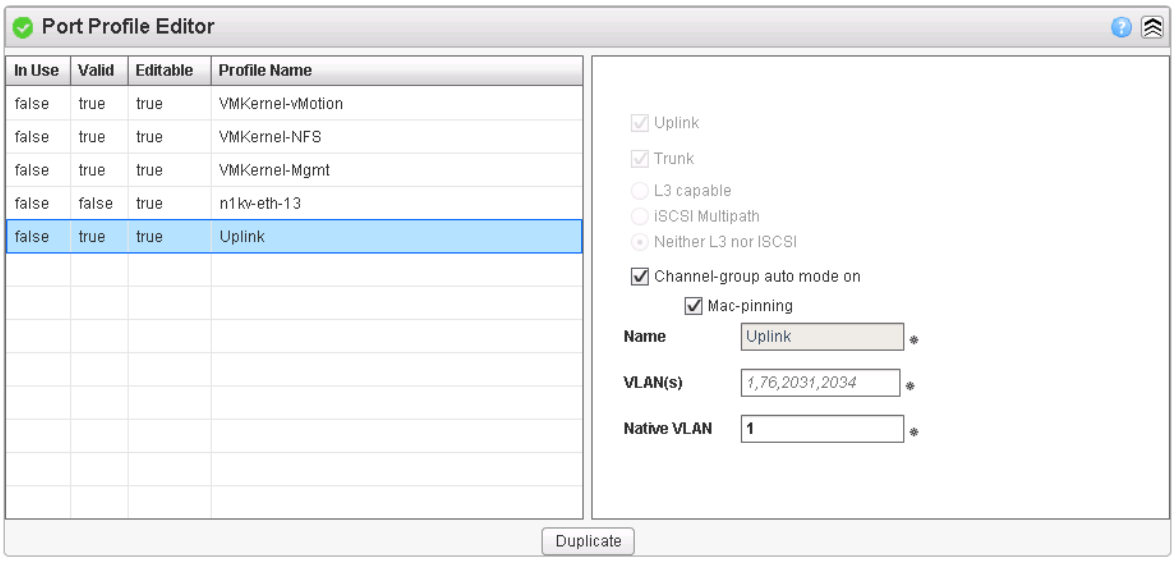



18. Change the Name to Uplink.

19. Change the VLAN to 1,76,2031,2034.

20. Remove 1 from the VLAN(s) list.

21. Enter 76 as the Native VLAN.

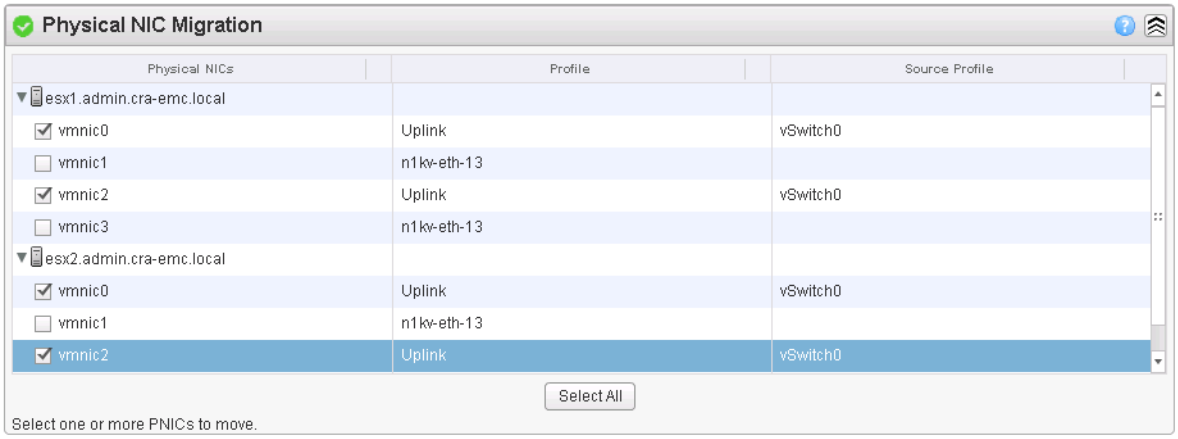



The warning message “No validation message is available” displays since the name changed.

22. Leave the second n1kv-eth-* Profile as is.

23. In the Physical NIC Migration section, select Uplink as the Profile for all vmnic’s with the Source Profile vSwitch0.

24. Do not change the settings for vmnic's without a Source Profile.



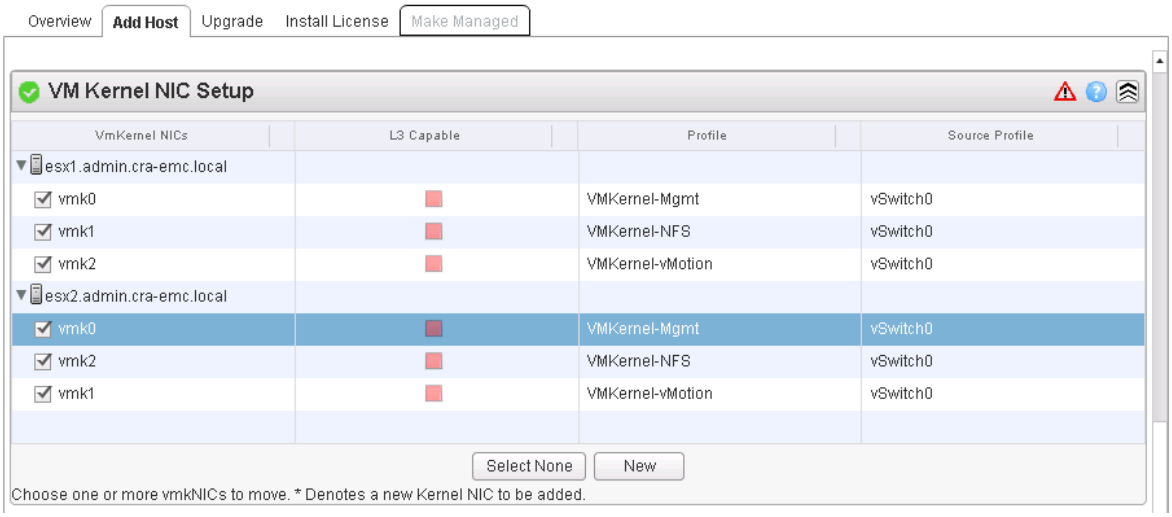

25. In the VM Kernel NIC Setup section, select the <<var_vmkern_mgmt_name>> Profile for vmk0.

26. In case <<var_vmkern_mgmt_name>> is not listed in the drop down menu, scroll up to the Port Profile Editor section, select <<var_vmkern_mgmt_name>> and click the Radio-Button for Neither L3 nor ISCSI.

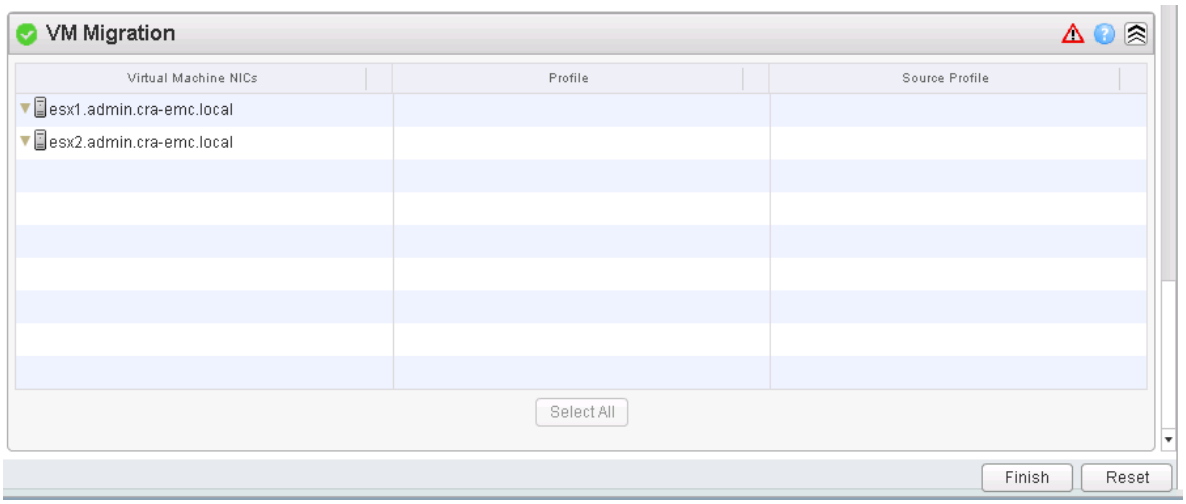
27. Select the <<var_vmkern_mgmt_name>> for vmk0 and change the Port-Profile back to L3 capable.

28. Select the <<var_esx_vmkernel_vmotion>> profile for vmk1.

29. Select the <<var_esx_vmkernel_nfs>> profile for vmk2.

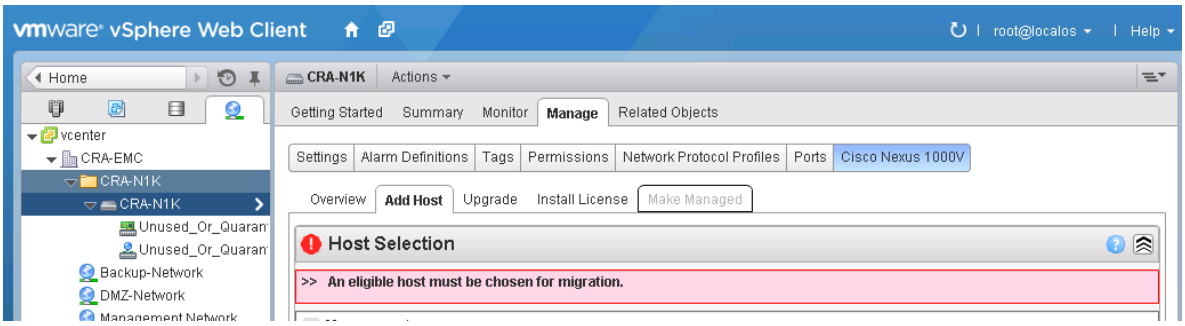



Since there are no Virtual Machines the VM Migration list is empty.

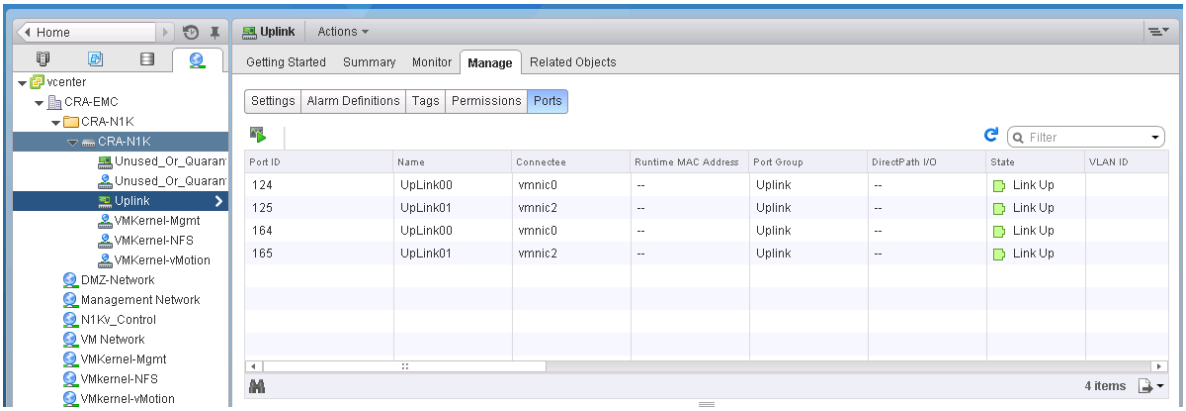



30. Click Finish.

31. Click the Refresh Icon.

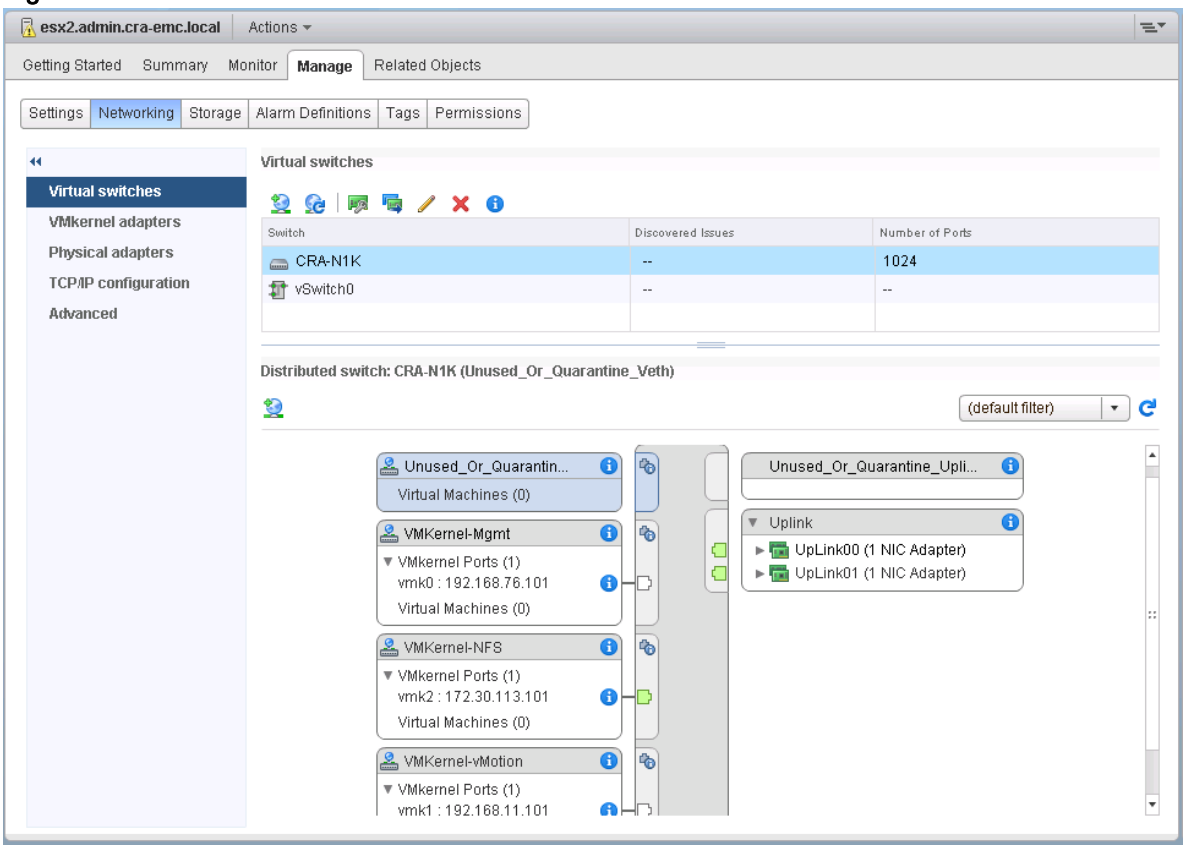



The new network configuration is listed on the left pane.




In the Networking Section of the ESX-Hosts, the new configuration is displayed.

**Figure 335 Virtual Center – Virtual Switches View with Nexus1000V**




Since the hosts lost the network connection to vCenter as part of the migration process, all hosts are listed with the Bang-Sign for errors. Acknowledge all the errors and reset them back to normal status.

To integrate the Cisco Nexus 1000V into the Cisco UCS Performance Manager, it is required to configure the SNMP Community String on the Cisco Nexus 1000V VSM. To configure the SNMP Community String, complete the following steps:

1. Use SSH to <<var_n1k_vsm_ip>> to log in to the Cisco Nexus 1000V VSM.
2. Log in as admin and the password <<var_mgmt_passwd>>.

```
CRA-N1K# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CRA-N1K(config)# snmp-server community monitor ro
```

3. Save the running configuration to start-up.

```
CRA-N1K(config)# copy run start
```

For all VLANs in the Datacenter Reference Architecture a Port-Profile is required on the Cisco Nexus 1000V VSM. For the Management Network with the VLAN ID <<var_mgmt_vlan_id>> the following commands are used to configure the Port-Profile:

4. Use SSH to <<var_n1k_vsm_ip>> to log in to the Nexus 1000V VSM.
5. Log in as admin and the password <<var_mgmt_passwd>>.

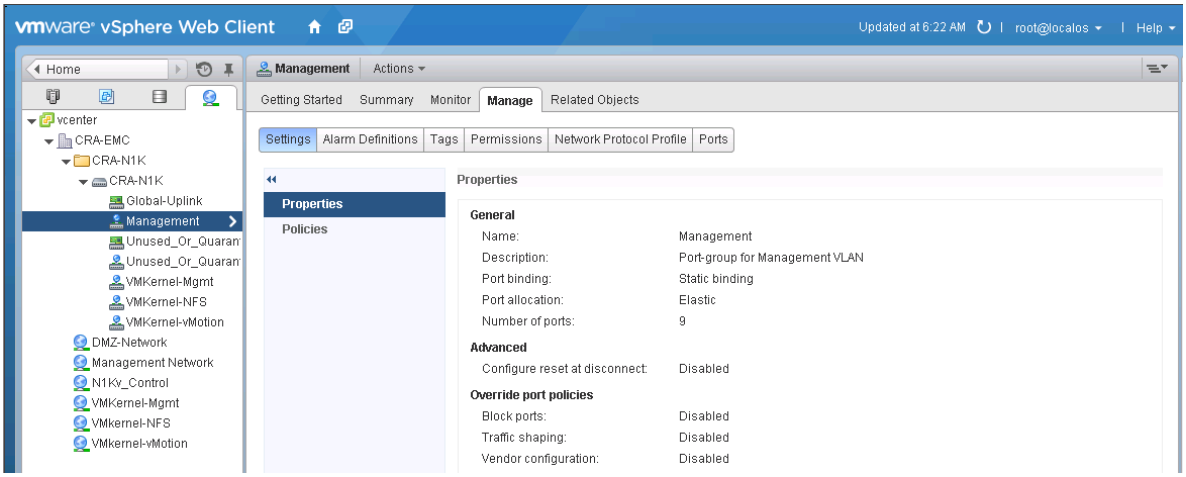
```
CRA-N1K# conf t
Enter configuration commands, one per line.  End with CNTL/Z.


port-profile type vethernet <<var_n1k_mgmt_pp-name>>
  description Port-group for Management VLAN
  state enabled
  vmware port-group
  switchport mode access
  switchport access vlan <<var_mgmt_vlan_id>>
  port-binding static auto expand
  no shut
  exit
exit
```

6. Save the running configuration to start-up.

```
copy run start
```

The new defined Port-Profile is visible in the vSphere Web Client.



## Connect VLAN-Groups to Cisco Nexus1000V

In this section, you will add the VLAN-Group Client-Zone to the Cisco Nexus1000V using the Cisco Nexus1000V plugin in the VMware vSphere Web Client and on the Cisco Nexus1000V VSM console. For every VLAN-Group in the Cisco UCS domain dedicated vNICs, vmnic's and port-groups are required. You have to repeat the steps in the section for every VLAN-Group that is defined.

To create a Port-Profile on the Cisco Nexus1000V, complete the following steps:

1. Open a SSH tool and connect to <<var_n1k_vsm_ip>>.
2. On the VSM enter configuration mode:

```
conf t
```

3. Create the Port-Profile:

```
port-profile type ethernet <<var_n1k_client_pp_name>>
mtu 9000
switchport mode trunk
switchport trunk allowed vlan 2
switchport trunk native vlan 2
channel-group auto mode on mac-pinning
vmware port-group
no shutdown
state enabled
```

4. Save the running configuration to start-up:

```
copy running-config startup-config
```

5. Validate the configuration:

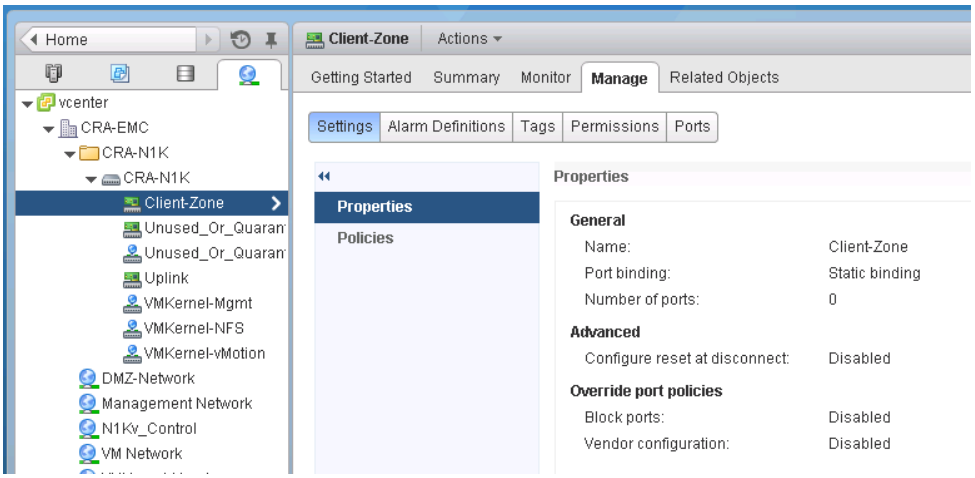
```
CRA-N1K(config)# show port-profile

port-profile Client-Zone
 type: Ethernet
 description:
 status: enabled
 max-ports: 512
 min-ports: 1
```

```
  inherit:
  config attributes:
   mtu 9000
   switchport mode trunk
   switchport trunk allowed vlan 2
   switchport trunk native vlan 2
   channel-group auto mode on mac-pinning
   no shutdown
  evaluated config attributes:
   mtu 9000
   switchport mode trunk
   switchport trunk allowed vlan 2
   switchport trunk native vlan 2
   channel-group auto mode on mac-pinning
   no shutdown
  assigned interfaces:
  port-group: Client-Zone
  system vlans: none
  capability l3control: no
  capability iscsi-multipath: no
  capability vxlan: no
  capability l3-vservice: no
  port-profile role: none
  port-binding: static

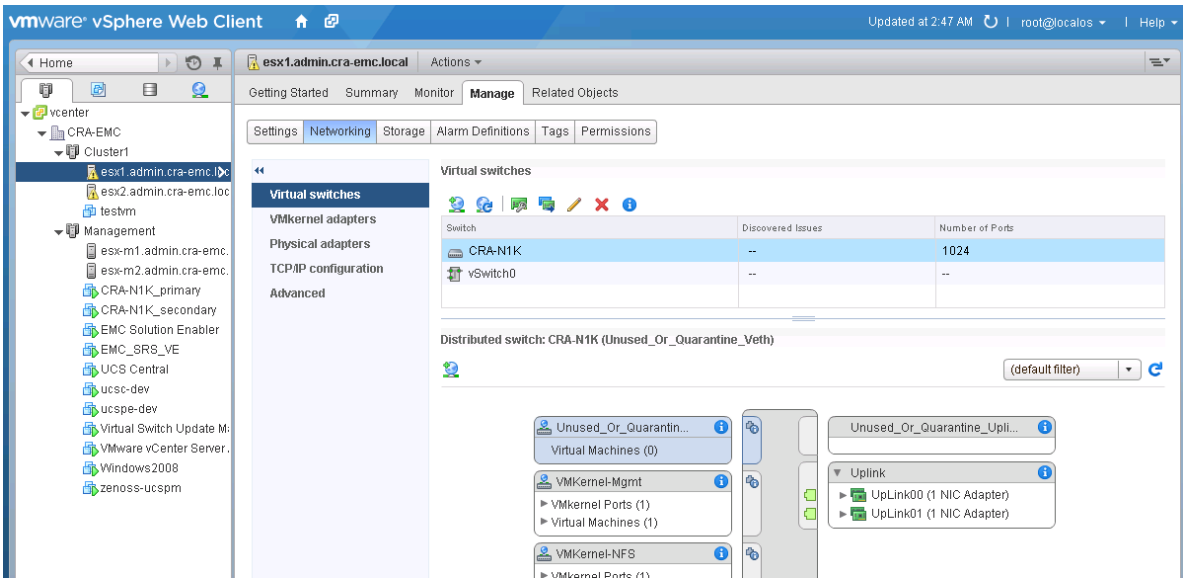
CRA-N1K(config)#
```

You can view new Port-Profile in the VMware vSphere Web Client.



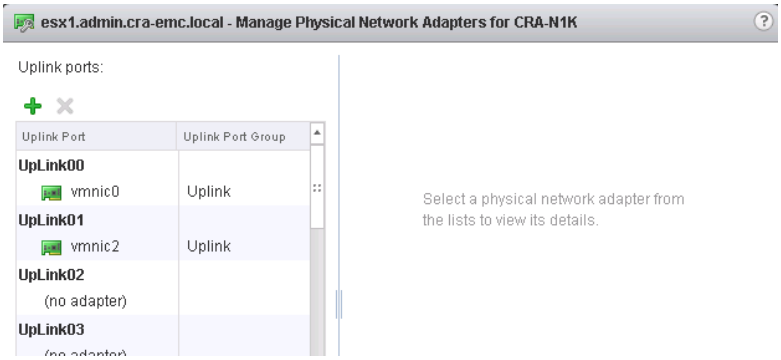

To add VMware vmnic's to the created Port-Profile, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. In the Home screen, click Hosts and Clusters.
4. Click the ESX host <<var_esxX_fqdn>>.
5. In the right pane click Manage Tab and Networking.
6. Select Virtual Switches and <<var_n1k_vsm_name>>.




7. Click the  Icon for, Manage physical network adapters.

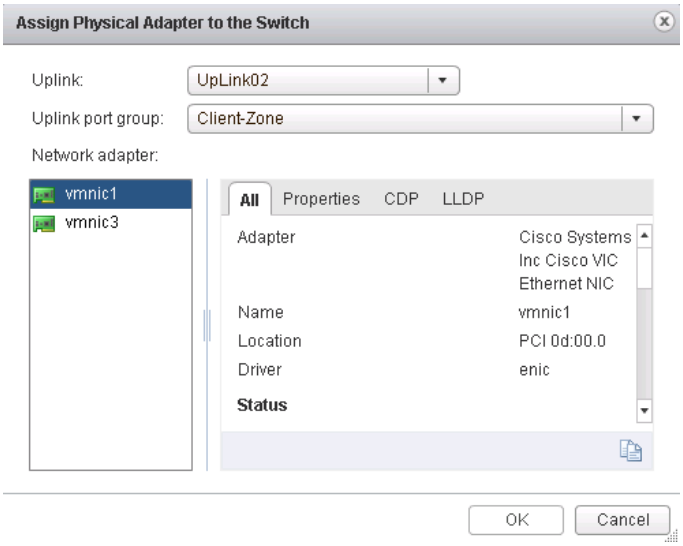
8. In the new window click the +-Icon.




9. Select one vmnic from the list of Network Adapters.

10. Select <<var_n1k_client_pp_name>> from the Uplink port group drop-down menu.

11. Click OK.

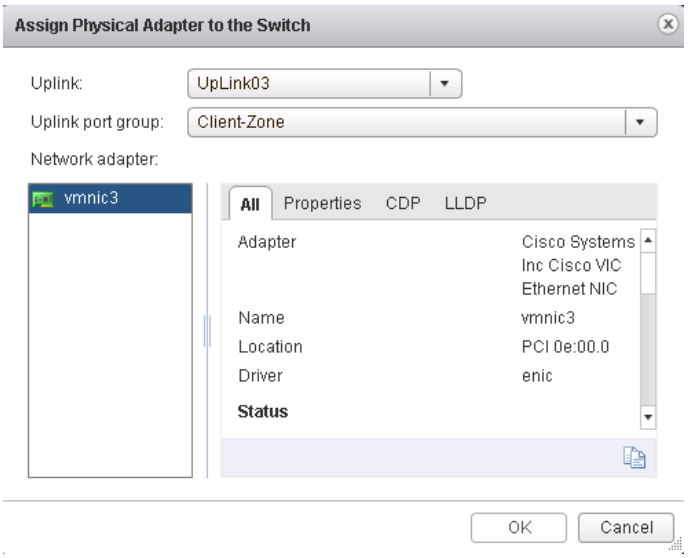



12. Click the +-Icon.

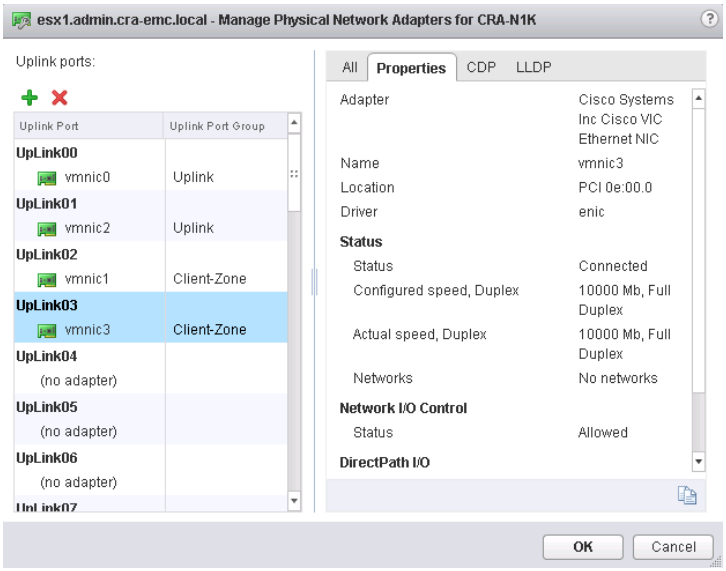
13. Select one vmnic from the list of Network Adapters.

14. Select <<var_n1k_client_pp_name>> from the Uplink port group drop-down menu.

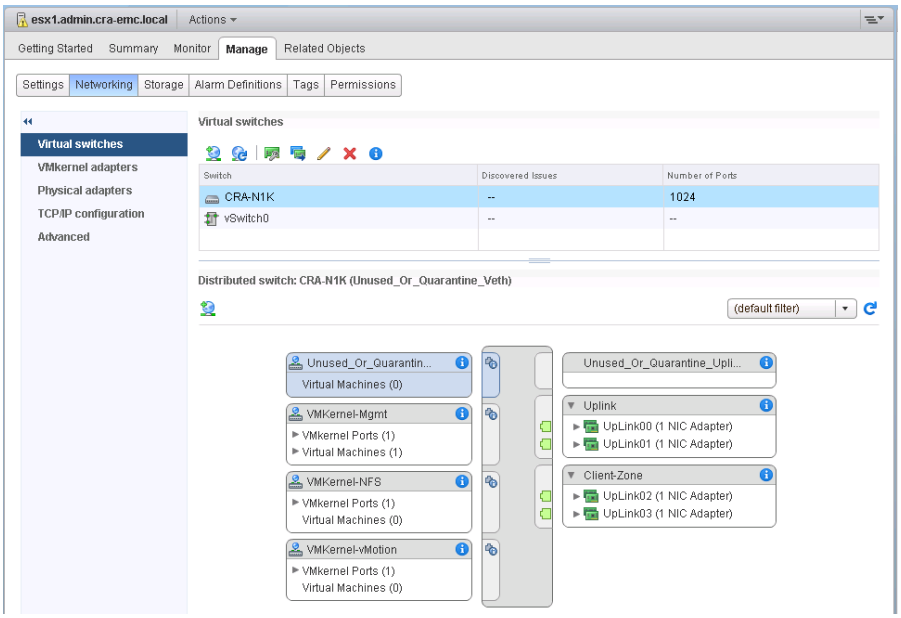
15. Click OK.




16. Click OK.

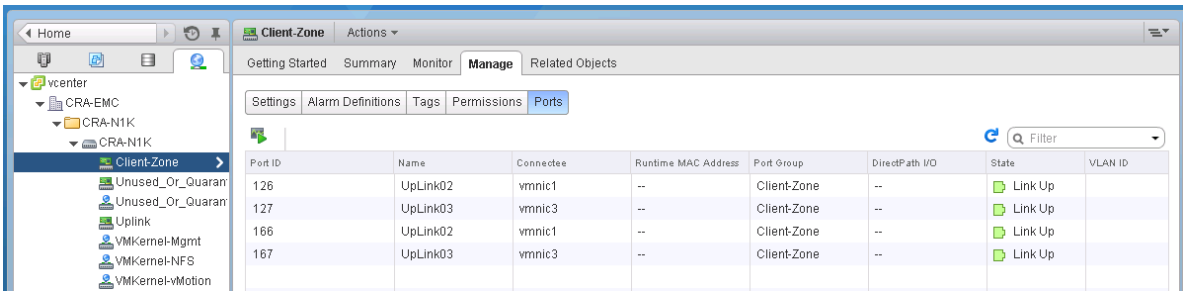



The vmnic's are shown as connected in the Client-Zone.




17. Repeat Step 4 – 17 for the other ESX hosts.

18. Validate the Ports status of the Client-Zone in the Networking section of the VMware vSphere Web Client.




## Configure Cisco Nexus 1000V

There are additional configurations required after the first hosts are connected to the Cisco Nexus1000V VSM.

Use SSH to log on to the VSM module and complete the following steps:

1. Open a SSH tool and connect to <<var_n1k_vsm_ip>>

2. On the VSM enter configuration mode:

```
conf t
```

3. The default configuration of the Uplink ports done by the Virtual Switch Update Manager is with MTU1500 only. For the NFS traffic Jumbo Frame support is required.

```
port-profile Uplink
```

```
mtu 9000
no shut
```

4. Save the running configuration to start-up:

```
copy running-config startup-config
```

5. Validate the configuration:

```
CRA-N1K(config)# show port-profile name Uplink

port-profile Uplink
 type: Ethernet
 description:
 status: enabled
 max-ports: 512
 min-ports: 1
 inherit:
 config attributes:
  mtu 9000
  switchport mode trunk
  switchport trunk allowed vlan 1,76,2031,2034
  switchport trunk native vlan 1
  channel-group auto mode on mac-pinning
  no shutdown
 evaluated config attributes:
  mtu 9000
  switchport mode trunk
  switchport trunk allowed vlan 1,76,2031,2034
  switchport trunk native vlan 1
  channel-group auto mode on mac-pinning
  no shutdown
 assigned interfaces:
  port-channel1
```

```
    port-channel2
    Ethernet3/1
    Ethernet3/3
    Ethernet4/1
    Ethernet4/3
  port-group: Uplink
  system vlans: 76,2031,2034
  capability l3control: no
  capability iscsi-multipath: no
  capability vxlan: no
  capability l3-vservice: no
  port-profile role: none
  port-binding: static


CRA-N1K(config)#
```

To allow the virtual machines access to the Software share on the Storage you have to configure a Port-Profile for the NFS network.

1. Log in to the Nexus1000V VSM, enter the configuration mode and use the following commands to setup the port-profile:

```
port-profile type veth <<var_n1k_nfs_pp_name>>
  vmware port-group
  switchport mode access
  switchport access vlan 2034
  port-binding static auto expand
  state enabled
  no shutdown
```

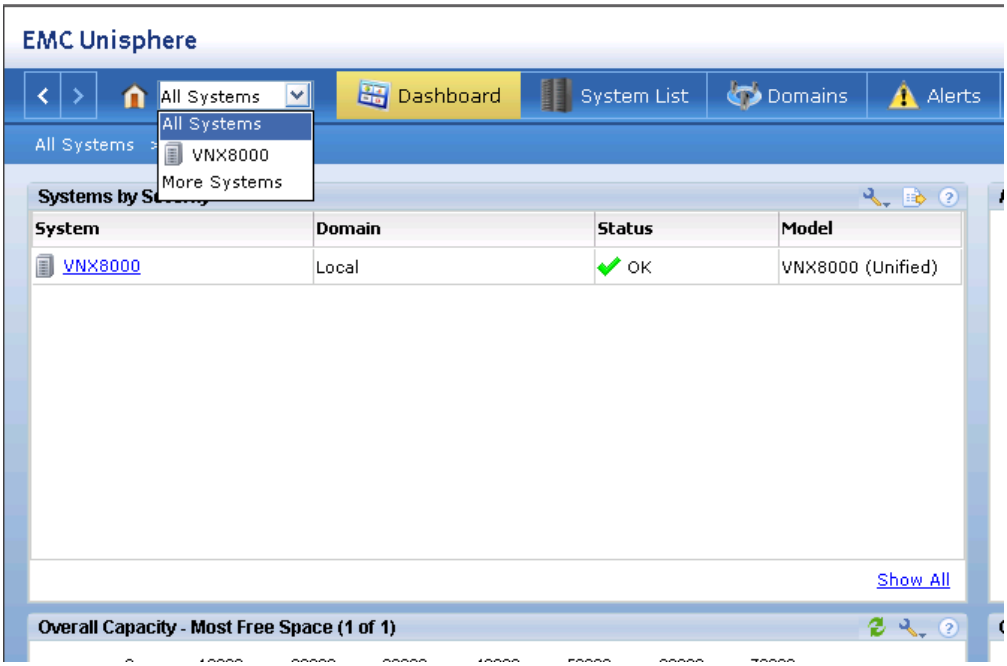
2. Save the running configuration as startup-configuration:

```
copy run start
```

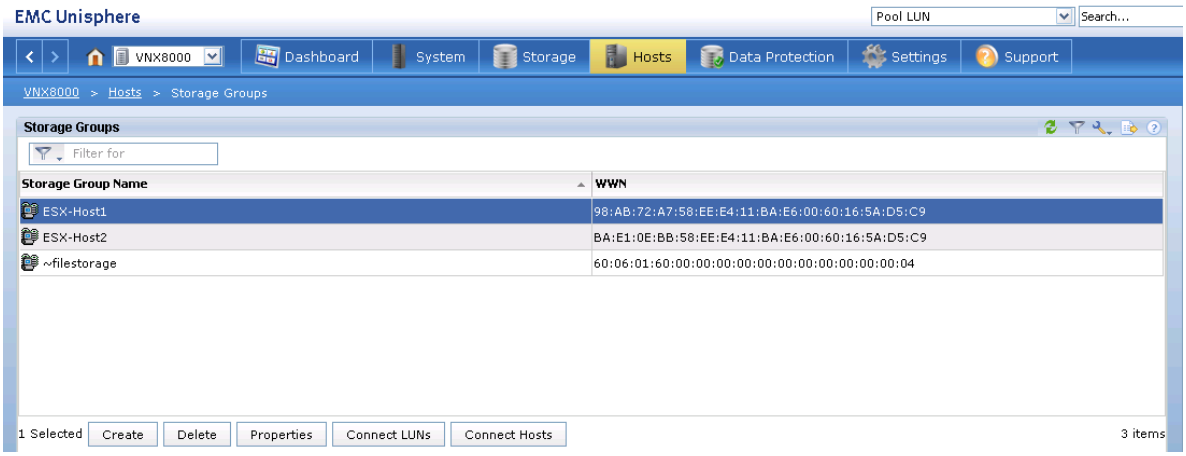
## Configure Storage Groups for Virtual Machine Templates

Now that VMware ESXi is installed, the LUN created on the VNX storage array to host the Virtual Machine Templates can be added to the Storage Groups. To configure the storage group, complete the following steps:

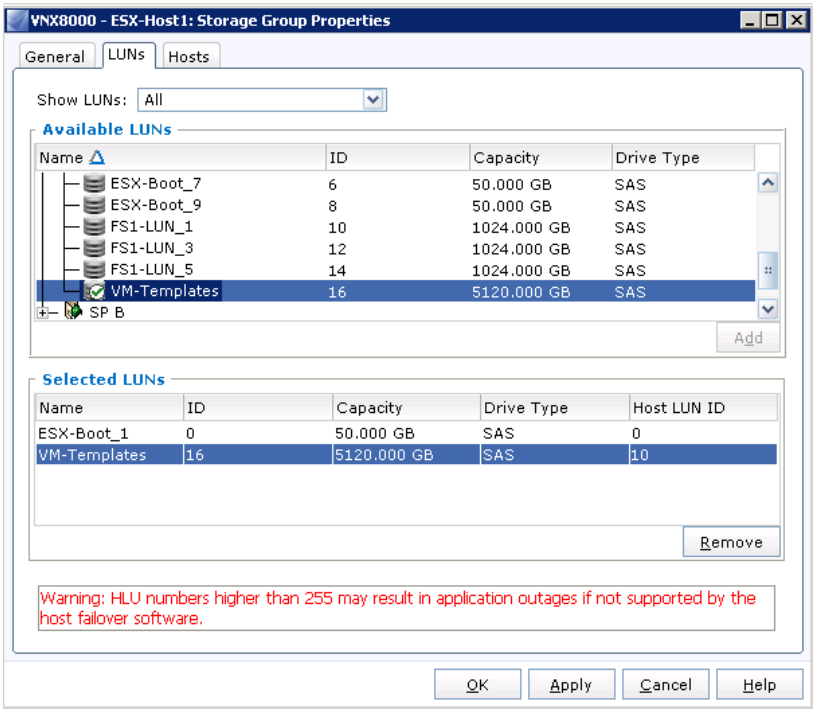
1. Open a Web Browser and connect to EMC VNX Unisphere
2. From the drop-down menu select the VNX <<var_vnx1_name>>.



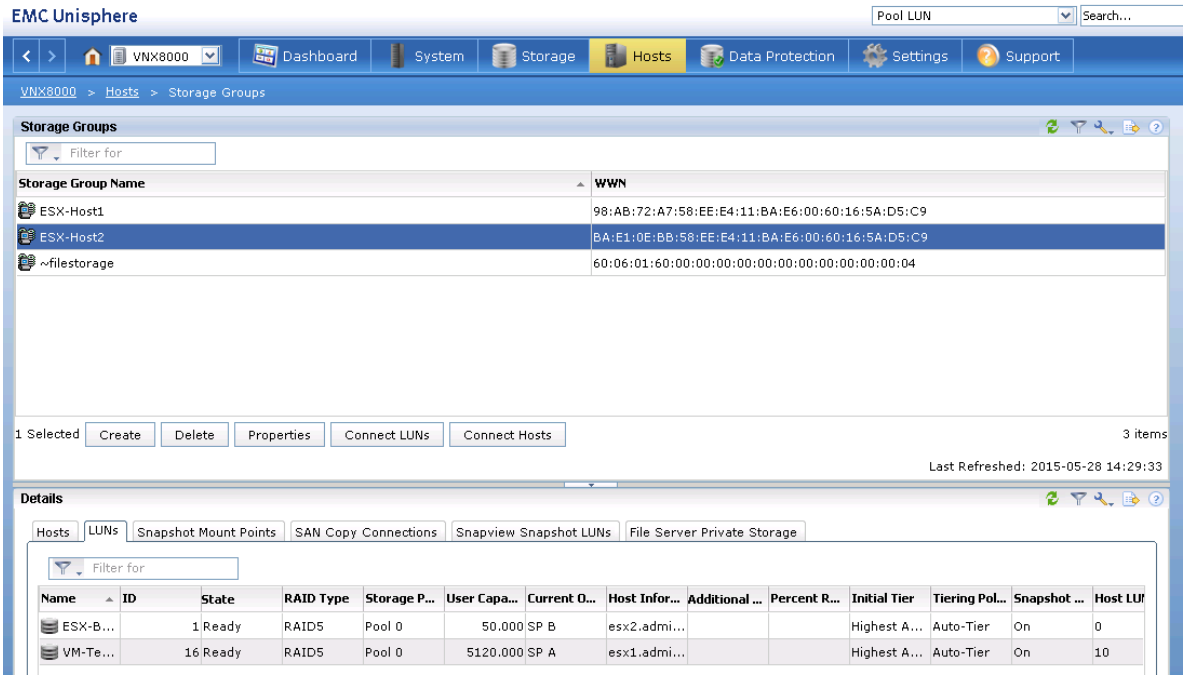

3. Click Hosts.
4. Click Storage Groups.
5. Click an existing storage group for an ESX Host.
6. Click Properties.




7. Click LUNs tab.
8. Select All from the drop-down menu for Show LUNs.
9. Click OK in the Message window.
10. Select VM-Templates LUN from the List.
11. Click Add.
12. Select the VM-Templates LUN now in the Selected LUNs section.
13. Select 10 as the Host LUN ID.
14. Click OK.
15. Click Yes in the Confirm Window.
16. Click OK.



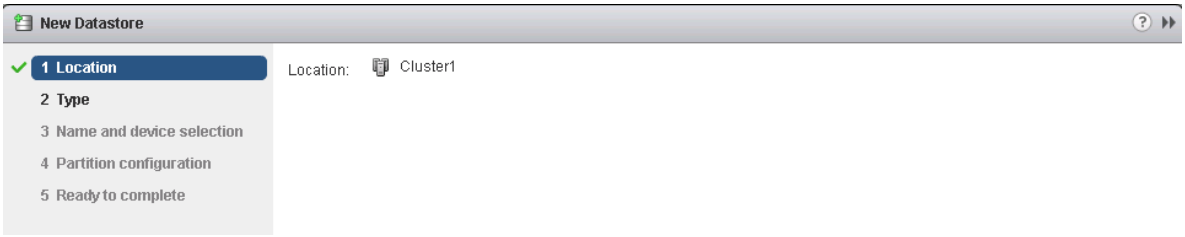

17. Repeat these steps for all five servers. The result will look like the screen shot below:




## Mount Datastores

In this section, mount the NFS share created for Software images and the LUN created for VM-Templates on the VNX storage to the ESX hosts. To mount the datastores, complete the following steps:

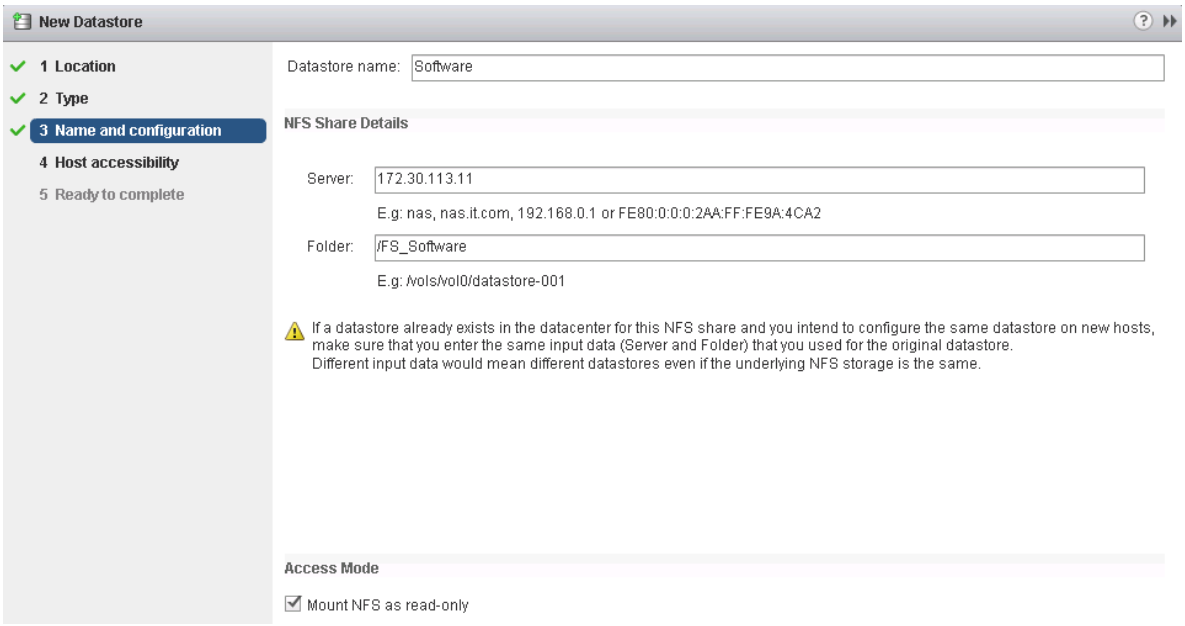
1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click <<var_vc_cluster1_name>>.
5. Click Actions > New Datastore.
6. On the Location Page, click Next.




7. Select NFS as the Type.
8. Click Next.

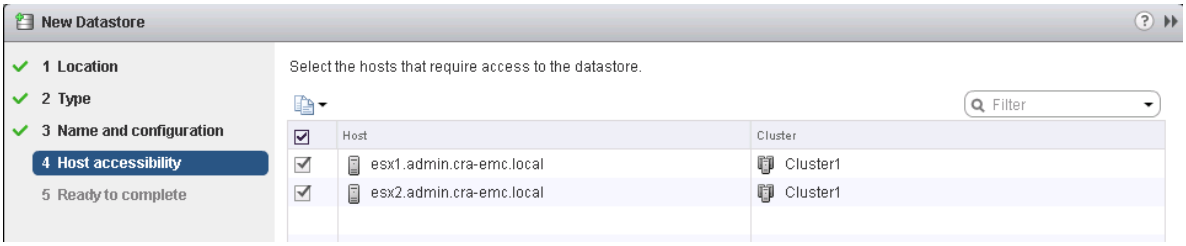



9. Enter <<var_vc_ds1_name>> as the Datastore name.
10. Enter <<var_vnx1_dm2_ip>> as the Server.
11. Enter <<var_vnx1_nfs1_share>> as the Folder.
12. Click the Check-Box for Mount NFS as read-only.
13. Click Next.




14. Select all hosts.

15. Click Next.



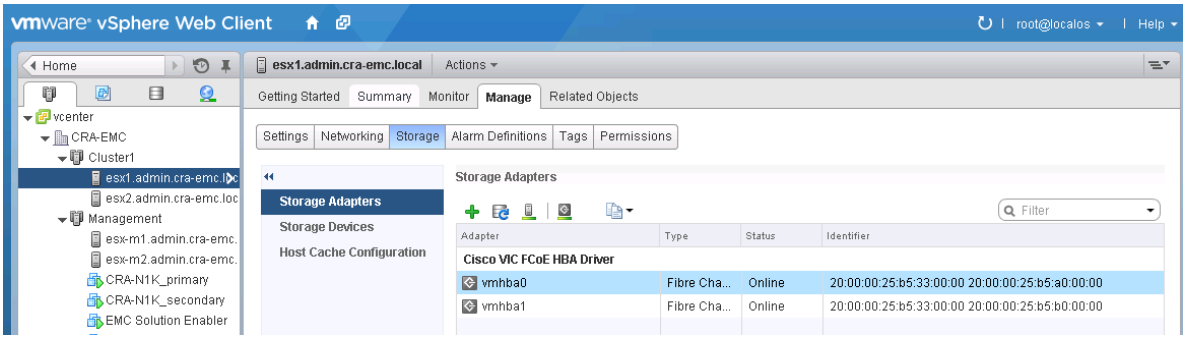

16. Review the information.

17. Click Finish.



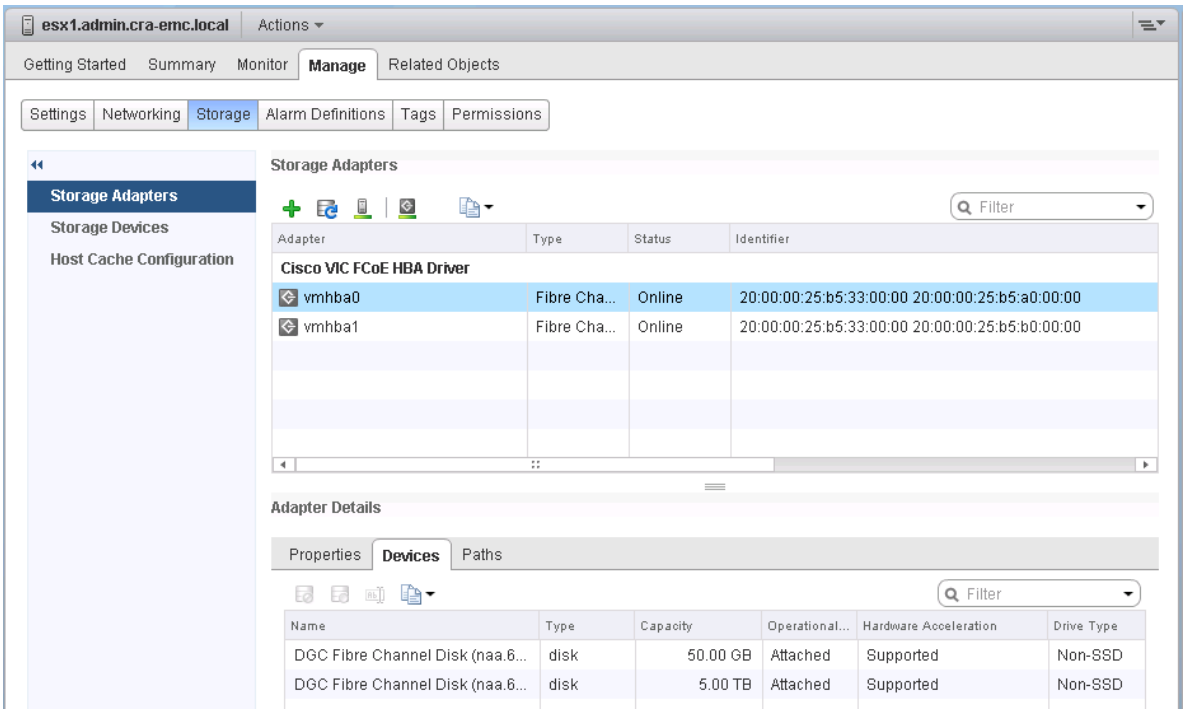

18. Select <<var_esx1_name>>.

19. Click Manage in the right pane.
20. Click Storage.
21. Click Storage Adapters.
22. Click the  Icon.



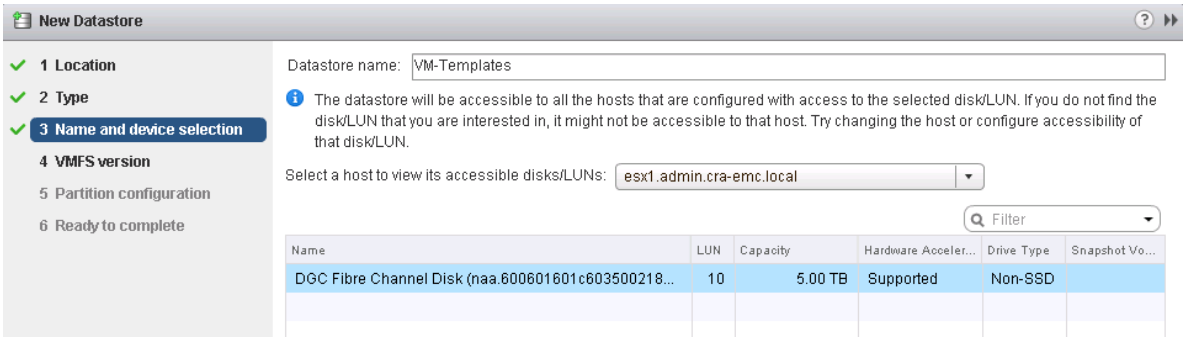

23. Click Devices in the Adapter Details section.

Two disks are shown; the boot LUN with 50GB and the VM-Template LUN with 5TB.

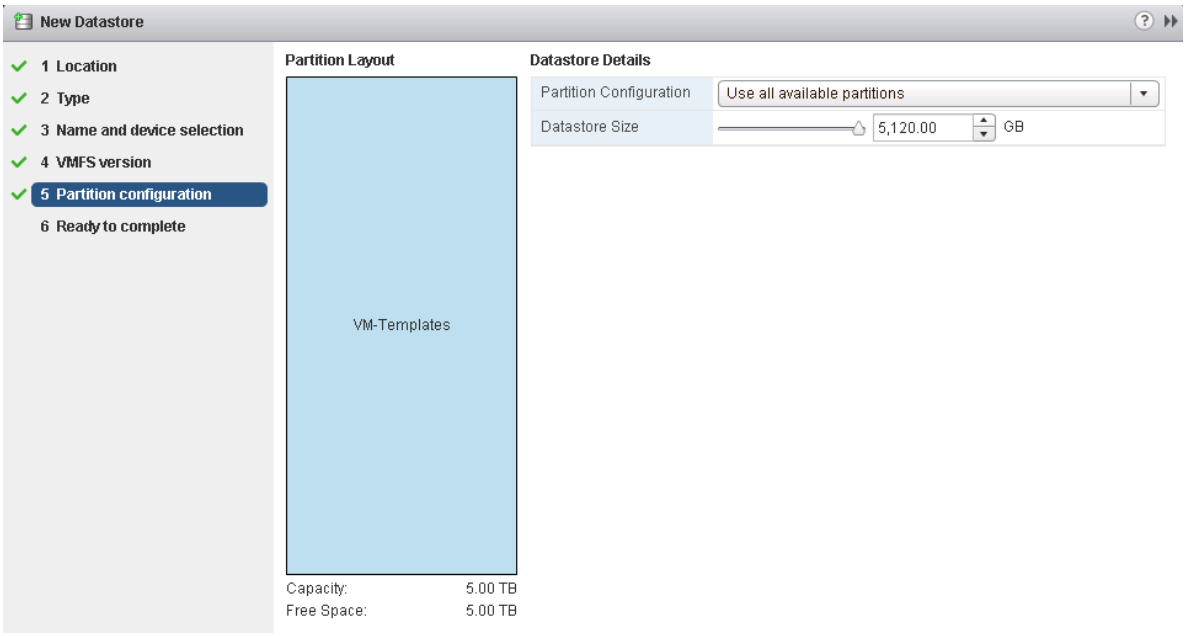



24. Repeat Step 18 – 24 for all ESX-Hosts.
25. Select <<var_vc_cluster1_name>>.
26. Click Actions.

27. Select New Datastore.
28. Click Next in the Location view.
29. Click VMFS in the Type view.
30. Click Next.
31. Enter <<var_vm-templ_ds-name>> as the Datastore Name.
32. Select a Host with access to the LUN.
33. Select the Device with LUN ID 10 and 5TB capacity.
34. Click Next.

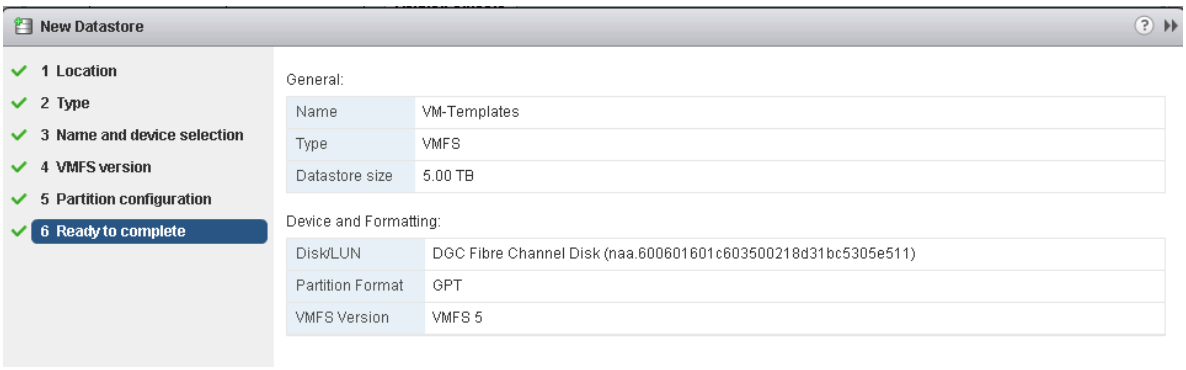



35. Select VMFS 5 in the Version view.
36. Click Next.
37. Select Use all available partitions.
38. Use the maximum size.
39. Click Next.




40. Review the information.

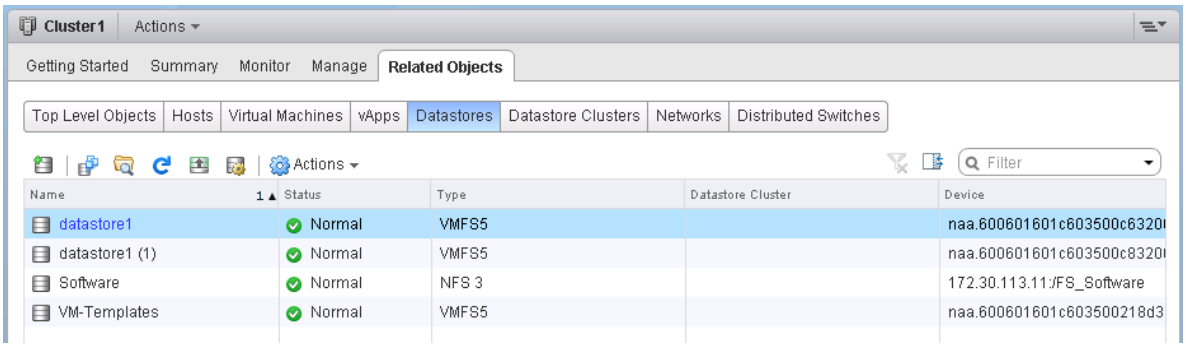
41. Click Finish.




42. Click the Related Objects Tab for Cluster 1.

43. Click Datastores.

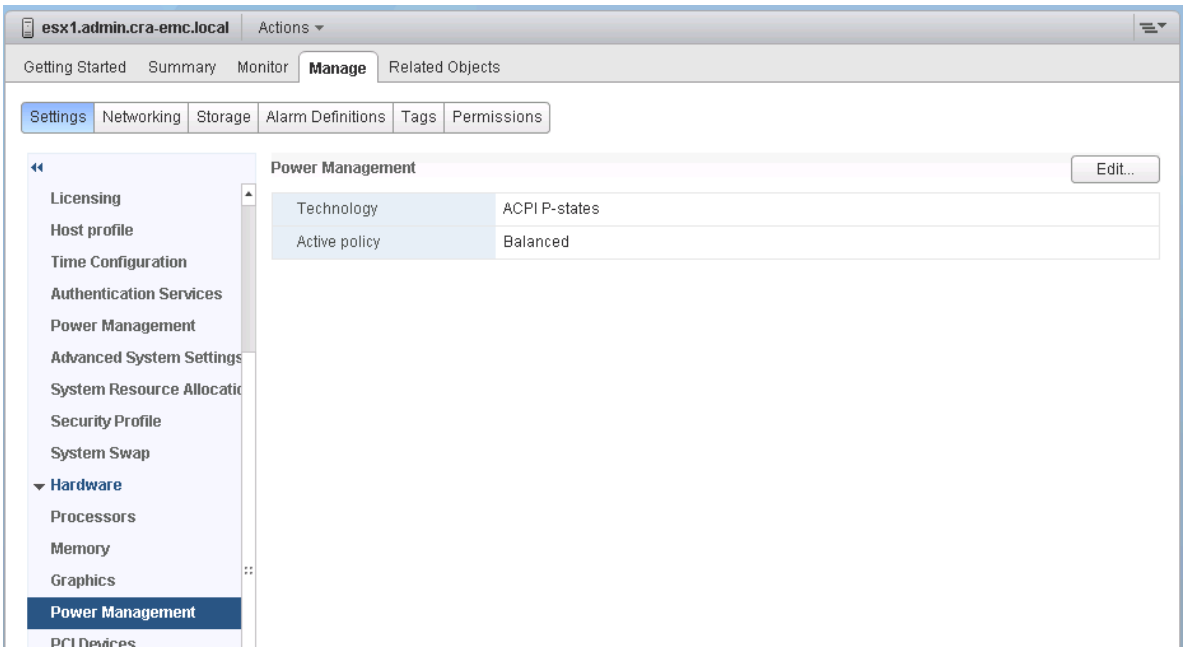
The new datastore is listed.




## Configure ESX-Hosts for SAP HANA

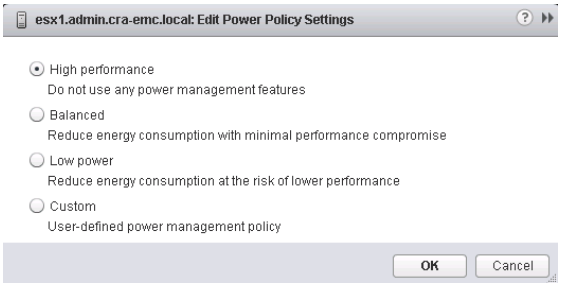
To configure the ESXi as per SAP HANA requirement, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Log in as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click <<var_esx1_name>>.
5. Click Manage in the right pane.
6. Click Settings.
7. Click Power Management.
8. Click Edit.




9. Select High performance.

10. Click OK.



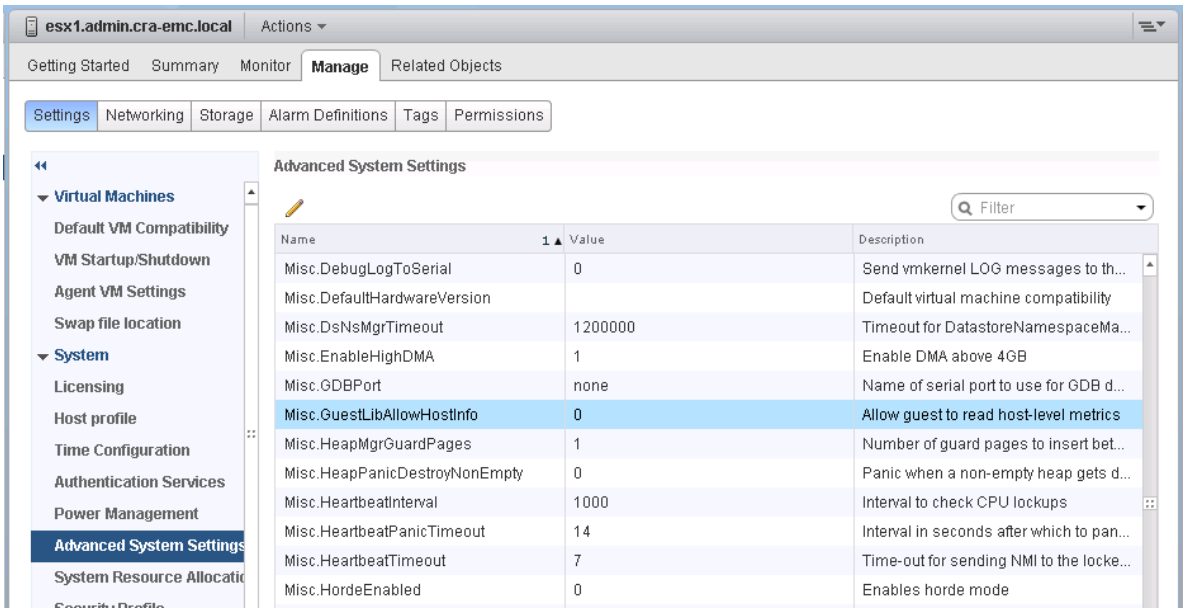

11. Click Advanced System Settings.

12. Scroll down to Select Misc.GuestLibAllowHostInfo.



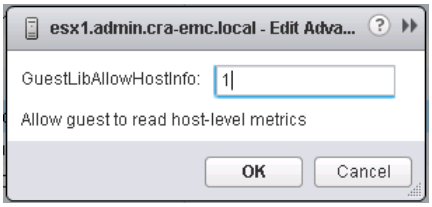
This is required based on SAP Note:1606643

13. Click the Pencil Symbol.




14. Enter 1 into the Field.

15. Click OK.




16. Repeat these steps for all ESX hosts that are used to run SAP HANA.

## Virtual Machine Templates

SAP supports virtualization of SAP HANA on validated single-node SAP HANA appliances or through SAP HANA TDI verified hardware configurations. The existing SAP HANA storage requirements regarding partitioning, configuration and sizing of data, log and binary volumes remain valid.

It is important to note that a vCPU is not exactly equivalent to a full physical core because it is mapped to a logical execution thread. When hyper-threading is enabled, a physical core has two execution threads. This means, two vCPUs are needed in order to use both of them. However, the additional thread created by enabling hyper-threading does not double the performance of the core. It has been determined that enabling hyper-threading usually increases overall SAP HANA system performance by approximately 20 percent.

Refer to “SAP HANA Guidelines for running virtualized” for more information [http://scn.sap.com/docs/DOC-60312](http://scn.sap.com/docs/DOC-60312)

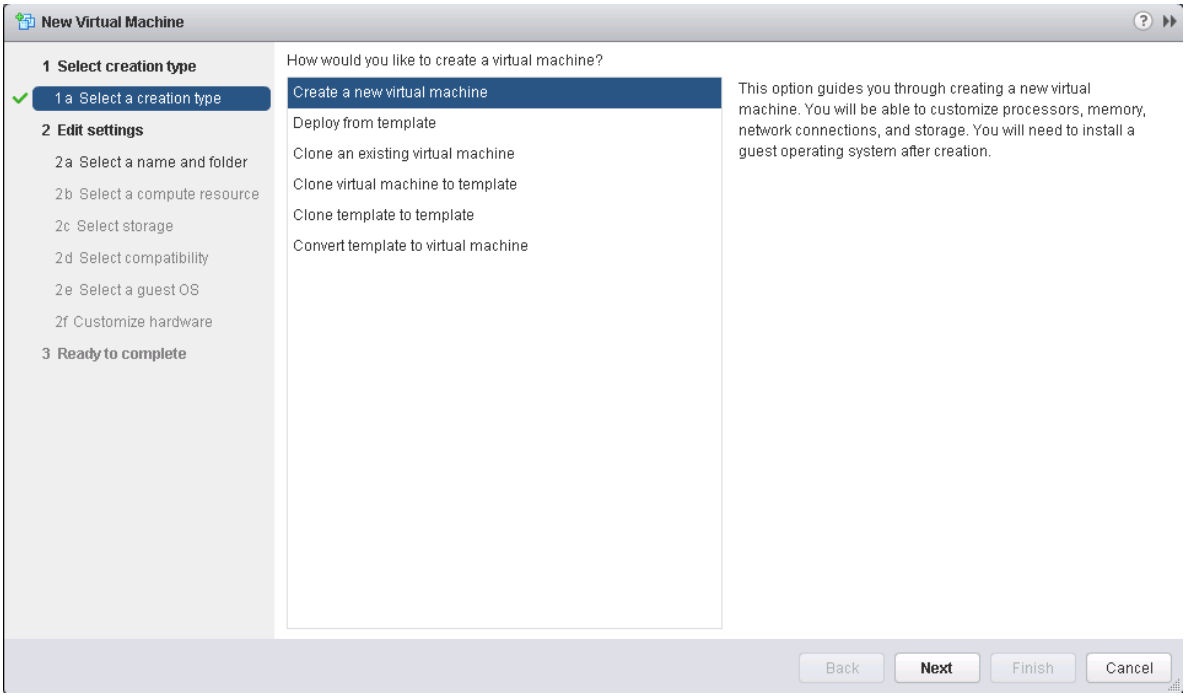
## Virtual Machine Template with SUSE Linux Enterprise for SAP Applications

Creating the virtual machine template requires two steps. The first step is to install a virtual machine and to configure all settings for SAP HANA. The second step is to convert the virtual machine into a virtual machine template.

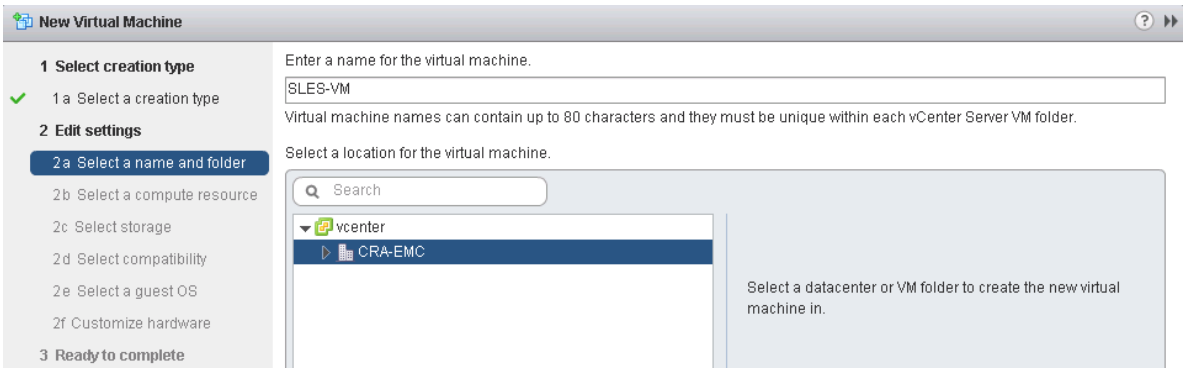
### Create a Virtual Machine for Virtualized SAP HANA (vHANA)

To build a virtual machine (VM) for vHANA, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click <<var_vc_cluster1_name>>.
5. Click Actions.
6. Select New Virtual Machine to start the Wizard.
7. Click Next.

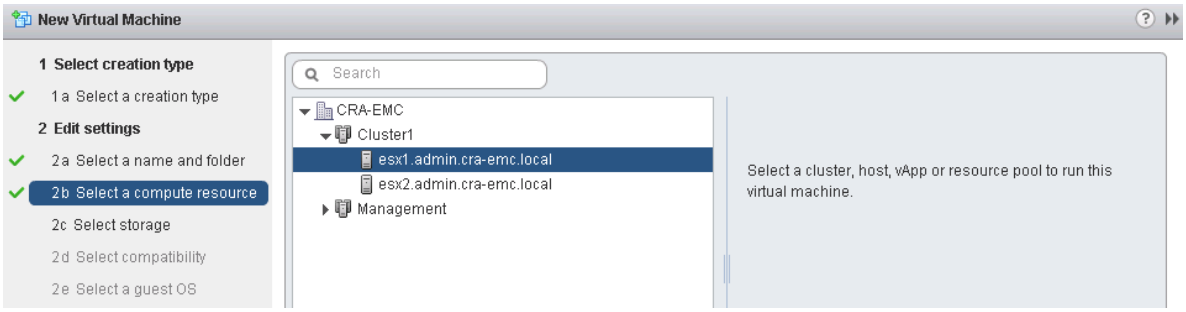



8. Enter <<var_sles_vm_name>> as the Name of the Virtual Machine.
9. Click Next.



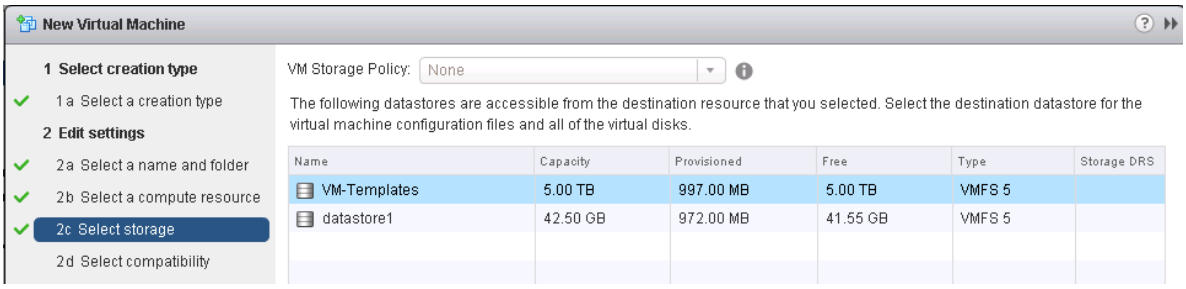

10. Select Cluster1 or a ESX host within Cluster 1 as compute resource.

11. Click Next.



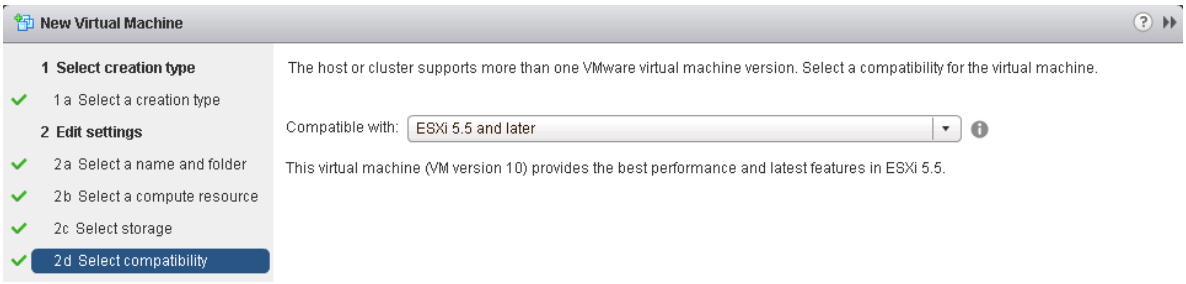

12. Select << >> as the storage.

13. Click Next.

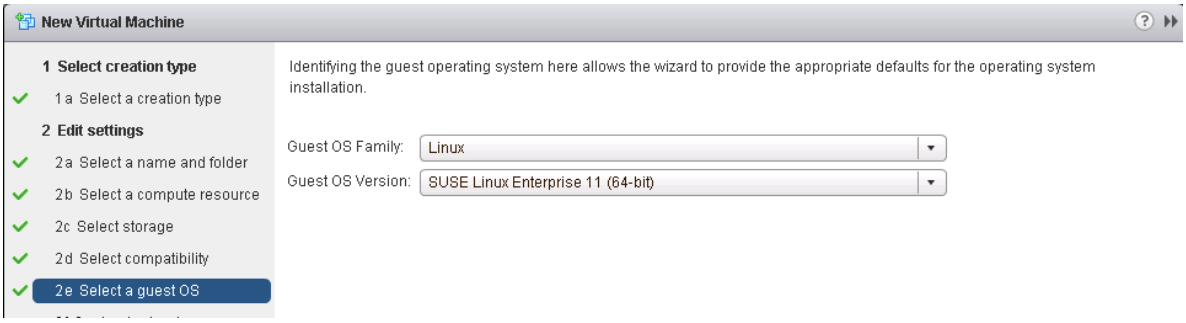



14. For the Compatible with option select ESXi 5.5 or later.

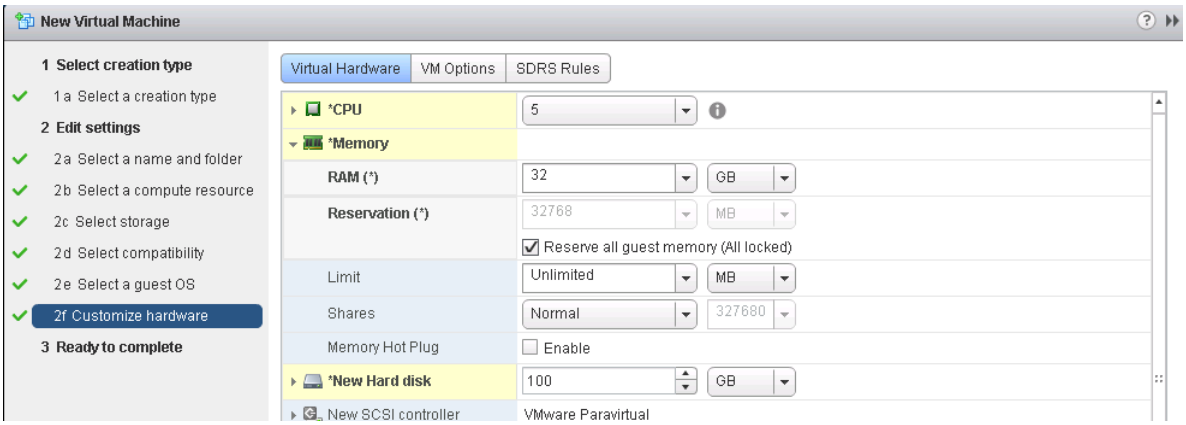
15. Click Next.




16. Select Linux from the drop-down menu for Guest OS Family.
17. Select SUSE Linux Enterprise 11 (64-bit) as the Guest OS Version.
18. Click Next.




19. Select 5 as the # of CPUs.
20. Enter 32 and GB for the Memory.
21. Click the Arrow left of Memory.
22. Select the Check-Box to Reserve all guest memory (All locked).
23. Enter 100 and GB for the Hard disk.
24. Select Network from the New device drop-down menu.
25. Click Add.



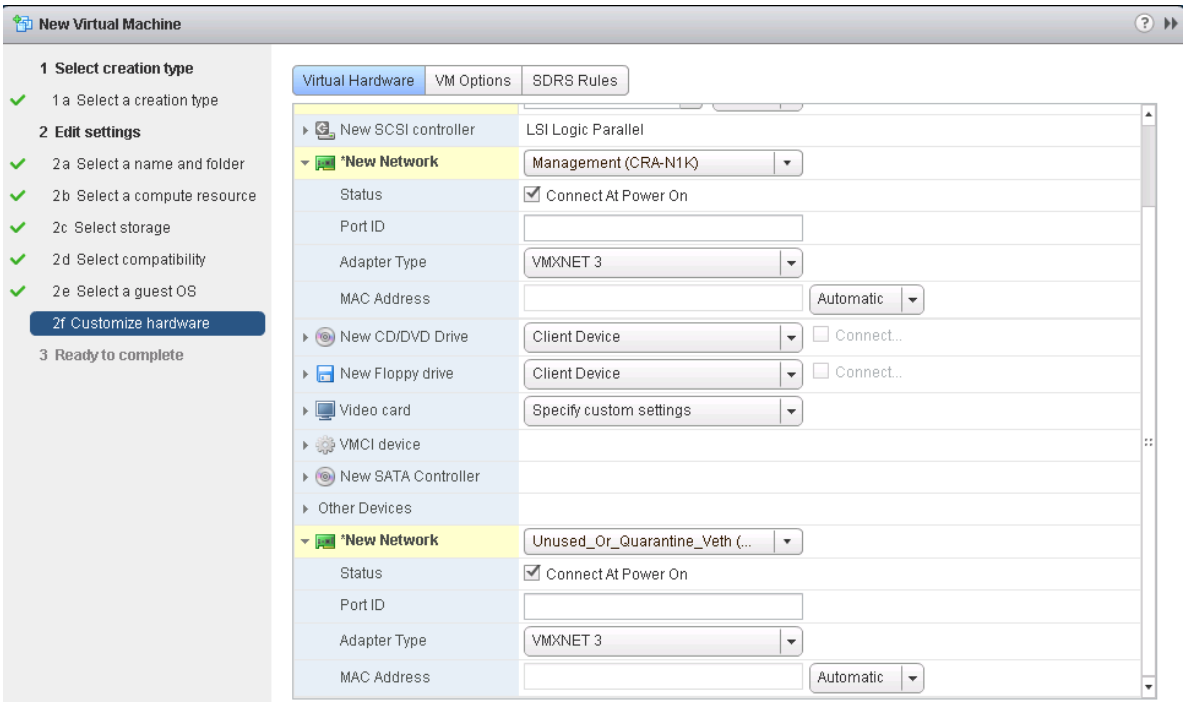

26. Select Management (CRA-N1K) for the first New Network devices.

27. Select Unused_Or_Quarantine_Veth for the second New Network device.

28. Click the Arrow left of both Network Cards.

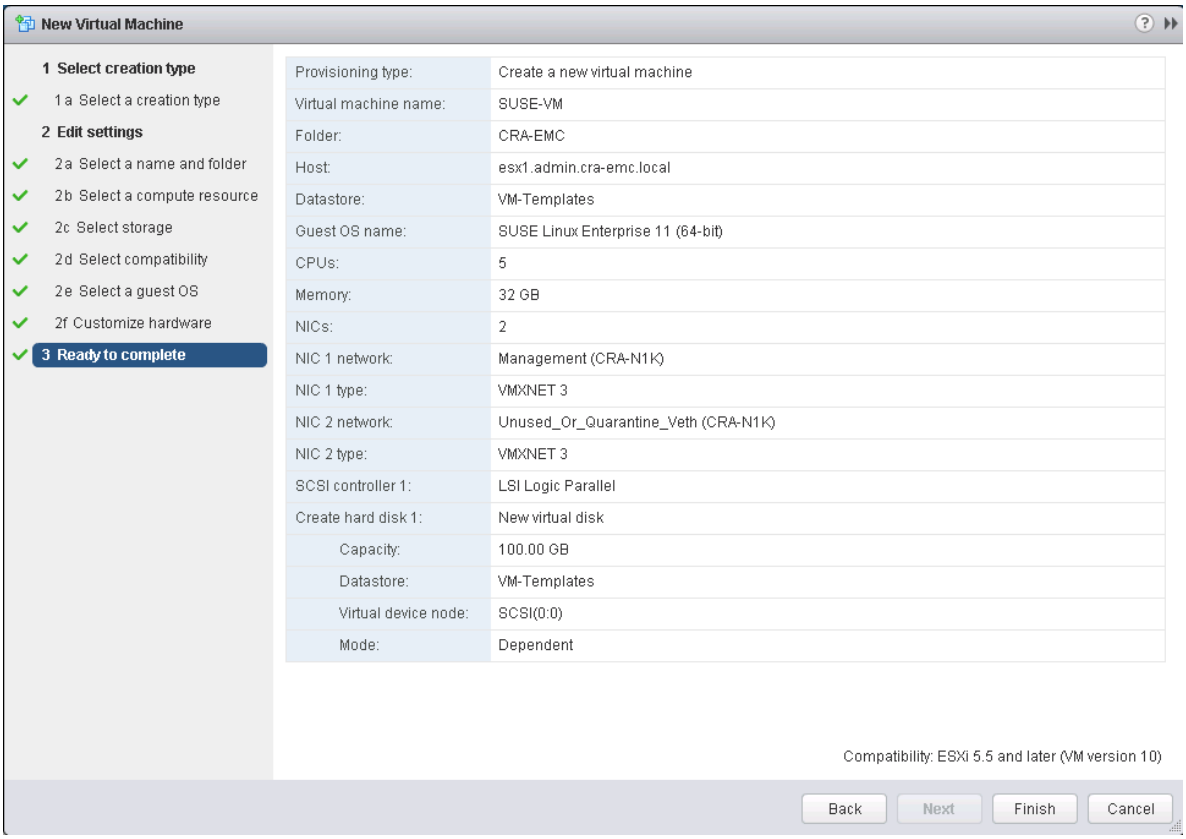
29. Select VMXNET3 as the Adapter Type for all network cards.

30. Click Next.




31. Review the information.

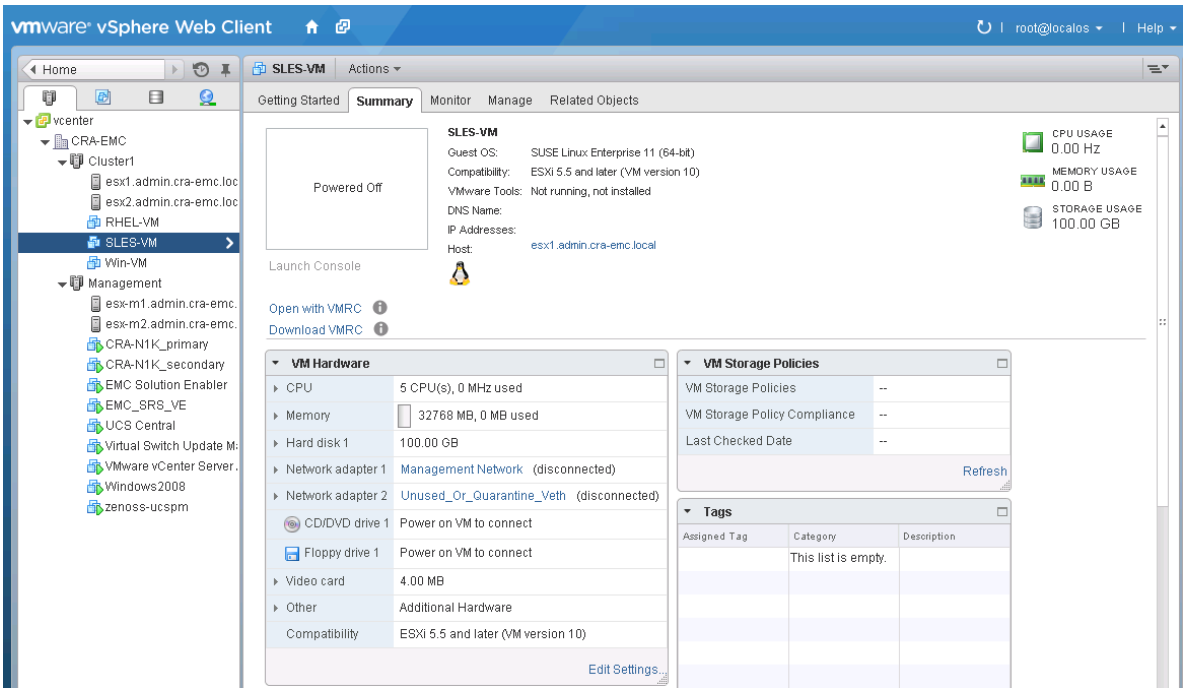
32. Click Finish.




## Install and Configure SUSE Linux Enterprise for Virtualized SAP HANA (vHANA)

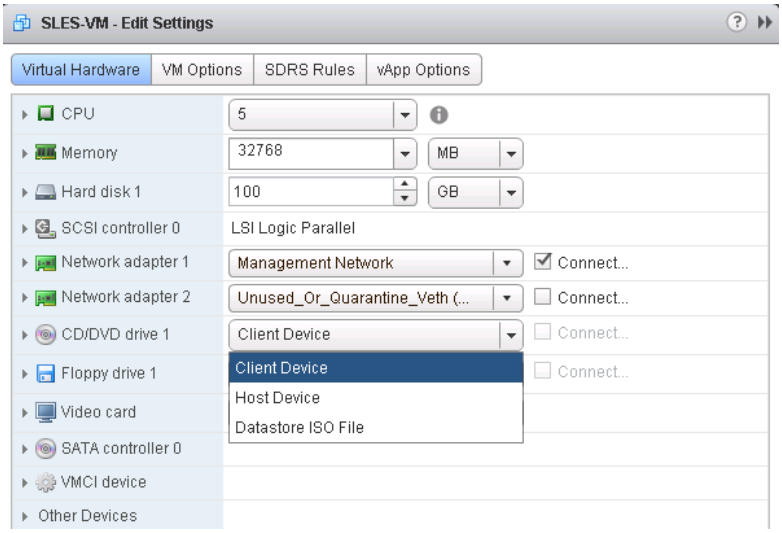
To install and configure SUSE, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Select <<var_vc_ucscentral_vm_name>>.
5. Click Summary Tab in the right pane.
6. Click Edit Settings at the bottom of the VM Hardware section.




7. Click the drop-down Menu for CD/DVD drive 1.

8. Select Datastore ISO File.

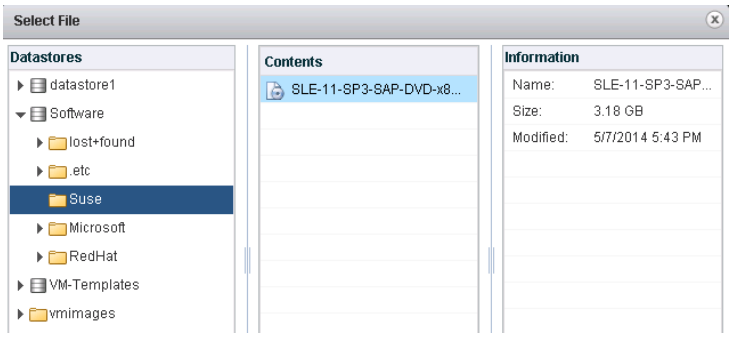



9. Select the Datastore Software.

10. Click directory where the SUSE Linux Enterprise ISO is located.

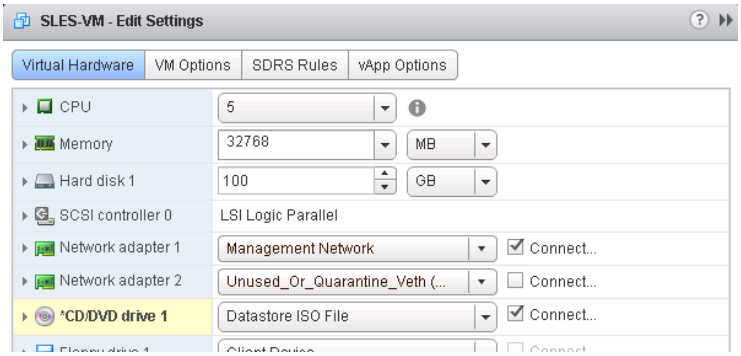
11. Select the ISO file.

12. Click OK.




13. Select the Connect checkbox.

14. Click OK.



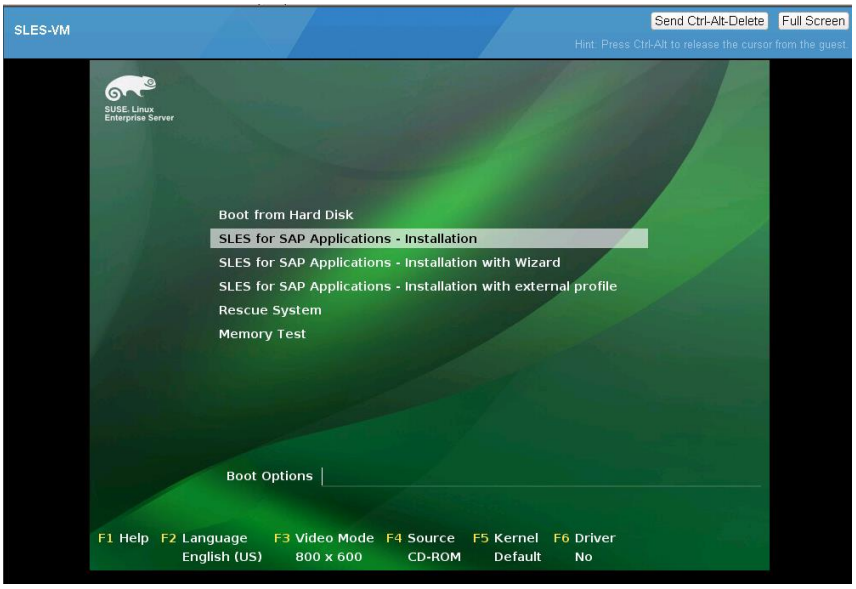

15. Click Actions.

16. Select Power On.

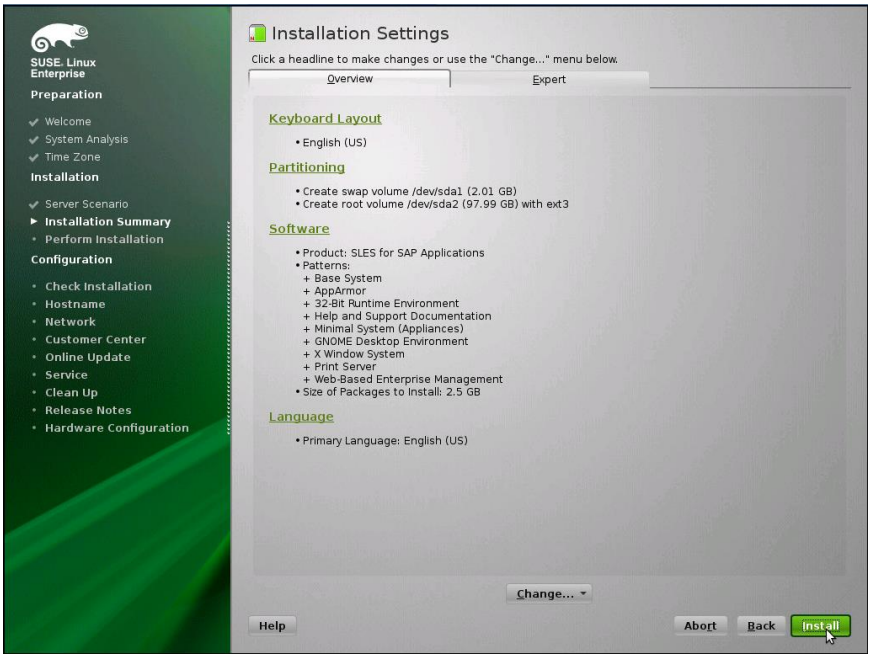
17. Click Launch Console.

18. Select SLES for SAP Applications – Installation.

19. Press Enter.




20. Follow the instructions on the screens and select the settings that fits best for you until the Installation Summary screen.




21. Click Change.

22. Select Software.

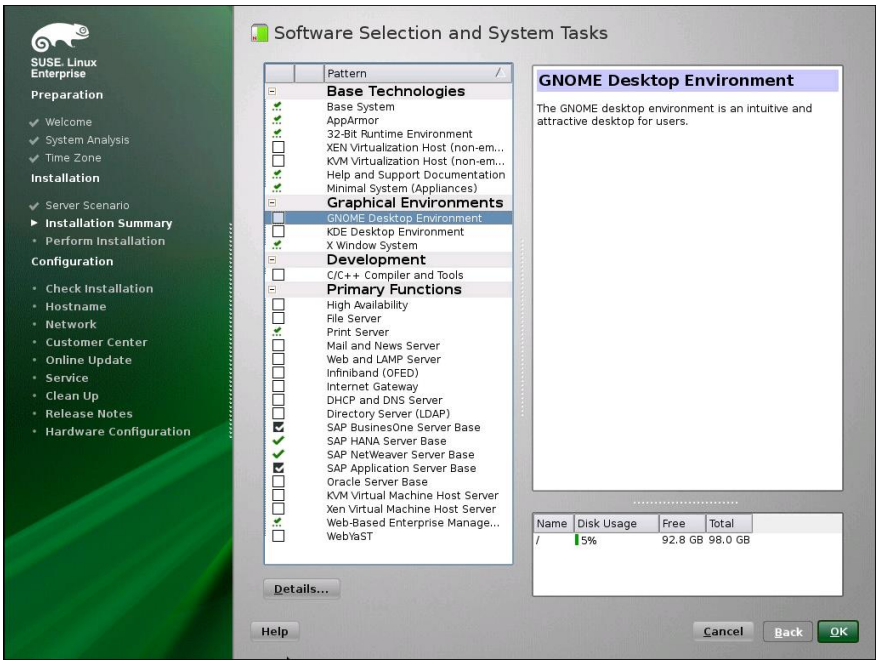
23. Unselect  GNOME Desktop Environment.

24. Select SAP HANA Server Base.

25. If this VM-Template is used for other SAP Applications, select SAP NetWeaver Base.

26. Click OK.

27. Click Accept.






The Partitioning proposed by SUSE is good to run SAP HANA. If you have differing best practices for partitioning, please change the partitioning accordingly.

28. Click Install.

29. On the Confirm Installation Window, Click Install.

30. SUSE Enterprise Linux installation will start and after the packages are installed the Virtual Machine automatically reboots.

31. After the reboot, enter <<var_mgmt_passwd>> as the Password.

32. On the Network configuration screen, click disable in the Firewall section.

33. Click Network Interfaces.

34. Select eth0.

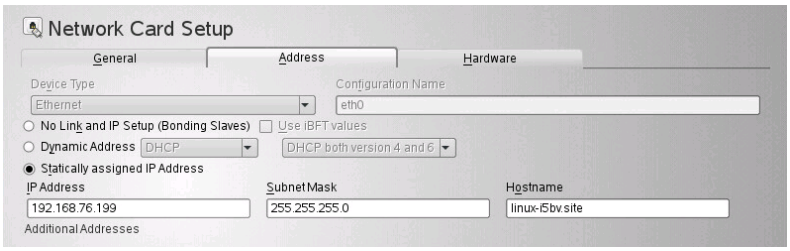
35. Click Edit.

36. Select Static assigned IP Address.

37. Enter <<var_mgmt_temp_ip>> as the IP Address – This IP Address is only temporarily used.

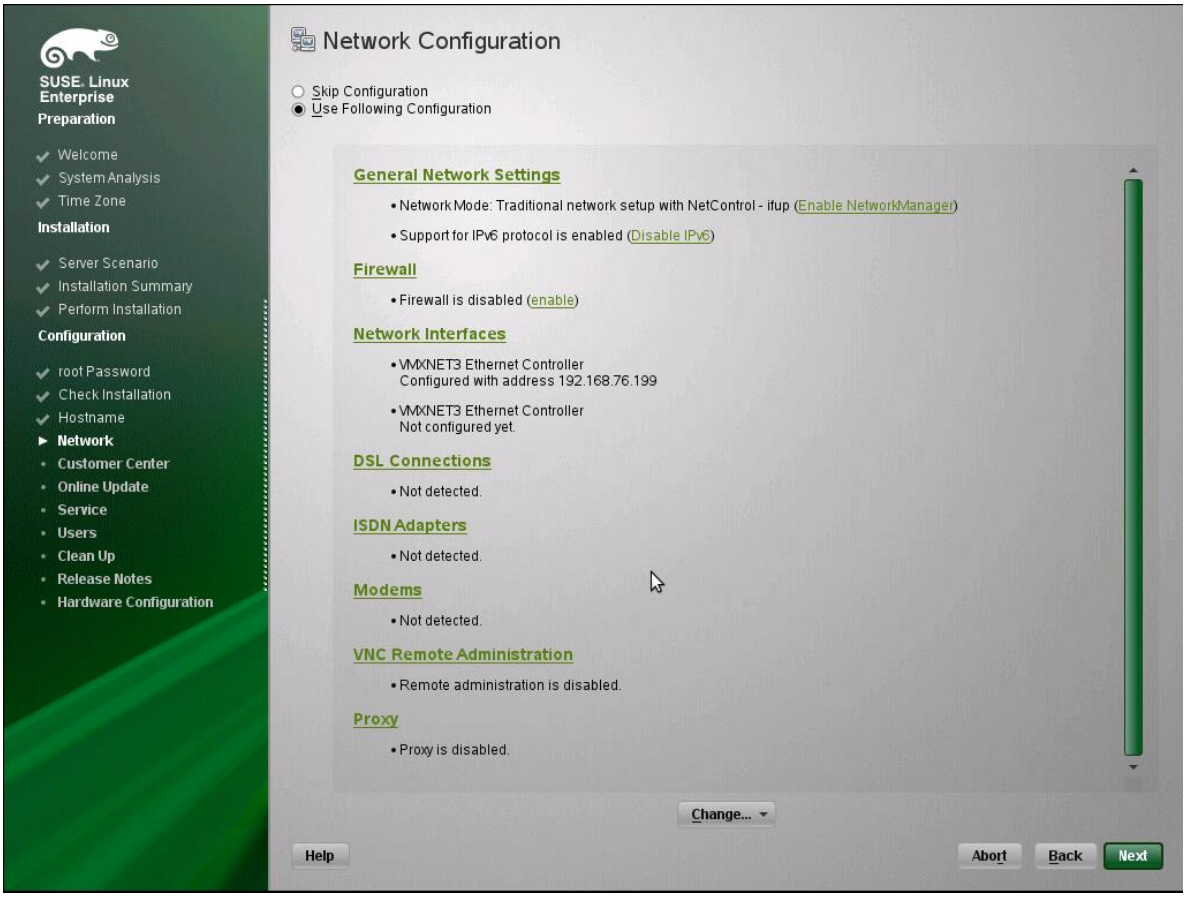
38. Enter <<var_mgmt_mask>> as the Subnet Mask.

39. Click Next.

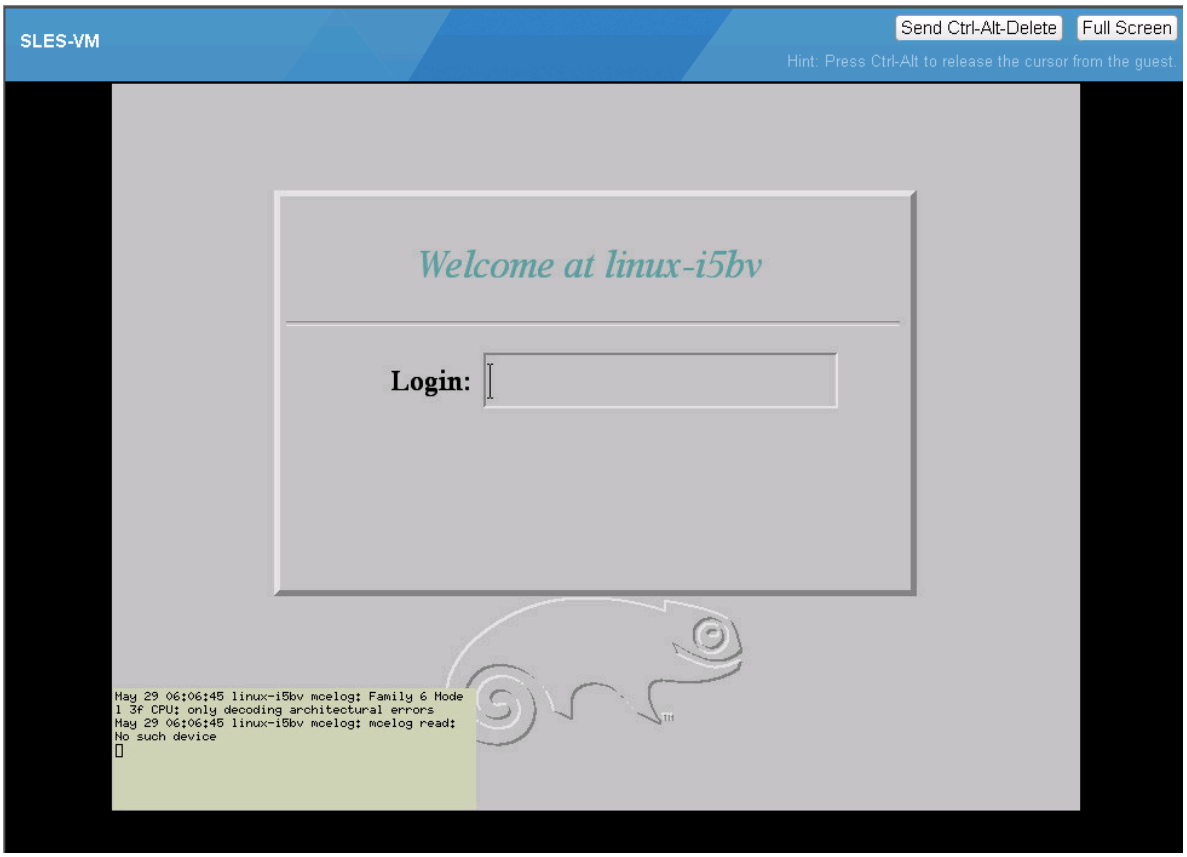



40. Click OK.

41. From the Network Configuration Screen, click Next.




42. Skip the Network Test and follow the instructions on the following screens until the configuration is finished.




43. Use a SSH client to log in to the installed system with the user root and the password <<var_mgmt_passwd>>.

44. Register the System at SUSE to get latest Patches.

The system must have access to the internet to proceed with this step.

suse_register -i -r -n -a email= <<email_address>> -a regcode-sles=<<registration_code>>

45. Update the system with the following command:

The system must have access to the internet to proceed with this step!

```
zypper update
```

46. Follow the on screen instructions to complete the update process. Reboot the server and login to the system again.

47. Configure the default init level to 3 by editing the following line in /etc/inittab

```
vi /etc/inittab


# The default runlevel is defined here
```

```
id:3:initdefault:
```

48. Configure the Network Time Protocol:

```
vi /etc/ntp.conf
```

```
server <<var_global_ntp_server_ip>>
fudge <<var_global_ntp_server_ip>> stratum 10
keys /etc/ntp.keys
trustedkey 1
```

49. Create User-Group sapsys:

```
groupadd –g 401 sapsys
```

50. It is recommended to disable Transparent Huge Pages and the swappiness on the system:

```
vi /etc/init.d/after.local
```

```
#!/bin/bash
# (c) Cisco Systems Inc. 2014
echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status
# set sappiness to 30 to avoid swapping
echo "Set swappiness to 30 to avoid swapping"
echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status
```

51. Based on different SAP Notes multiple entries in /etc/sysctl.conf are required:

```
vi /etc/sysctl.conf
```

```
#SAP Note 1275776
vm.max_map_count = 2000000
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
```

```
net.ipv4.tcp_slow_start_after_idle = 0
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_slot_table_entries = 128
# Memory Page Cache Limit Feature SAP Note 1557506
vm.pagecache_limit_mb = 4096
vm.pagecache_limit_ignore_dirty = 1
```

52. Edit boot loader configuration file /etc/sysconfig/bootloader. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

```
intel_idle.max_cstate=0
```

53. Append the intel_idle.max_cstate=0 processor.max_cstate=0 value to the kernel's parameter line in /boot/grub/menu.lst – 3.0.xxx-x.xx is the placeholder for your Kernel patch version:

```
vi /boot/grub/menu.lst

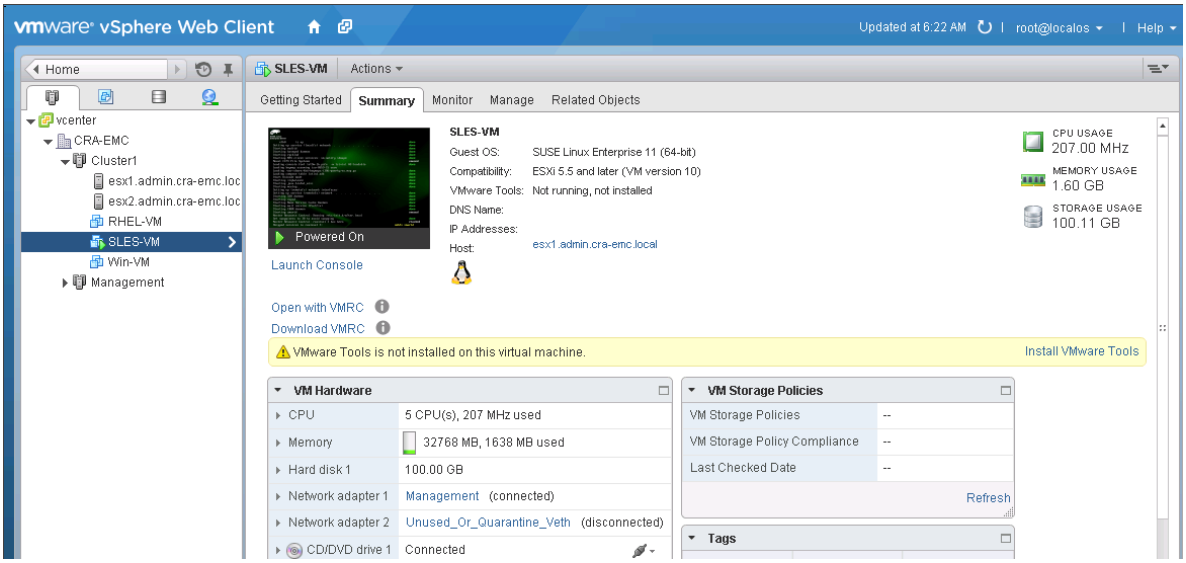

title SLES for SAP Applications - 3.0.XXX-X.XX
root (hd0,0)
kernel /boot/vmlinuz-3.0.XXX-X.XX-default root=/dev/sda2 resume=/dev/sda1
splash=silent showopts intel_idle.max_cstate=0 processor.max_cstate=0
initrd /boot/initrd-3.0.XXX-X.XX-default
```

54. Reboot the server:

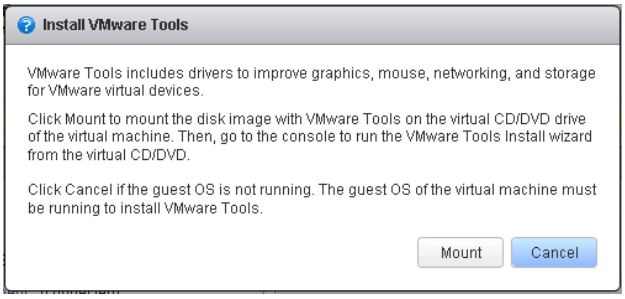
```
reboot
```

## Install the VMware Tools

1. Open vSphere Web Client and Select the Virtual Machine.
2. Click Install VMware Tools.




3. Click Mount.




4. Use a SSH client to login to the system.
5. To manually install the VMware Tools:

```
mount /dev/cdrom1 /media
cp /media/* /tmp
cd /tmp
tar -zxvf VMwareTools-*.tar.gz
cd /tmp/vmware-tools-distrib
```

```
./vmware-install.pl
```

6. Follow the onscreen instructions to complete the installation.

7. Reboot the system to finish the installation:

```
reboot
```

To create the Virtual Machine Template, clean up the OS Master Image, complete the following steps:

1. Use a SSH client to login to the system.

2. Clear the System Logs:

```
rm /var/log/* -r
```

3. Clear the Ethernet Persistent network information:

```
cat /dev/null > /etc/udev/rules.d/70-persistent-net.rules
```

4. Remove the Ethernet configuration files:

```
rm /etc/sysconfig/network/ifcfg-eth*
```

5. Remove the default gateway configuration:

```
rm /etc/sysconfig/network/routes
```

6. Shutdown the system:

```
halt
```

### Migrate Virtual Machine into a Virtual Machine Template

Migrate the Virtual Machine into a Virtual Machine Template that is used for future Virtual Machine deployments. To migrate the virtual machine, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.

2. Logon as root and the password <<var_mgmt_passwd>>.

3. Click Hosts and Clusters.

4. Click the virtual machine.

5. Click Actions > All vCenter Actions.

6. Click Convert to Template.

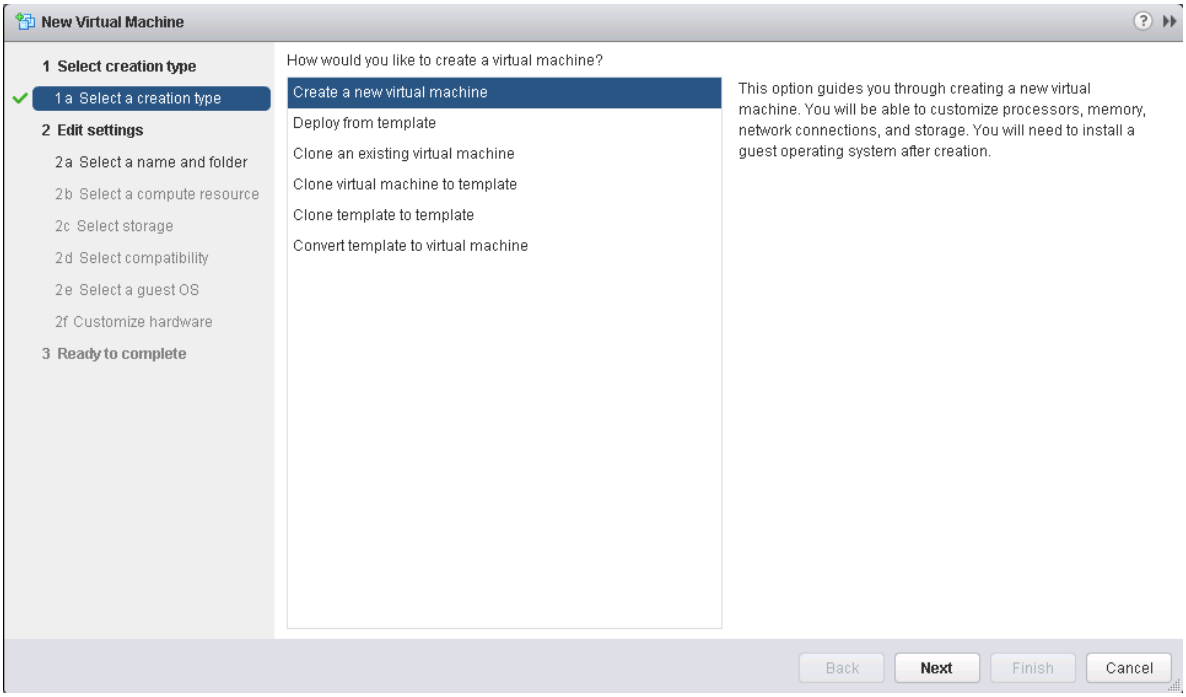
## Virtual Machine Template with Red Hat Enterprise Linux for SAP HANA

Creating the Virtual Machine template requires two steps. The first step is to install a Virtual Machine and to configure all settings for SAP HANA. The second step is to convert the Virtual Machine into a Virtual Machine Template.

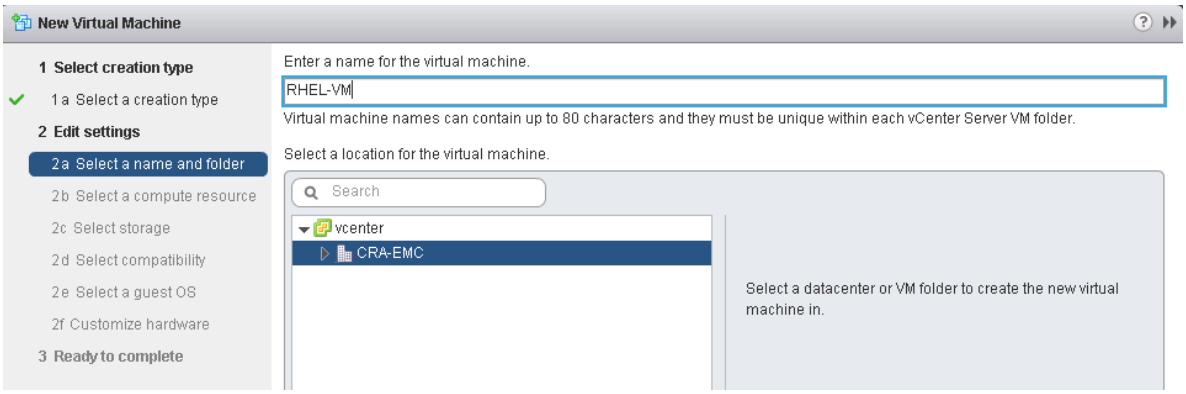
### Create a Virtual Machine for Virtualized SAP HANA (vHANA)

To build a virtual machine (VM) for vHANA, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click <<var_vc_cluster1_name>>.
5. Click Actions.
6. Select New Virtual Machine to start the Wizard.
7. Click Next.

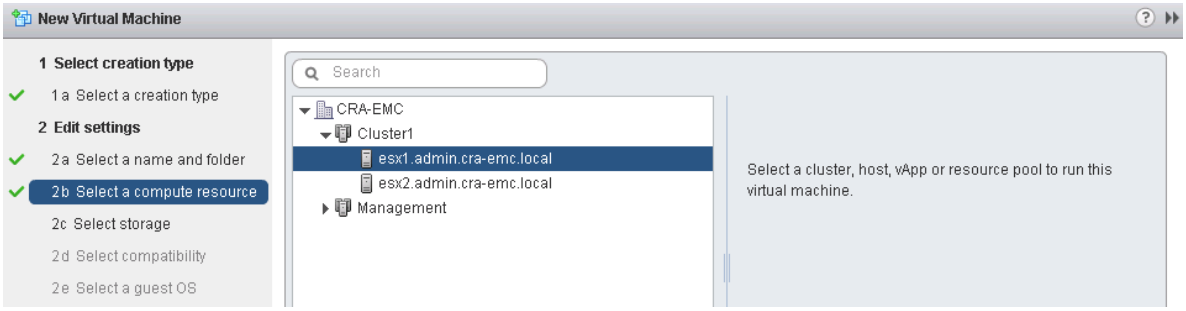



8. Enter <<var_rhel_vm_name>> as the Name of the Virtual Machine.
9. Click Next.



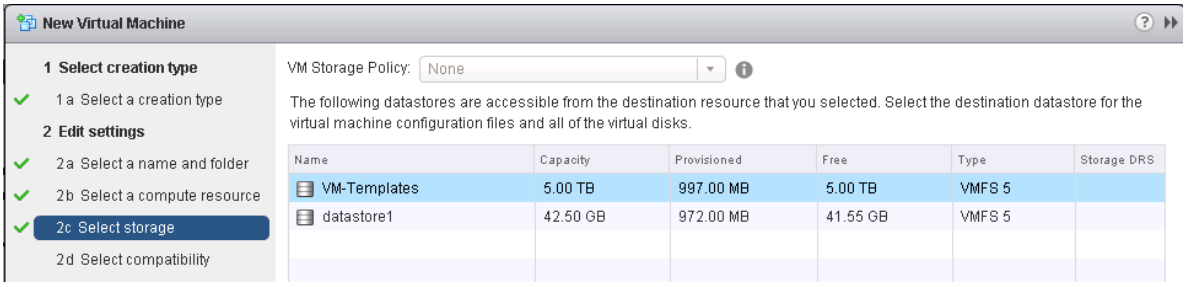

10. Select Cluster1 or a ESX host within Cluster 1 as compute resource.

11. Click Next.



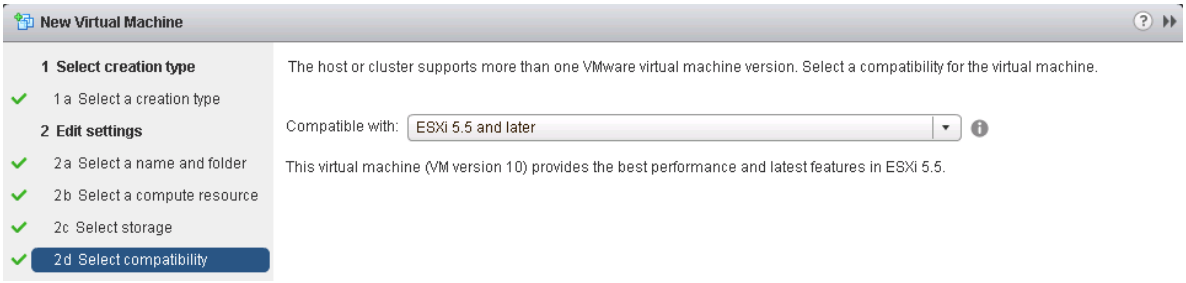

12. Select << >> as the storage.

13. Click Next.

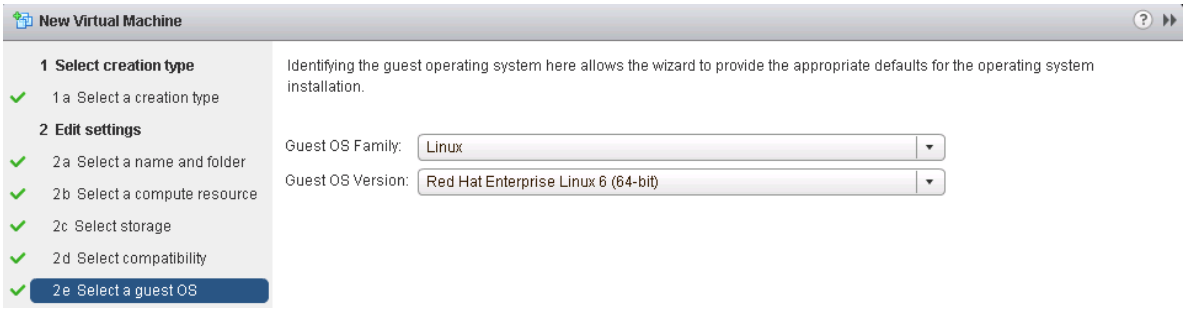



14. For the Compatible with option select ESXi 5.5 or later.

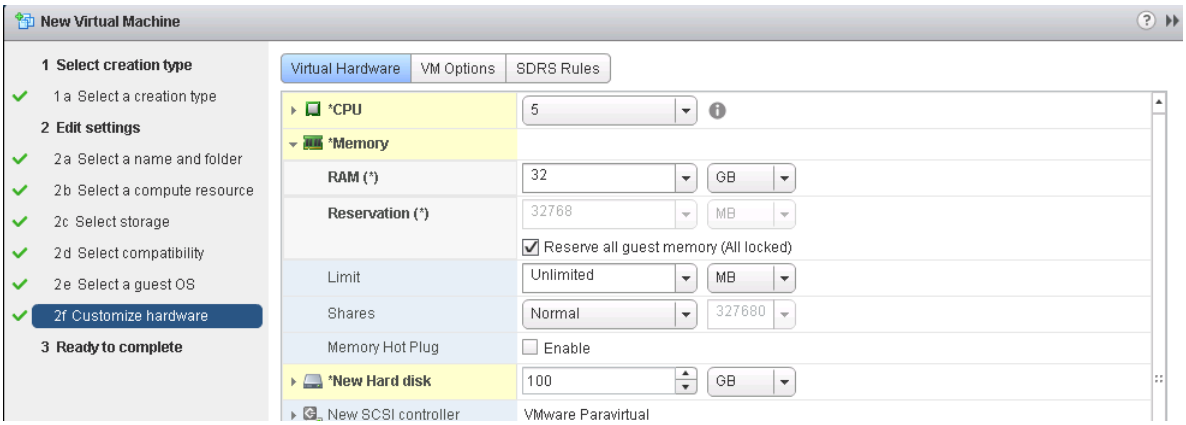
15. Click Next.




16. Select Linux from the Drop-down menu for Guest OS Family.
17. Select Red Hat Enterprise Linux 6 (64-bit) as the Guest OS Version.
18. Click Next.




19. Select 5 as the # of CPUs.
20. Enter 32 and GB for the Memory.
21. Click the Arrow left of Memory.
22. Select the checkbox to Reserve all guest memory (All locked).
23. Enter 100 and GB for the Hard disk.
24. Select Network from the New device drop-down menu.
25. Click Add.



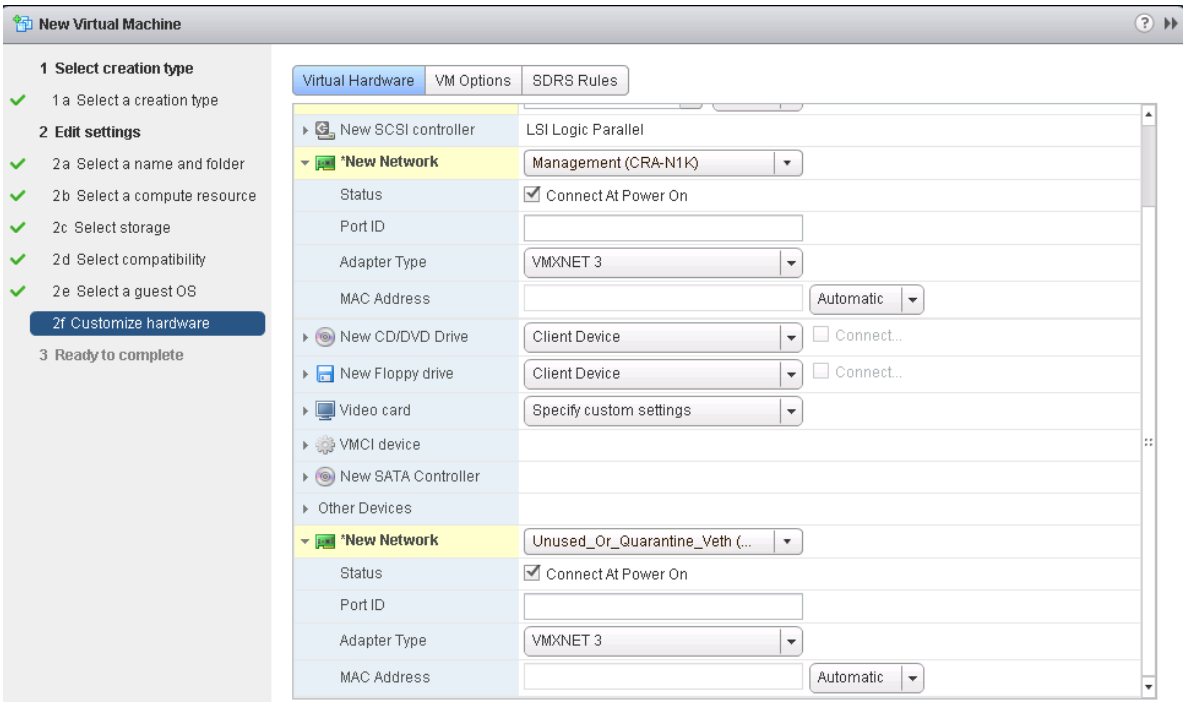

26. Select Management (CRA-N1K) for the first New Network devices.

27. Select Unused_Or_Quarantine_Veth for the second New Network device.

28. Click the Arrow left of both Network Cards.

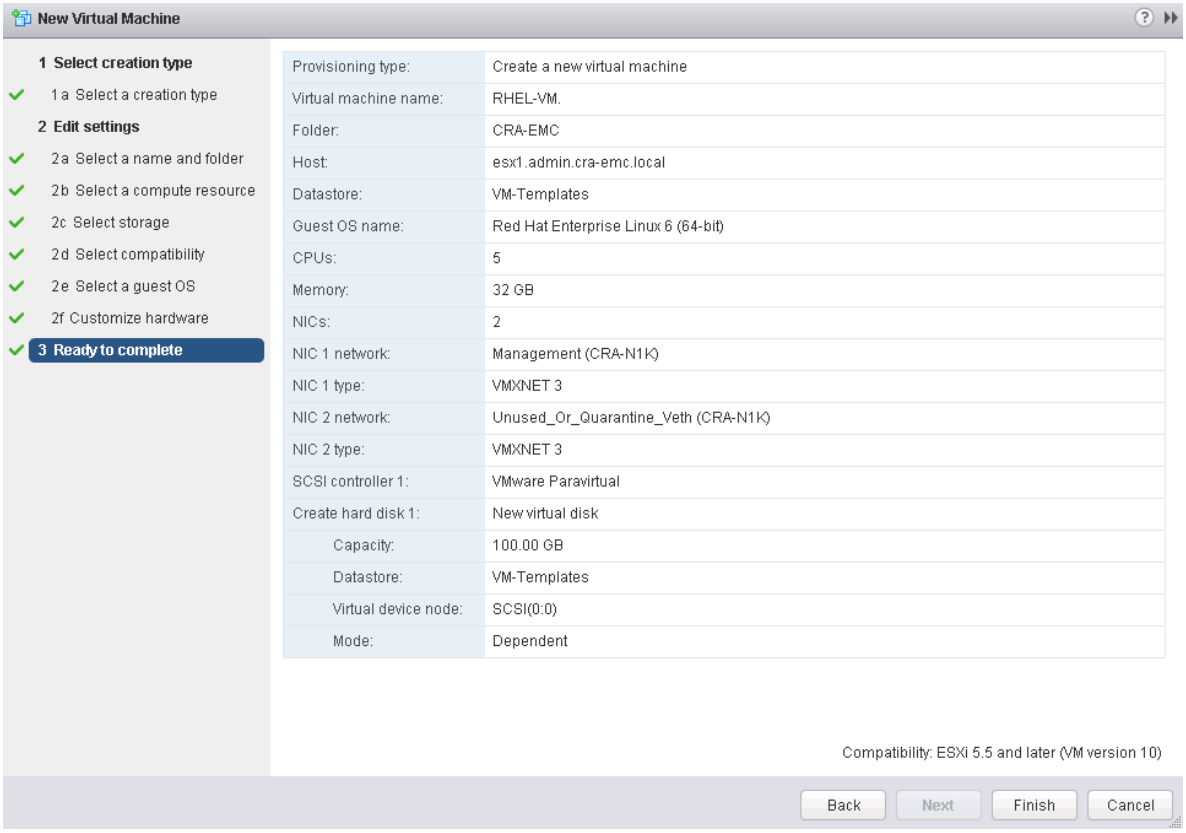
29. Select VMXNET3 as the Adapter Type for all network cards.

30. Click Next.




31. Review the information.

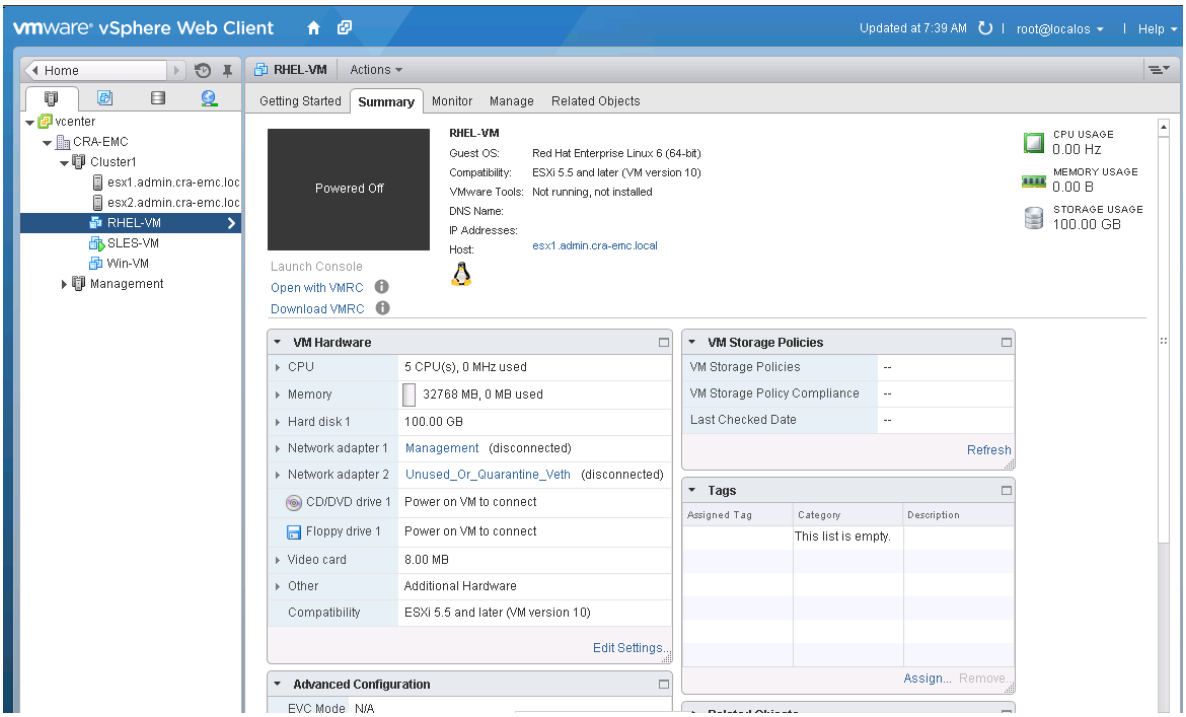
32. Click Finish.




## Install and Configure Red Hat Enterprise Linux for Virtualized SAP HANA (vHANA)

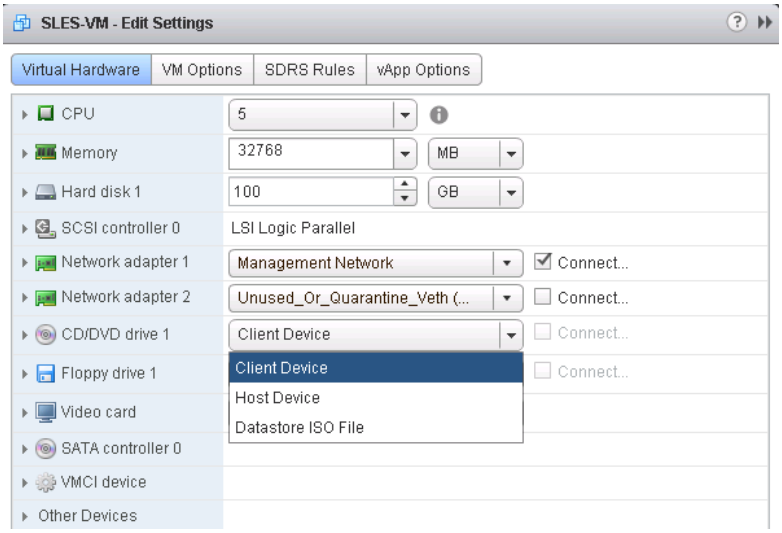
To install and configure Red Hat, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Select <<var_vc_ucscentral_vm_name>>.
5. Click Summary tab in the right pane.
6. Click Edit Settings at the bottom of the VM Hardware section.




7. Click the drop-down menu for CD/DVD drive 1.

8. Select Datastore ISO File.

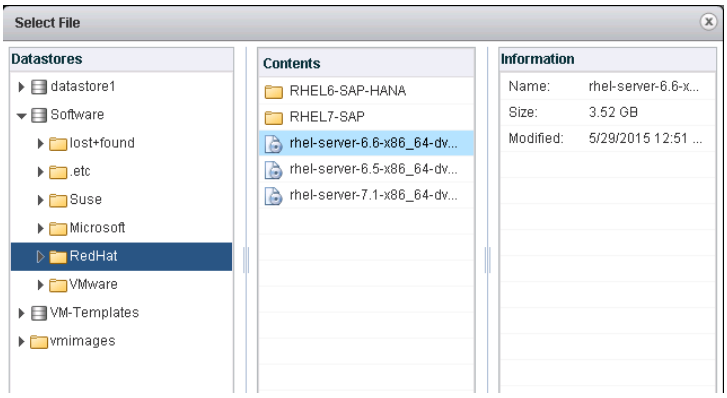



9. Select the Datastore Software.

10. Click the directory where the Red Hat Enterprise Linux ISO is located.

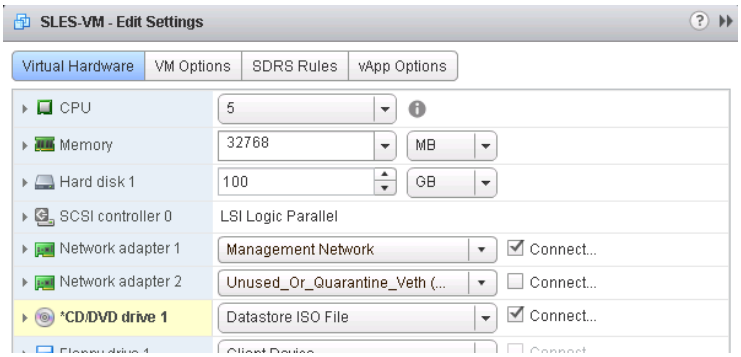
11. Select the ISO file.

12. Click OK.




13. Select the Connect checkbox.

14. Click OK.



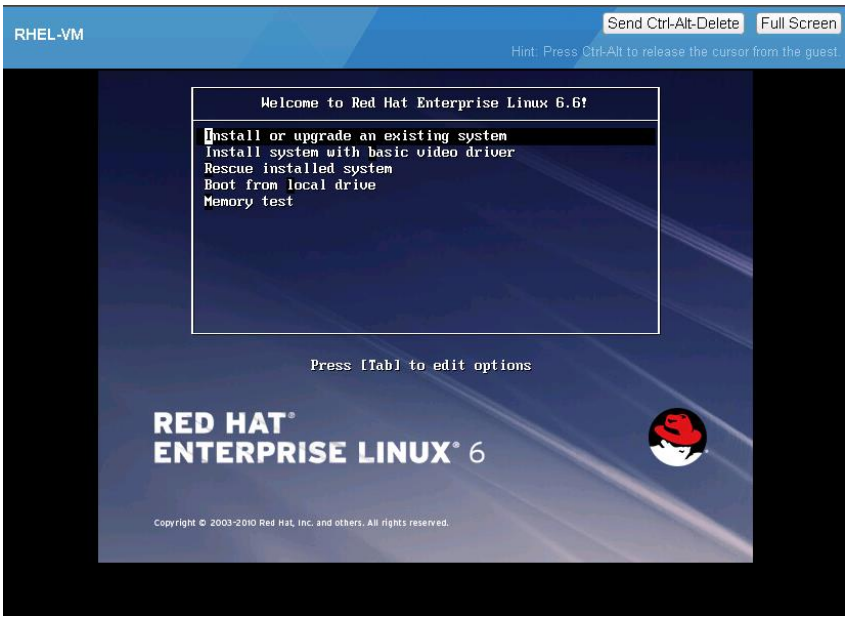

15. Click Actions.

16. Select Power On.

17. Click Launch Console.

18. Select Install or upgrade an existing system.

19. Press Enter.

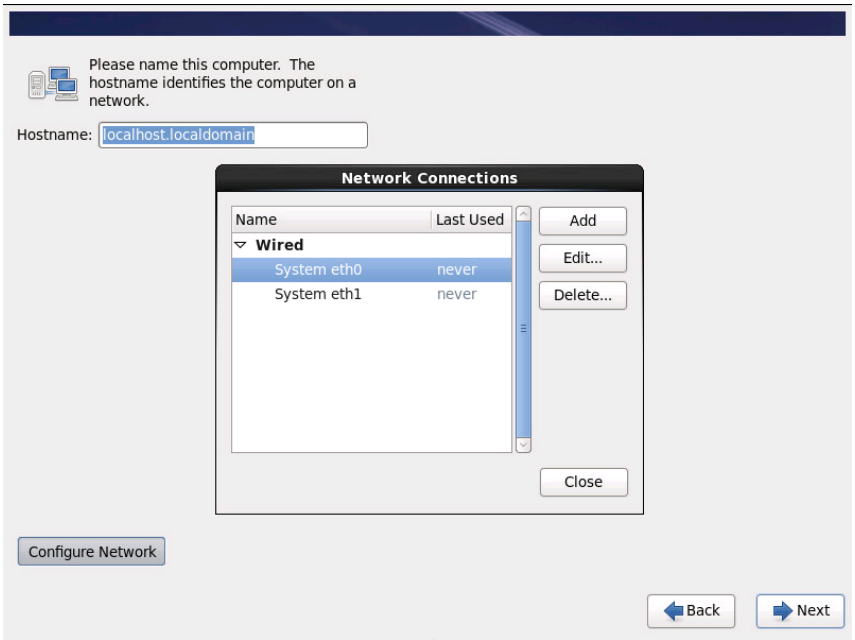



Follow the instructions on the proceeding screens and select the settings until the Installation Summary screen appears.

20. Click Configure Network.

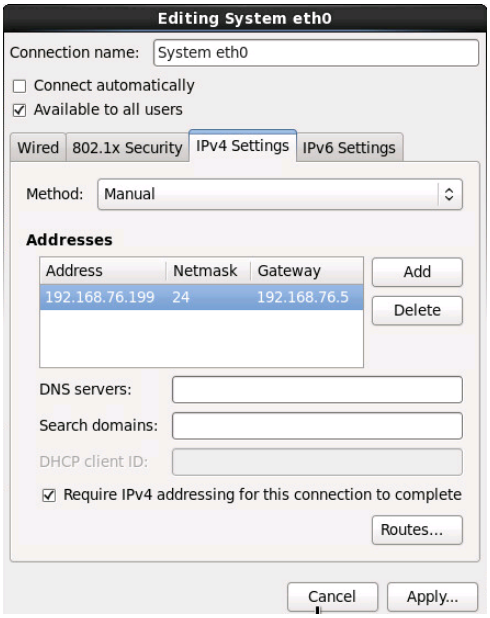
21. Select System eth0.

22. Click Edit.

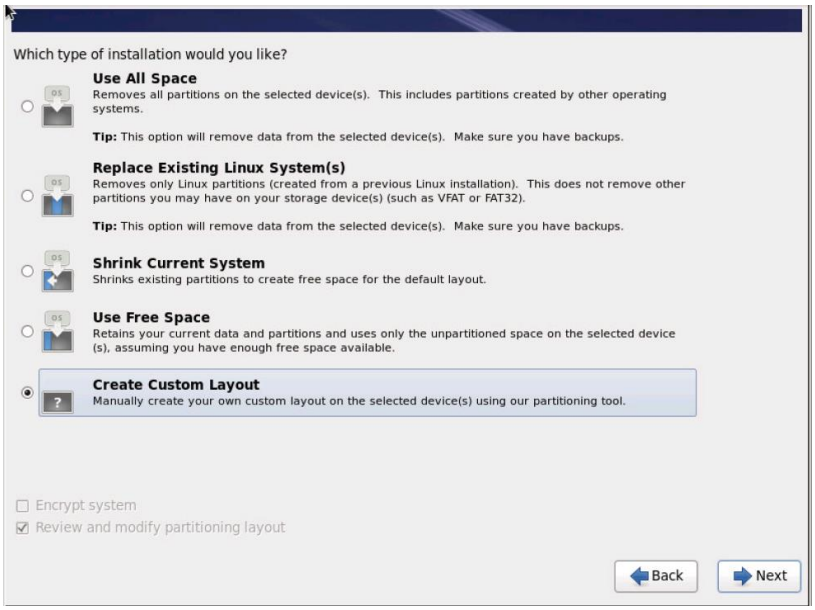



23. Click IPv4 Settings tab.

24. Select Manual.
25. Click Add.
26. Enter <<var_mgmt_temp_ip>> as the Address – This IP Address is only used temporarily.
27. Enter <<var_mgmt_netmask>> as the Netmask.
28. Enter <<var_mgmt_gw>> as the Gateway.
29. Select Connect automatically.
30. Click Apply.



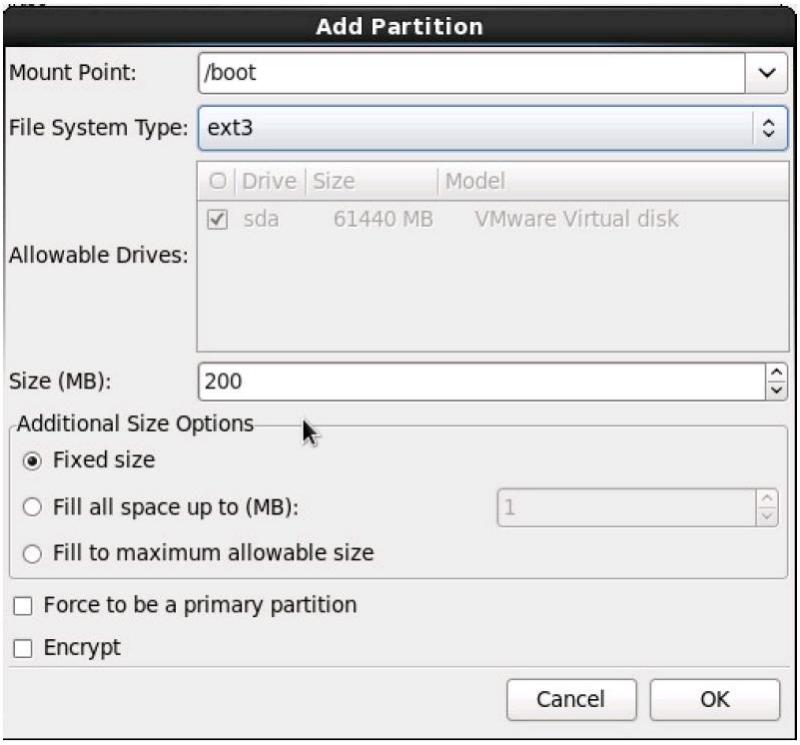

31. Click Close.
32. Click Next.
33. Select the right Time Zone and click Next.
34. Use <<var_mgmt_passwd>> as the root password, and click Next.
35. Select Create Custom layout for customized disk partitioning and click Next.




36. With the disk sdd create two partitions for /boot and root volume group:

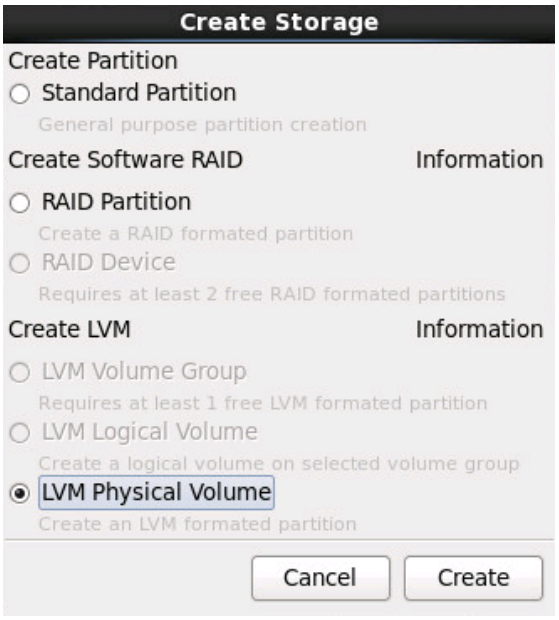
    a. Click Create, Choose Standard Partition and click Create.

    b. Choose /boot as mount point, File System Type ext3 and Size 200 MB and click OK.

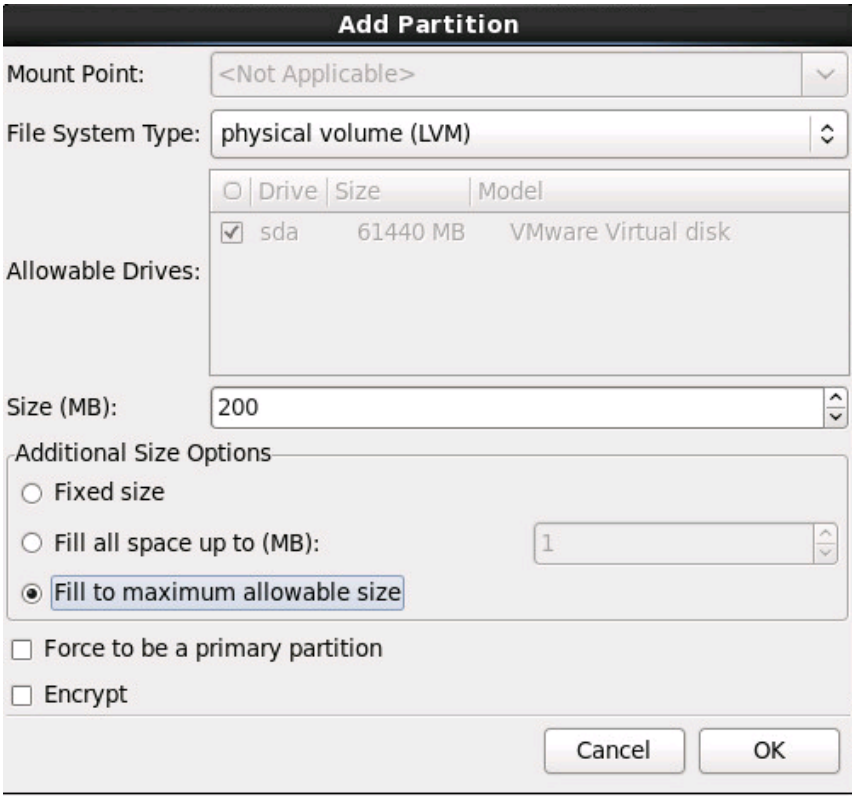



37. Click Create.

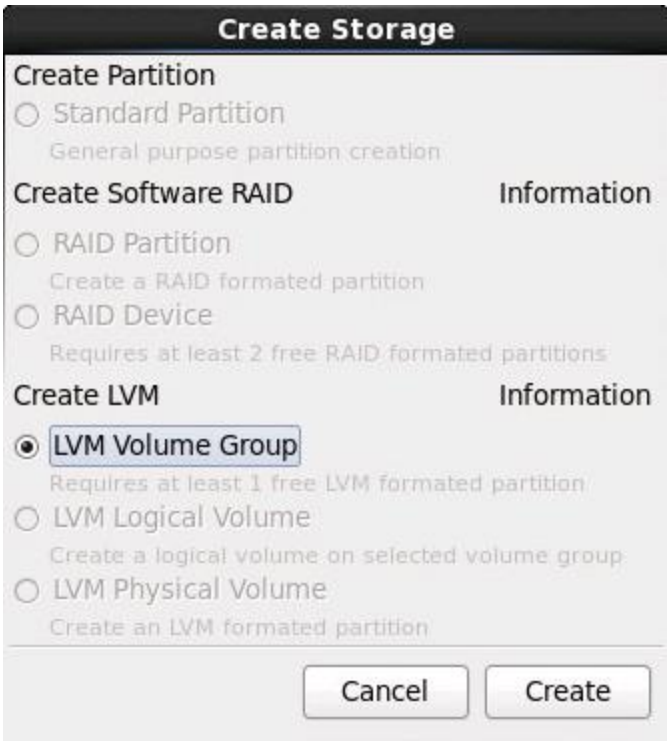
38. Choose LVM Physical Volume and click Create.



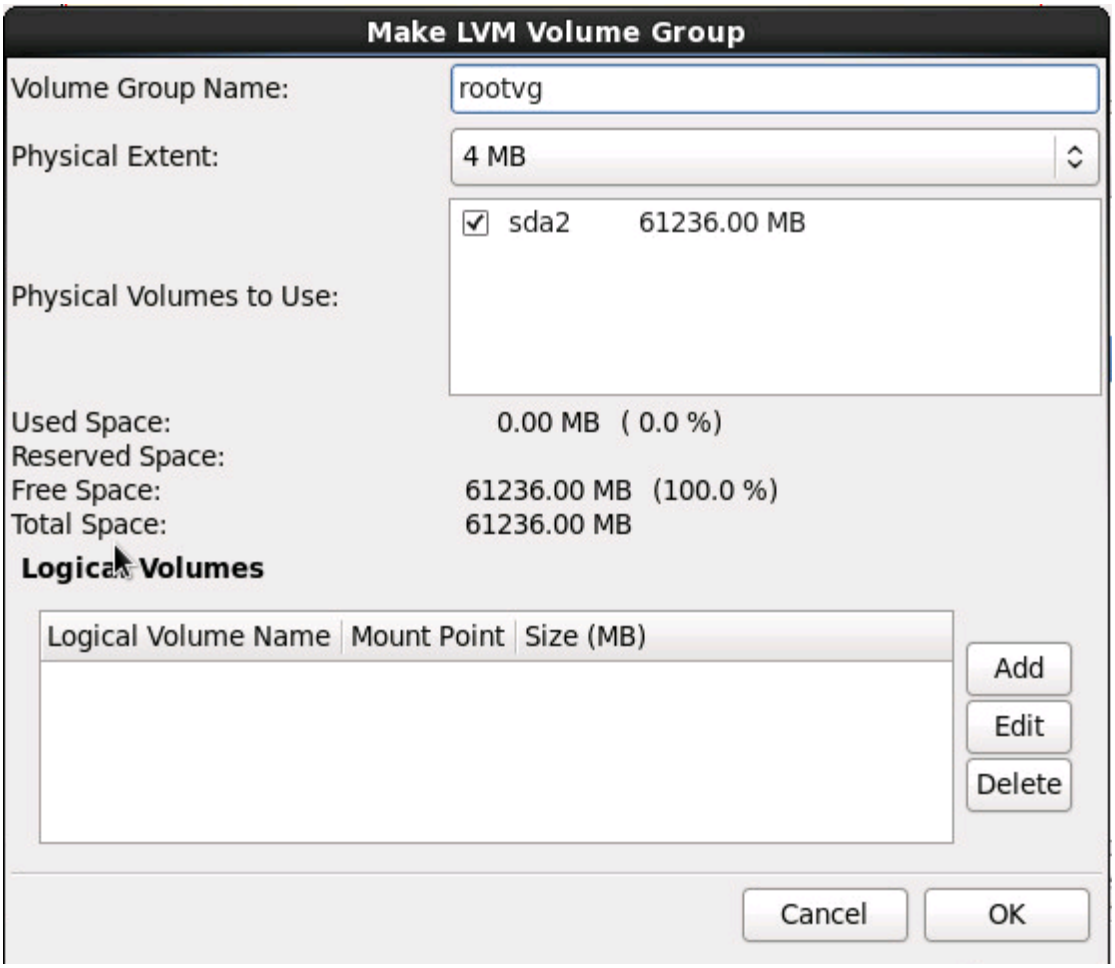

39. Select Fill to maximum allowable size and click OK.




40. Click Create, choose LVM Volume Group and click Create.

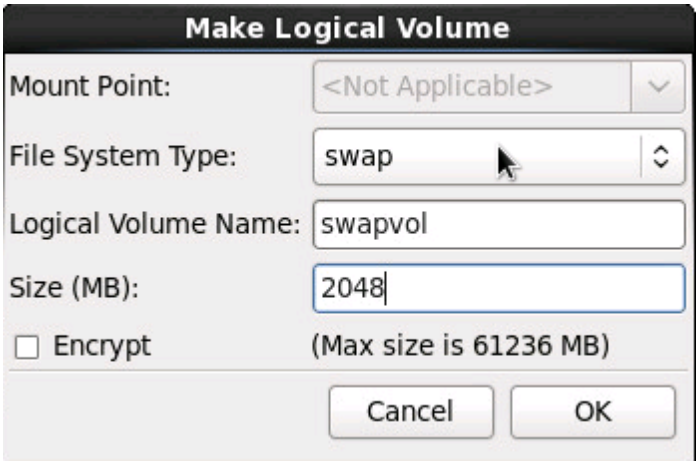



41. Enter rootvg as Volume Group Name.



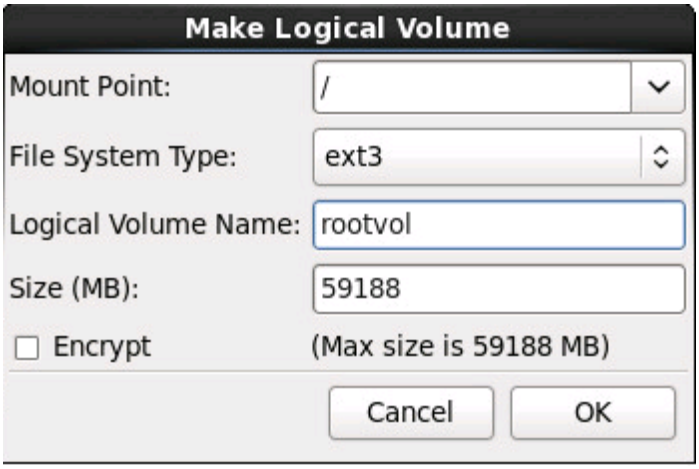

42. Click Add Under Logical Volumes.

43. Choose File System Type swap, enter Logical Volume Name swapvol and Size (MB) 2048. Click OK.



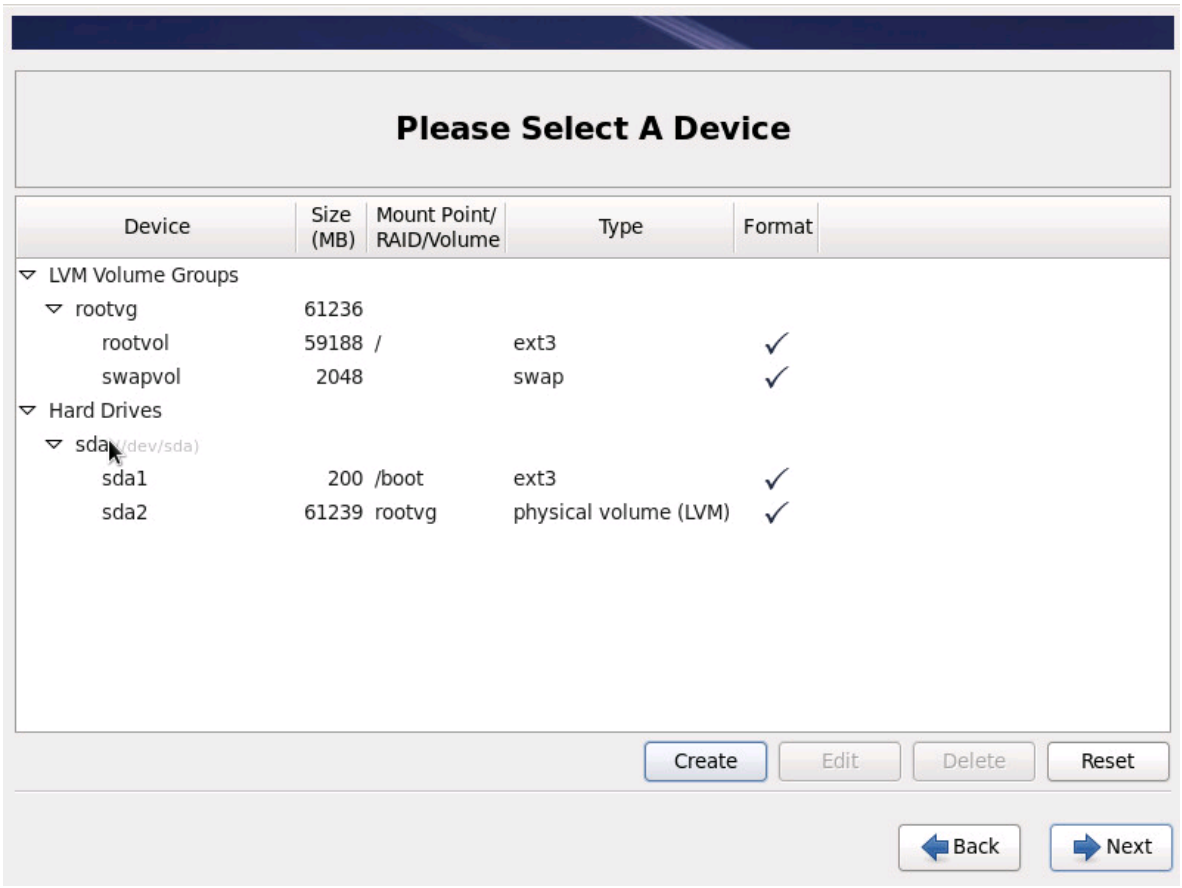

44. Click Add Under Logical Volumes.

45. Choose Mount Point /, File System Type ext3, enter Logical Volume Name rootvol and Leave Max Size. Click OK.




46. Click OK.

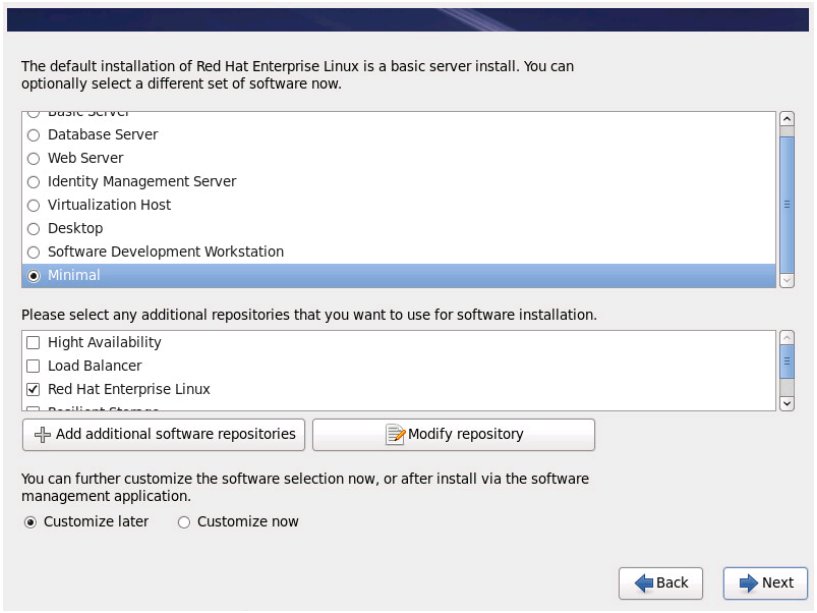
The final disk layout screen will look similar to the screenshot below:



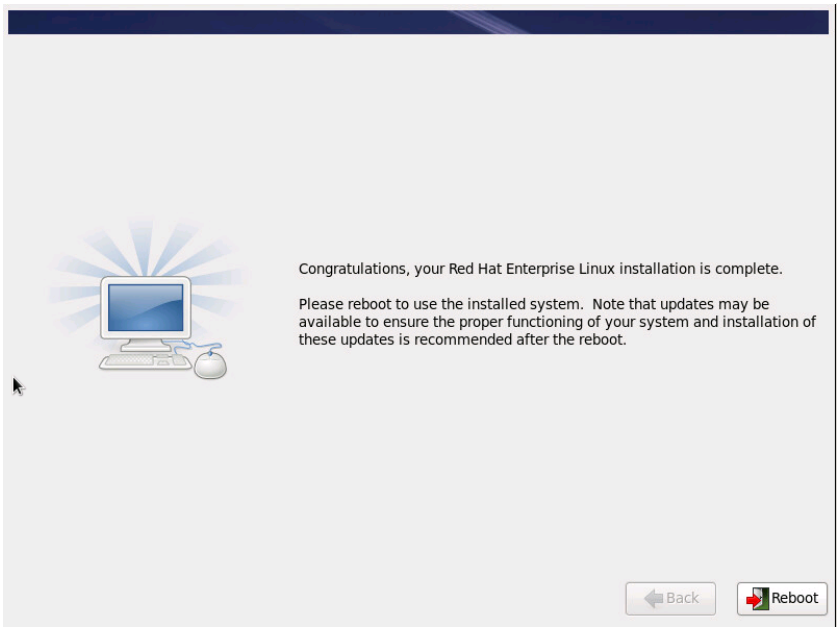

47. Click Next to proceed with the next step of the installation.

48. Select the installation mode as Minimal.

49. Click Next.




50. When the installation is complete, the server requires a reboot. Click Reboot.




51. Use a SSH client to login to the newly installed system as root.

52. Register the system with Red Hat to get updates:

```
subscription-manager register --username <<username>> --force --auto-attach
```

```
Password:

The system has been registered with ID: xxxxxxxx-xxxx-xxxx-xxxx-6a06be40e199

Installed Product Current Status:

Product Name: Red Hat Enterprise Linux Server

Status:       Subscribed
```

53. Install all security updates to the system:

```
yum -y install yum-security

yum --security update

yum -y update kernel kernel-firmware

yum -y groupinstall base
```

54. Install dependencies in accordance with the SAP HANA Server Installation and Update Guide and the numactl package if the benchmark HWCCT is used :

```
yum install gtk2 libicu xulrunner ntp sudo tcsh libssh2 expect cairo graphviz
iptraf krb5-workstation krb5-libs.i686 nfs-utils lm_sensors rsyslog compat-sap-
c++ openssl098e openssl PackageKit-gtk-module libcanberra-gtk2 libtool-ltdl xauth
compat-libstdc++-33 numactl
```

55. Disable SELinux:

```
vi /etc/sysconfig/selinux # This file controls the state of SELinux on the
system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - No SELinux policy is loaded.

SELINUX=disabled

# SELINUXTYPE= can take one of these two values:

# targeted - Targeted processes are protected,

# mls - Multi Level Security protection.

SELINUXTYPE=targeted
```

56. Disable kdump Service:

```
service kdump stop
```

```
chkconfig kdump off
```

57. Compat-sap-c++ Install the most important package compat-sap-c++ from the RHEL for SAP HANA:

```
rpm -ivh tuned-0.2.19-13.el6_6.1.noarch.rpm
rpm –ivh tuned-profiles-sap-hana-0.2.19-13.el6_6.1.noarch.rpm
tuned-adm profile sap-hana-vmware
```

58. Sysctl.conf: The following parameters must be set in /etc/sysctl.conf

```
# Parameters for HANA
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.ip_local_port_range=40000 61000
net.ipv4.neigh.default.gc_thresh1=256
net.ipv4.neigh.default.gc_thresh2=1024
net.ipv4.neigh.default.gc_thresh3=4096
net.ipv6.neigh.default.gc_thresh1=256
net.ipv6.neigh.default.gc_thresh2=1024
net.ipv6.neigh.default.gc_thresh3=4096
kernel.shmmax=137438953472
kernel.shmall=33554432
# Next line modified for SAP HANA Database on 2014.11.05_18.49.07
kernel.shmmni=524288
kernel.msgmni=32768
kernel.sem=1250 256000 100 8192
kernel.sysrq=1
vm.swappiness=60
# Next line modified for SAP HANA Database on 2014.11.05_18.49.07
vm.max_map_count=102000000
vm.memory_failure_early_kill=1
fs.file-max=20000000
fs.aio-max-nr=458752
```

```
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

59. Add the following line into /etc/modprobe.d/sunrpc-local.conf, Create the file, if it does not exist:

```
sunrpc.tcp_max_slot_table_entries = 128
```

60. For compatibility reasons, four symbolic links are required:

```
ln -s /usr/lib64/libssl.so.0.9.8e /usr/lib64/libssl.so.0.9.8
ln -s /usr/lib64/libssl.so.1.0.1e /usr/lib64/libssl.so.1.0.1
ln -s /usr/lib64/libcrypto.so.0.9.8e /usr/lib64/libcrypto.so.0.9.8
ln -s /usr/lib64/libcrypto.so.1.0.1e /usr/lib64/libcrypto.so.1.0.1
```

61. Transparent Hugepages In the file /boot/grub/grub.conf add the kernel command line argument:

```
transparent_hugepage=never
```

62. Use a tuned profile to minimize latencies:

```
yum -y install tuned
tuned-adm profile latency-performance
chkconfig tuned on
service tuned start
```

63. Create User-Group sapsys:

```
groupadd –g 401 sapsys
```

64. Disable Crash Dump :

```
chkconfig abrtd off

chkconfig abrt-ccpp off

service abrtd stop

service abrt-ccpp stop
```

65. Disable core file creation. To disable core dumps for all users, open /etc/security/limits.conf, and add the line:

```
* soft core 0

* hard core 0
```

66. Edit the /boot/grub/menu.lst and append the below parameter to the kernel line per SAP Note:

```
intel_idle.max_cstate=0
```

67. Reboot the system:

```
reboot
```

### Install VMware Tools

To install the VMware tools, complete the following steps:

1. Guest > Install/Upgrade VMware Tools and click OK.
2. Mount cdrom.

```
mount /dev/cdrom /mnt
```

3. Copy the Compiler gzip tar file to a temporary local directory, run:

```
cp /mnt/VMwareTools-<<version>>.tar.gz /tmp/
```

4. Untar the copied file:

```
cd /tmp

tar -zxvf VMwareTools-<<version>>.tar.gz
```

5. Change directory to extracted vmware-tools-distrib and run the vmware-install.pl PERL script.

```
cd /tmp/vmware-tools-distrib

./vmware-install.pl
```

6. Follow the onscreen instruction to complete the VMware tools installation.
7. Reboot the VM.

8. To create the VM template, clean up the master OS image.

9. Log into the server.

10. Stop logging services:

```
/sbin/service rsyslog stop
/sbin/service auditd stop
```

11. Remove old kernels:

```
/bin/package-cleanup --oldkernels --count=1
```

12. Clean out yum:

```
/usr/bin/yum clean all
```

13. Remove the Red Hat Registration information:

```
subscription-manager unregister
```

14. Clear the System Logs:

```
/usr/sbin/logrotate –f /etc/logrotate.conf
/bin/rm –f /var/log/*-???????? /var/log/*.gz
/bin/rm –f /var/log/dmesg.old
/bin/rm -rf /var/log/anaconda
/bin/cat /dev/null > /var/log/audit/audit.log
/bin/cat /dev/null > /var/log/wtmp
/bin/cat /dev/null > /var/log/lastlog
/bin/cat /dev/null > /var/log/grubby
```

15. Remove the SSH keys:

```
rm /etc/ssh/*key*
```

16. Clear the Ethernet Persistent network information:

```
cat /dev/null > /etc/udev/rules.d/70-persistent-net.rules
```

17. Remove the Ethernet configuration files:

```
rm /etc/sysconfig/network/ifcfg-eth*
```

18. Remove the default gateway configuration:

```
rm /etc/sysconfig/network/routes
```

19. Clean /tmp out:

```
/bin/rm –rf /tmp/*
/bin/rm –rf /var/tmp/*
```

20. Zero out all free space on the file systems, this reduce the required disk space for deployed VMs based on the template. You can use this script to do so or do it manually:

```
#!/bin/sh
# Determine the version of RHEL
COND=`grep -i Taroon /etc/redhat-release`
if [ "$COND" = "" ]; then
        export PREFIX="/usr/sbin"
else
        export PREFIX="/sbin"
fi

FileSystem=`grep ext /etc/mtab| awk -F" " '{ print $2 }'`

for i in $FileSystem
do
        echo $i
        number=`df -B 512 $i | awk -F" " '{print $3}' | grep -v Used`
        echo $number
        percent=$(echo "scale=0; $number * 98 / 100" | bc )
        echo $percent
        dd count=`echo $percent` if=/dev/zero of=`echo $i`/zf
        /bin/sync
        sleep 15
        rm -f $i/zf
done

VolumeGroup=`$PREFIX/vgdisplay | grep Name | awk -F" " '{ print $3 }'`
```

```
for j in $VolumeGroup
do
        echo $j
        $PREFIX/lvcreate -l `$PREFIX/vgdisplay $j | grep Free | awk -F" " '{
print $5 }'` -n zero $j
        if [ -a /dev/$j/zero ]; then
                cat /dev/zero > /dev/$j/zero
                /bin/sync
                sleep 15
                $PREFIX/lvremove -f /dev/$j/zero
        fi
done
```

21. Specify the system as unconfigured:

```
touch /.unconfigured
```

22. Remove the root user's shell history:

```
/bin/rm -f ~root/.bash_history
unset HISTFILE
```

23. Remove the root user's SSH history:

```
/bin/rm -rf ~root/.ssh/
/bin/rm -f ~root/anaconda-ks.cfg
*
```

24. Shutdown the system:

```
halt
```

## Migrate Virtual Machine into a Virtual Machine Template

For virtual machine deployments, you need to migrate the virtual machine into a virtual machine template. To migrate a virtual machine into a virtual machine template, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.

4. Click the virtual machine.
5. Click Actions > All vCenter Actions.
6. Click Convert to Template.

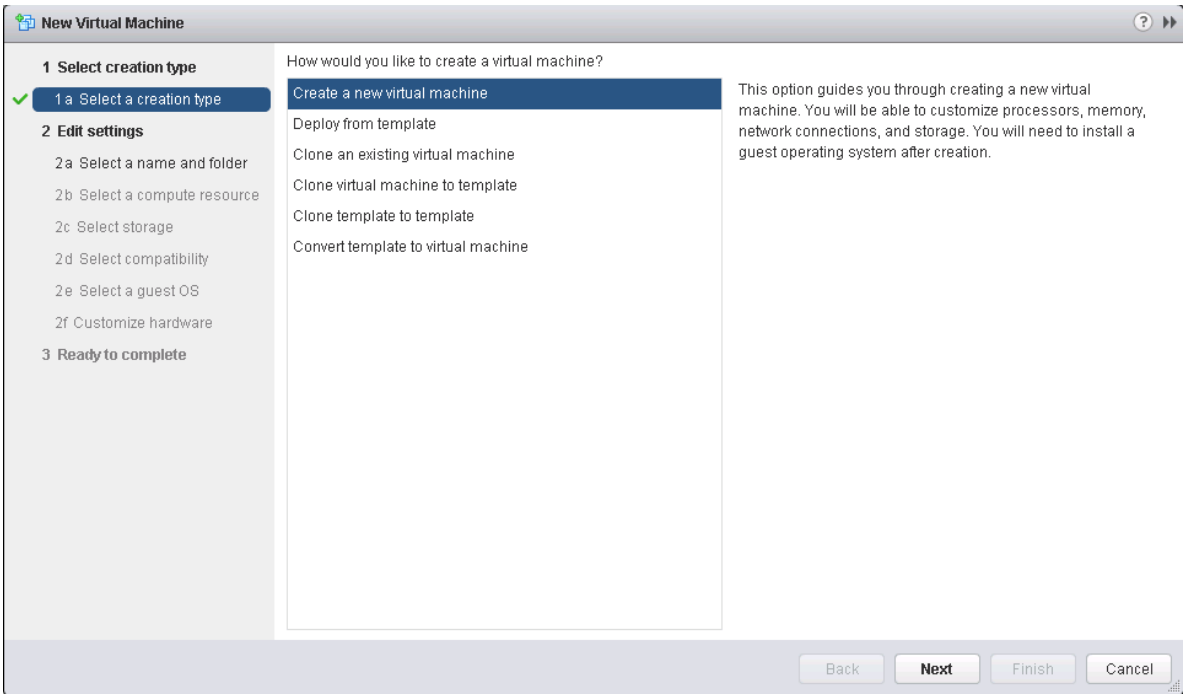
## Virtual Machine Template with Microsoft Windows

Creating the virtual machine template requires two steps. The first step is to install a Virtual Machine and to configure all settings for SAP Applications. The second step is to convert the Virtual Machine into a Virtual Machine Template.

### Create a Virtual Machine for Virtualized Applications

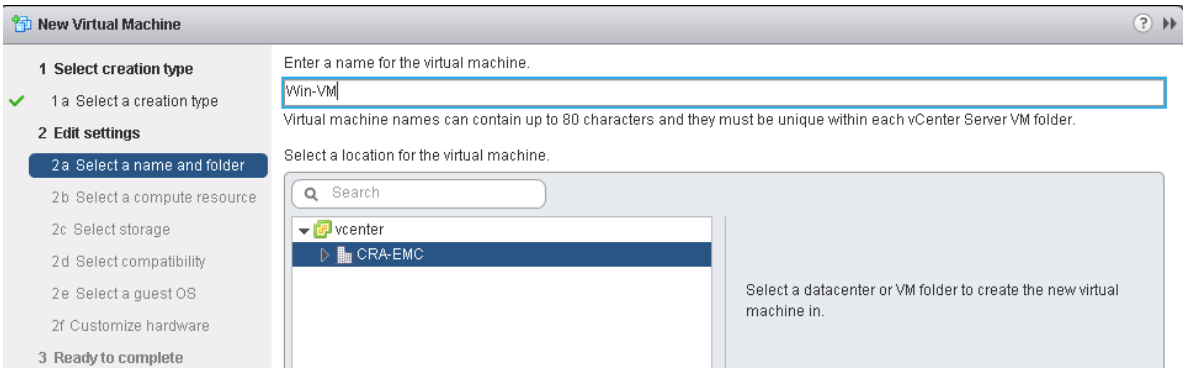
To build a virtual machine  for Microsoft Windows based Applications, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click <<var_vc_cluster1_name>>.
5. Click Actions.
6. Select New Virtual Machine to start the Wizard.
7. Click Next.



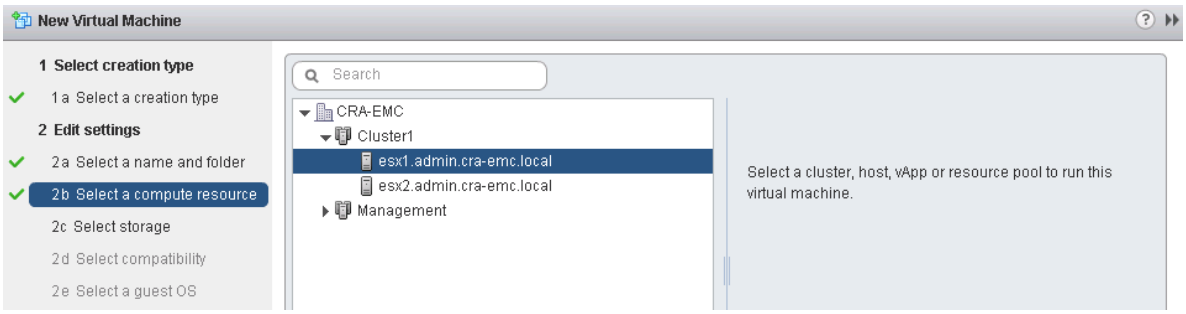

8. Enter <<var_win_vm_name>> as the Name of the Virtual Machine.

9. Click Next.



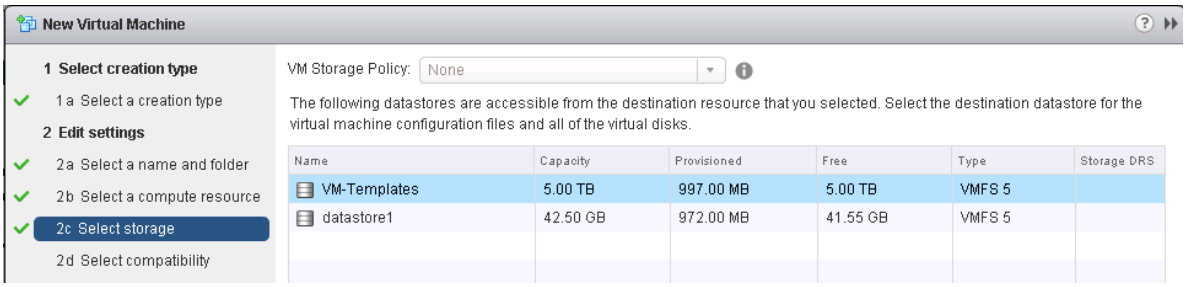

10. Select Cluster1 or a ESX host within Cluster 1 as compute resource.

11. Click Next.



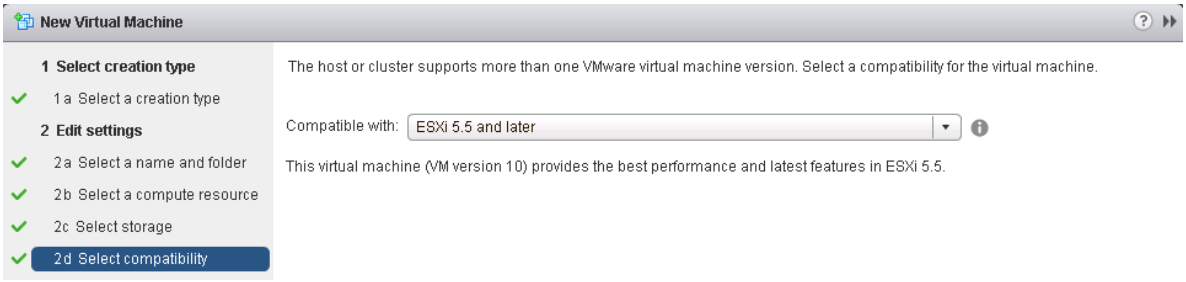

12. Select << >> as the storage.

13. Click Next.




14. For the Compatible with option select ESXi 5.5 or later.

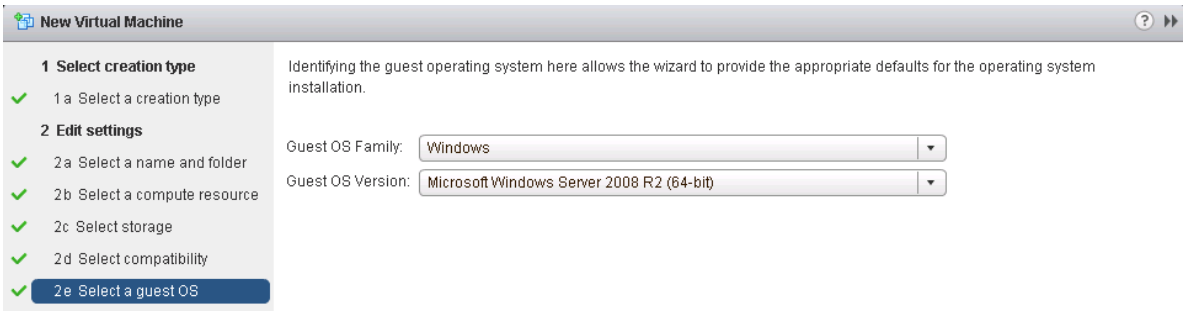
15. Click Next.



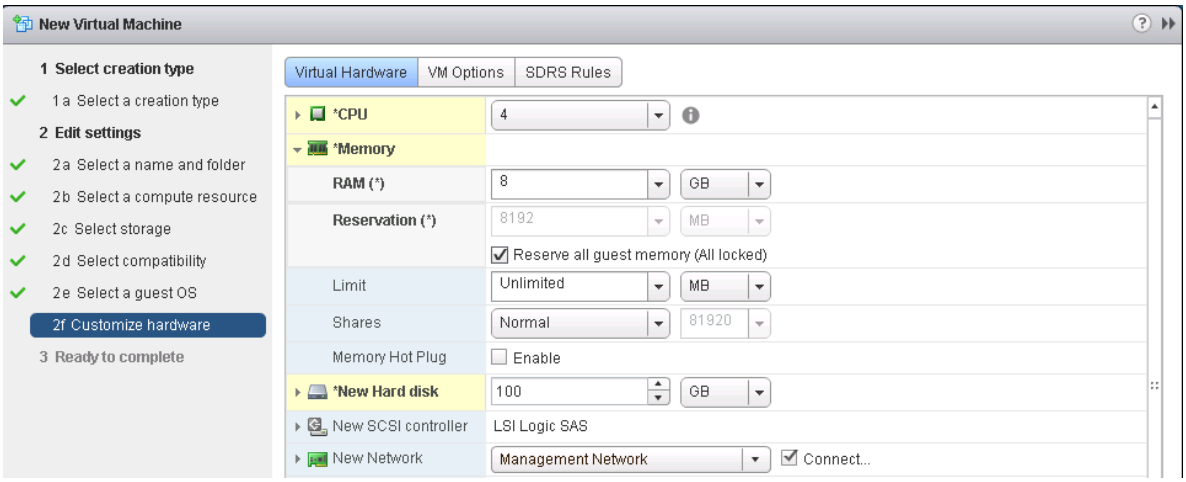

16. Select Windows from the Drop-down menu for Guest OS Family.

17. Select Microsoft Windows Server 2008 R2 (64-bit) as the Guest OS Version.

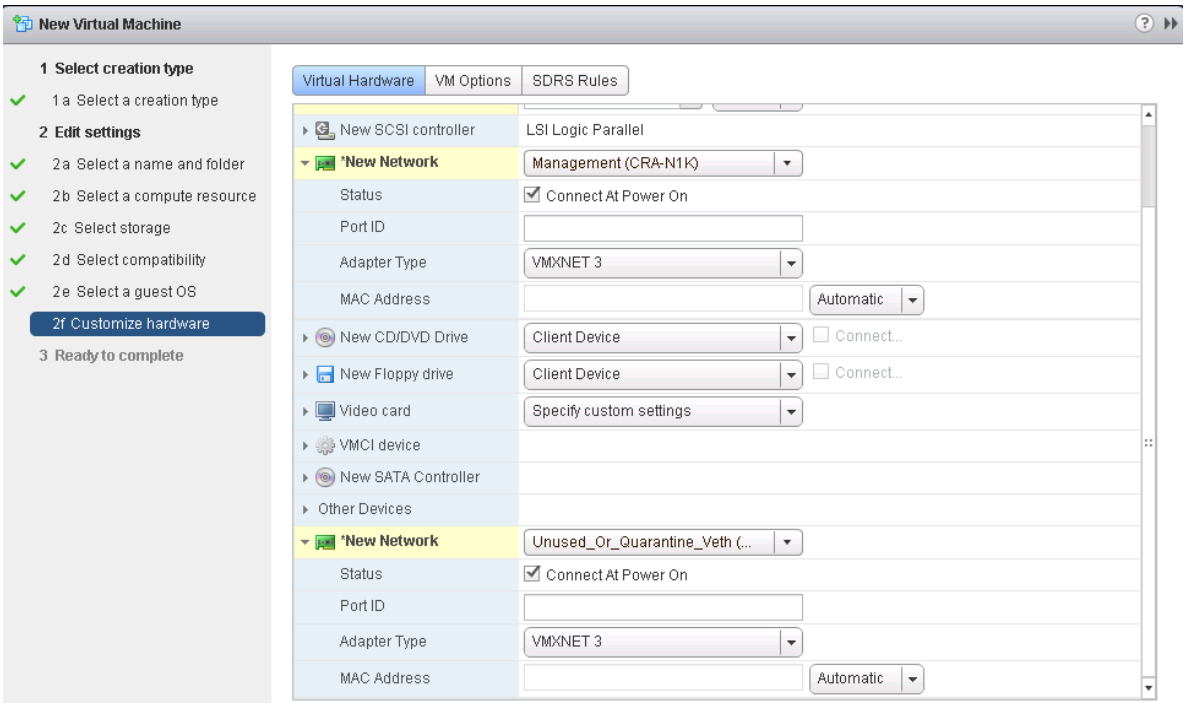
18. Click Next.




19. Select 4 as the # of CPUs.
20. Enter 8 and GB for the Memory.
21. Click the Arrow left of Memory.
22. Select the checkbox to Reserve all guest memory (All locked).
23. Enter 100 and GB for the Hard disk.
24. Select Network from the New device drop-down menu.
25. Click Add.

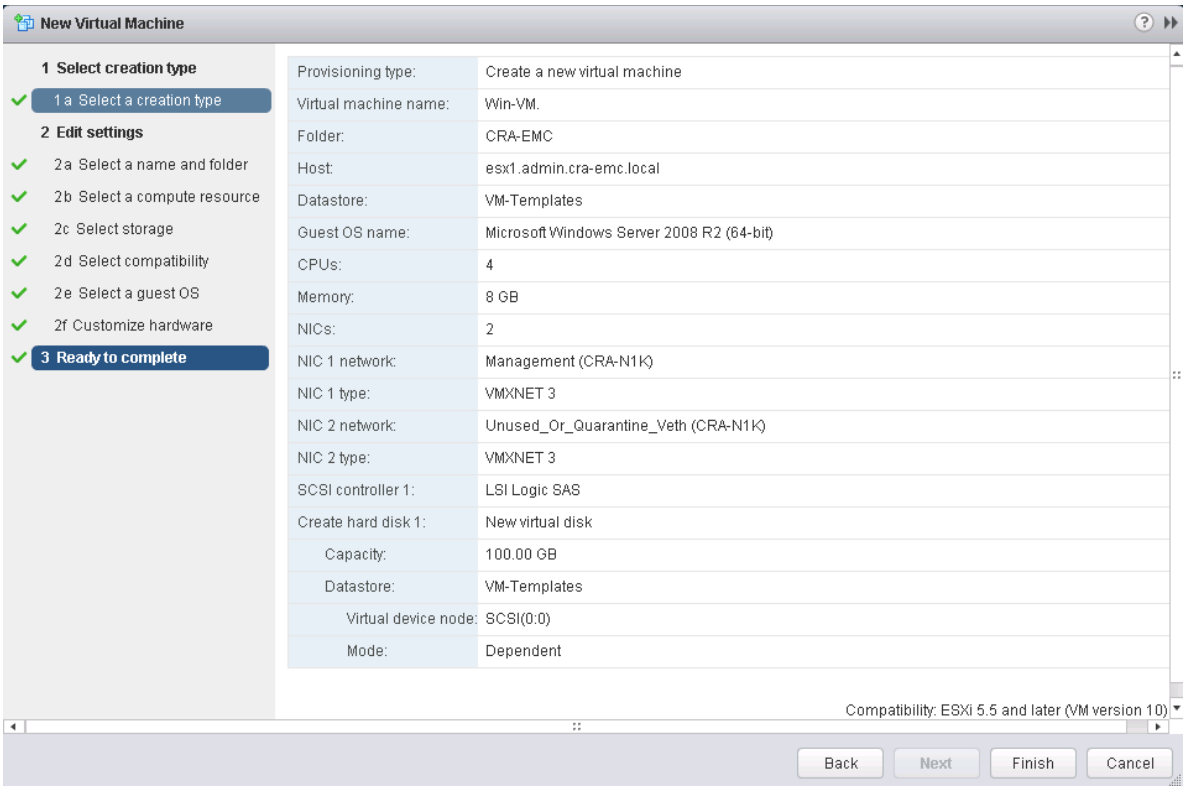



26. Select Management (CRA-N1K) for the first New Network devices.
27. Select Unused_Or_Quarantine_Veth for the second New Network device.
28. Click the Arrow left of both Network Cards.
29. Select VMXNET3 as the Adapter Type for all network cards.
30. Click Next.




31. Review the information.

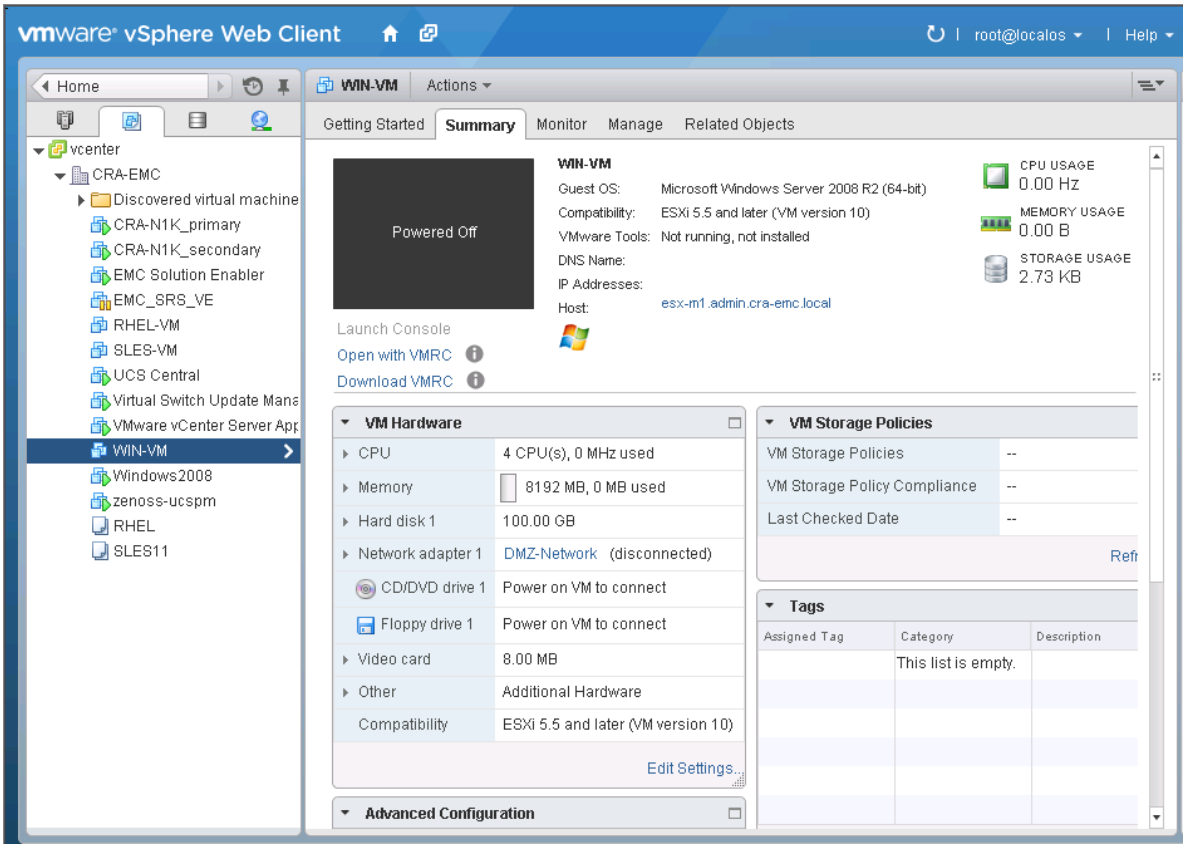
32. Click Finish.



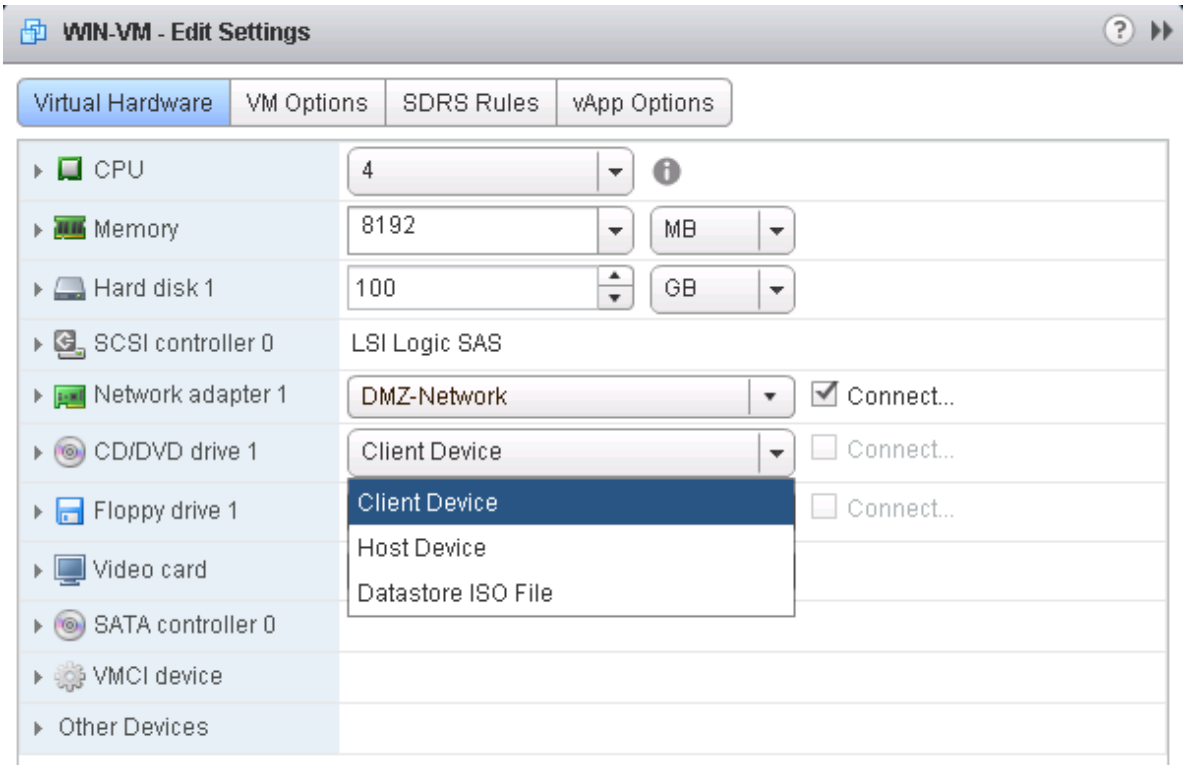
## Install and Configure the Microsoft Windows Server for Virtualized SAP Applications

To install and configure the Microsoft Windows server, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Select <<var_vc_win_vm_name>>.
5. Click Summary Tab in the right pane.
6. Click Edit Settings at the bottom of the VM Hardware section.




7. Click the drop-down menu for CD/DVD drive 1.
8. Select Datastore ISO File.

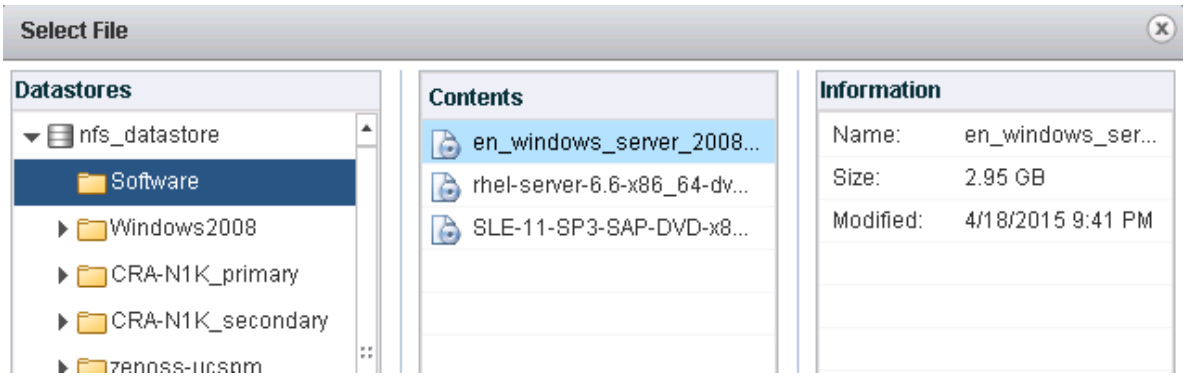



9. Select the Datastore Software.

10. Click directory where the Red Hat Enterprise Linux ISO is located.

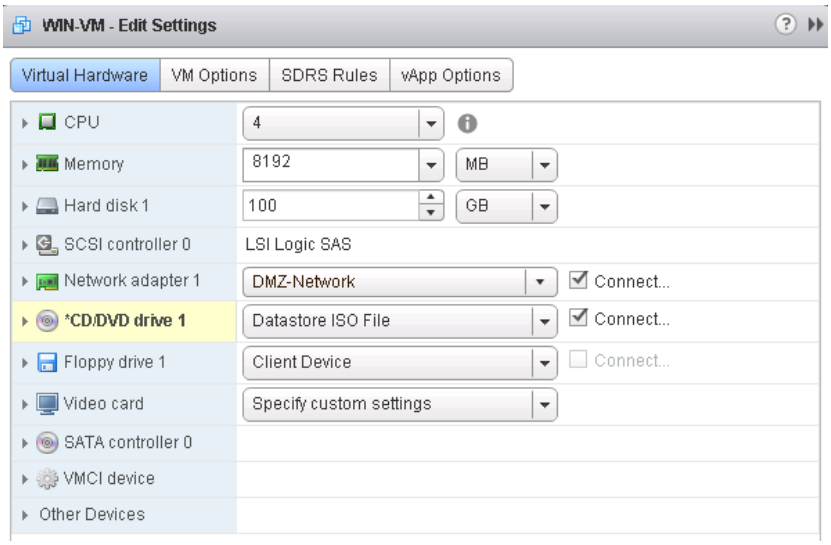
11. Select the ISO file.

12. Click OK.




13. Select the Connect checkbox.

14. Click OK.




15. Click Actions.
16. Select Power On.
17. Click Launch Console.

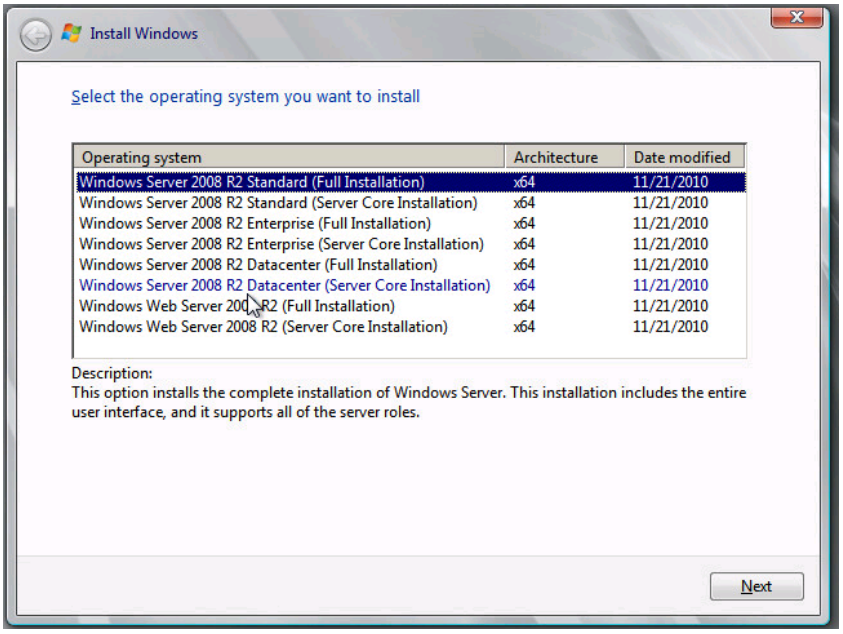
The system automatically starts from the Microsoft Windows Server DVD.

18. Select the Language and Keyboard settings that fits best for you.
19. Click Next.
20. Click Install now.



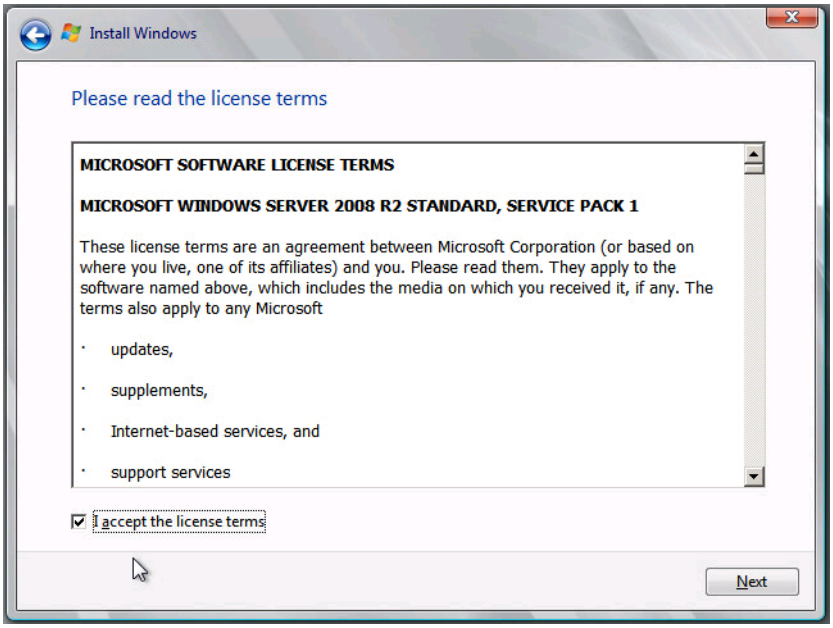
21. Select the Operating System Edition to install.

22. Click Next.




23. Accept the License Terms.

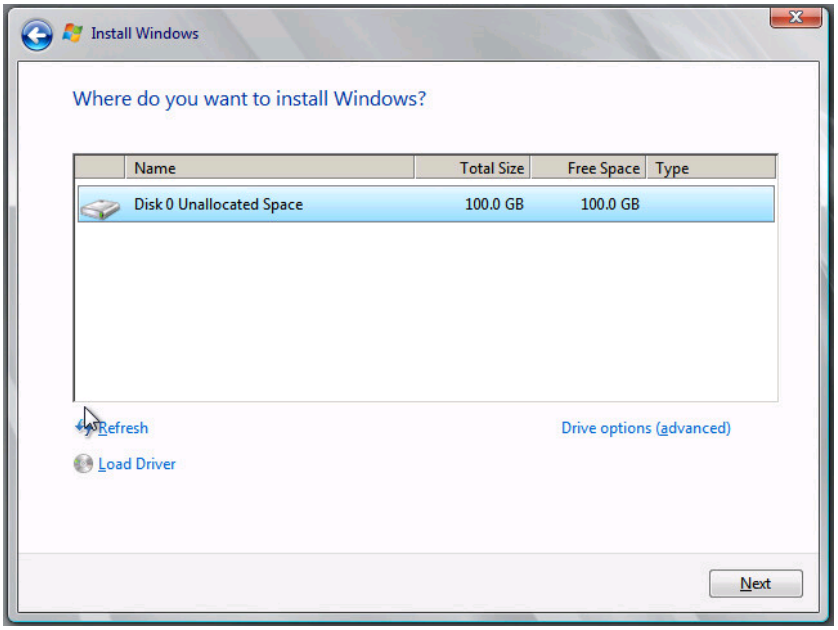
24. Click Next.



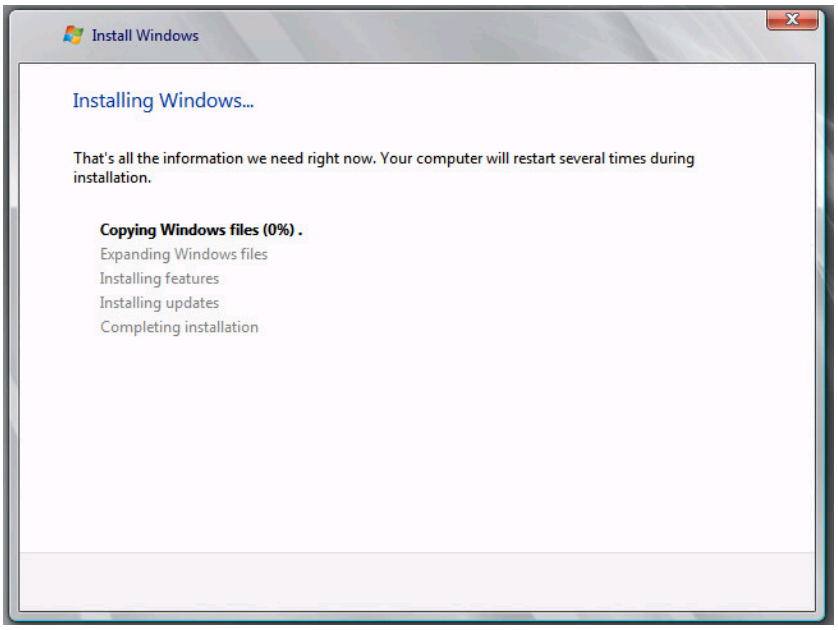

25. Select Custom (advanced).

26. Disk 0 with 100 GB must be shown as the destination.

27. Click Next.

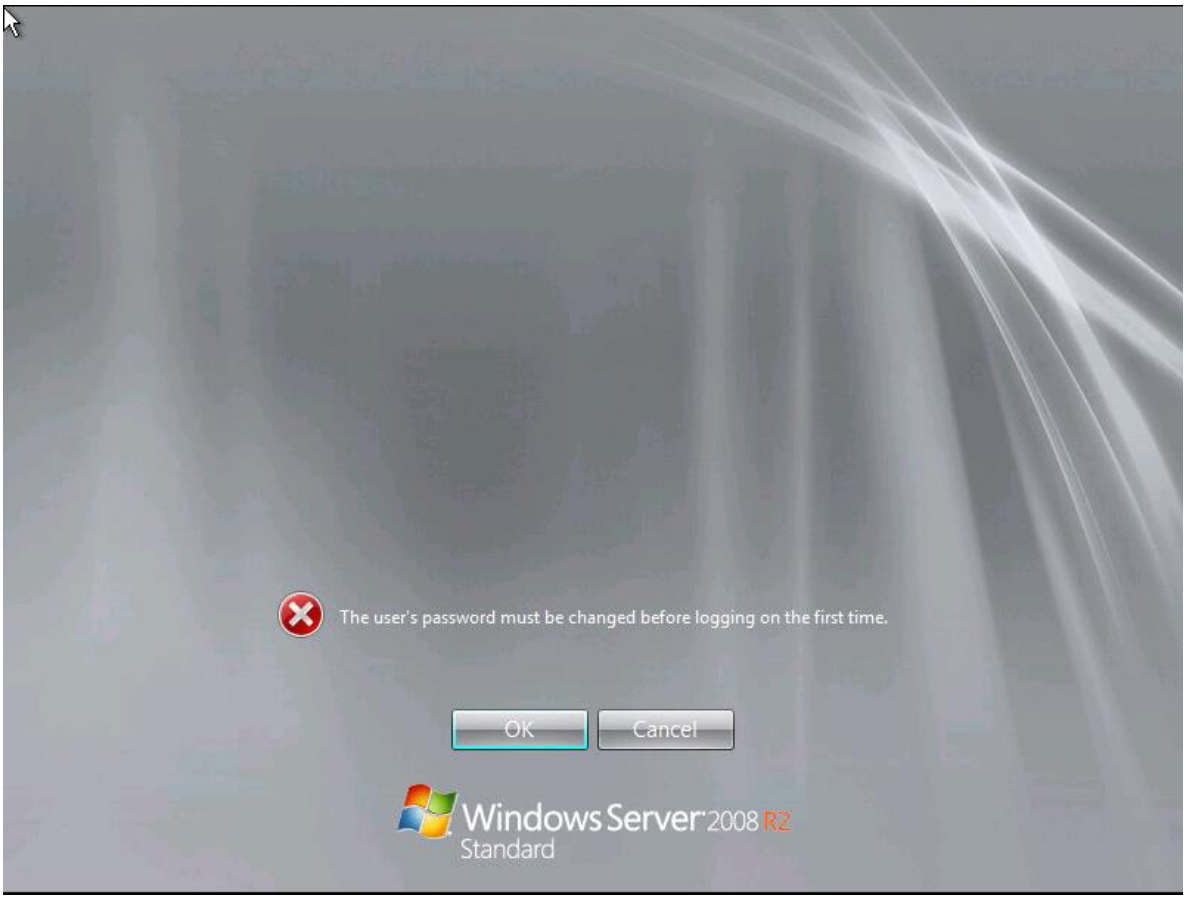



The installation starts.




The system automatically reboots as part of the installation process.

28. Click OK.




29. Enter <<var_mgmt_passwd>> as the new password for Administrator and confirm it.

30. Press Enter.

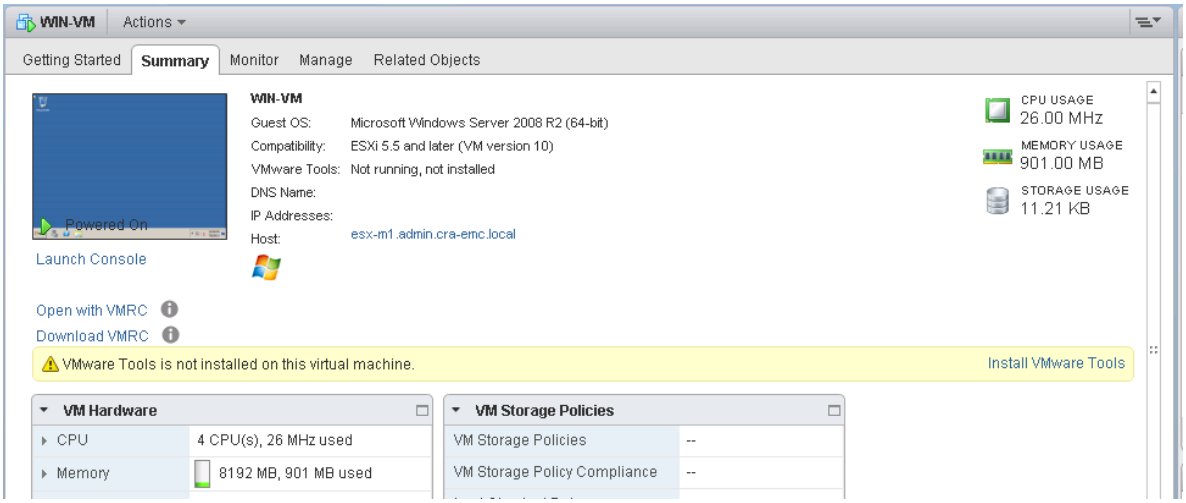
31. Click OK.



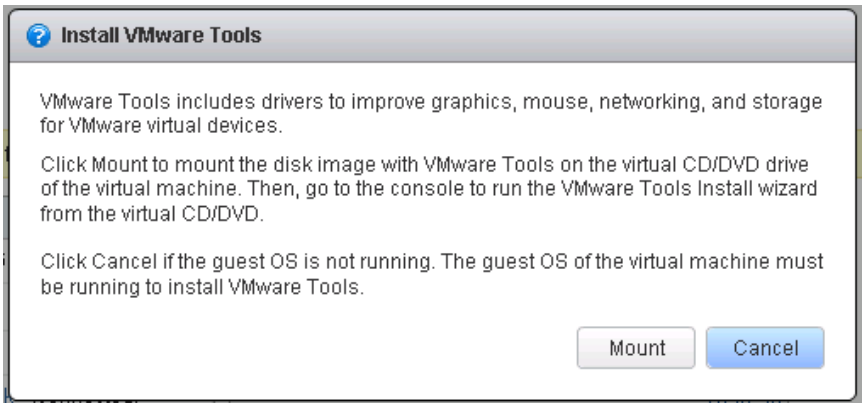

32. Install the VMware tools on the system.

33. In the vSphere Web Client window, select the virtual machine.

34. Click Install VMware Tools in the Yellow Warning bar.




35. Click Mount.

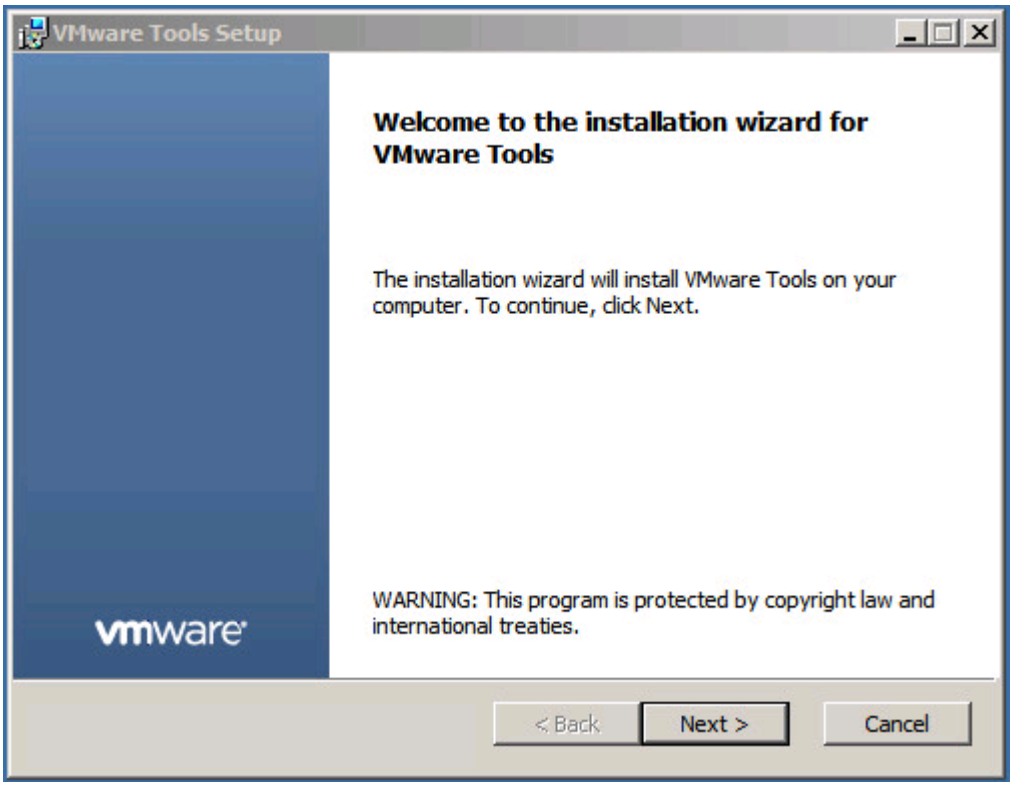



36. Go Back to the Console Window.

37. Click Run setup64.exe.



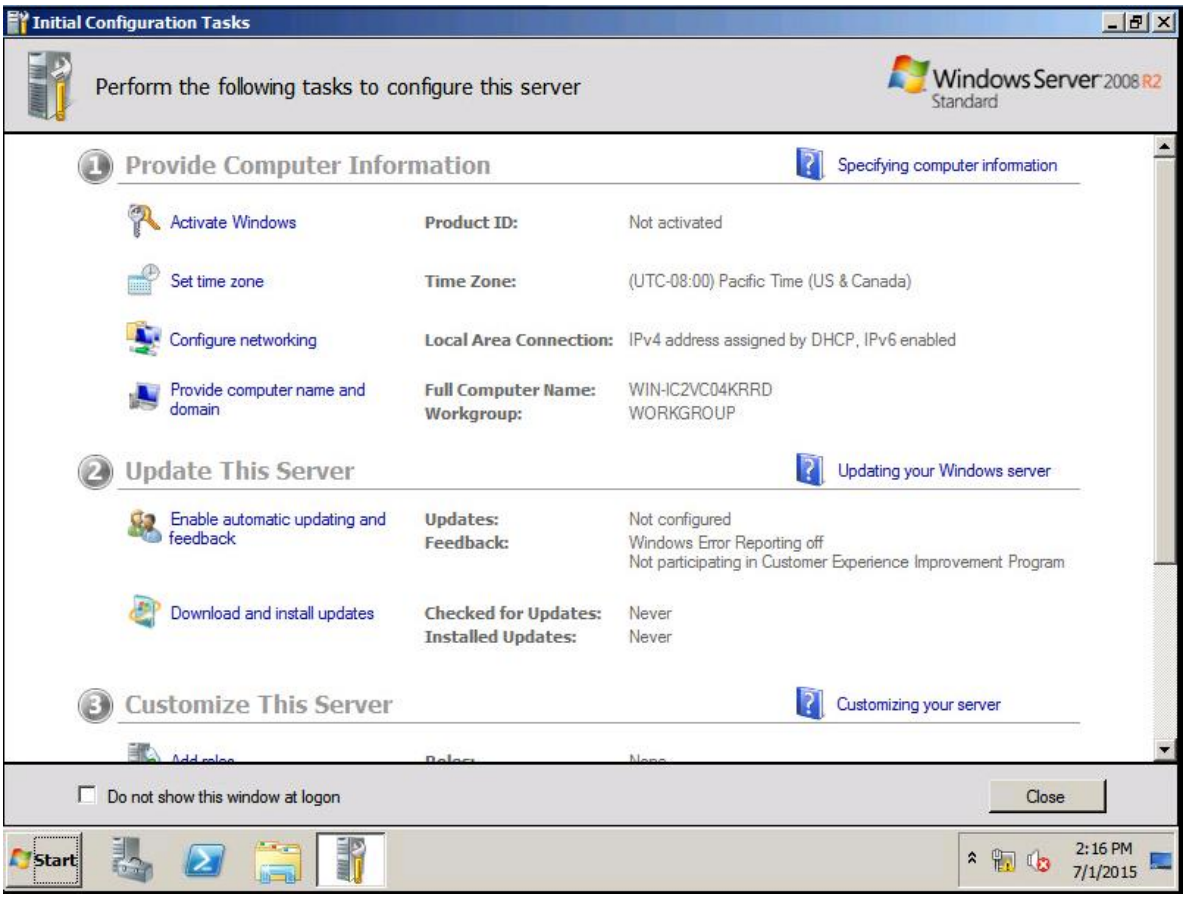

38. Follow the installation steps shown on the screen.




39. Click Yes to reboot the System.

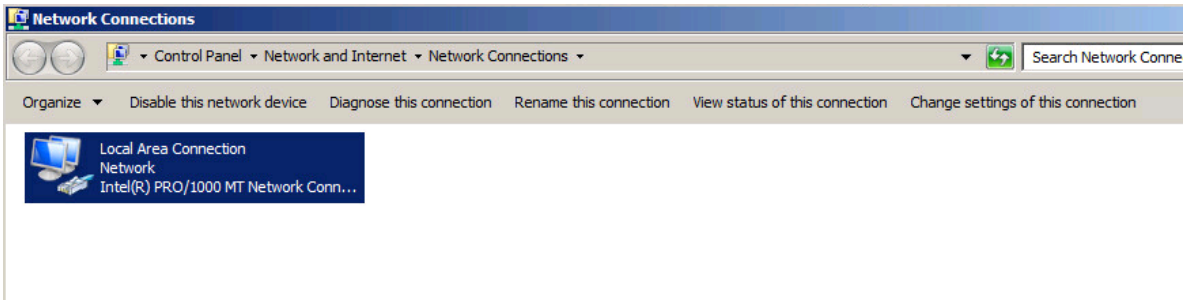
40. Log in to the System as Administrator.

41. In the Initial Configuration Tasks Window click Configure Networking.



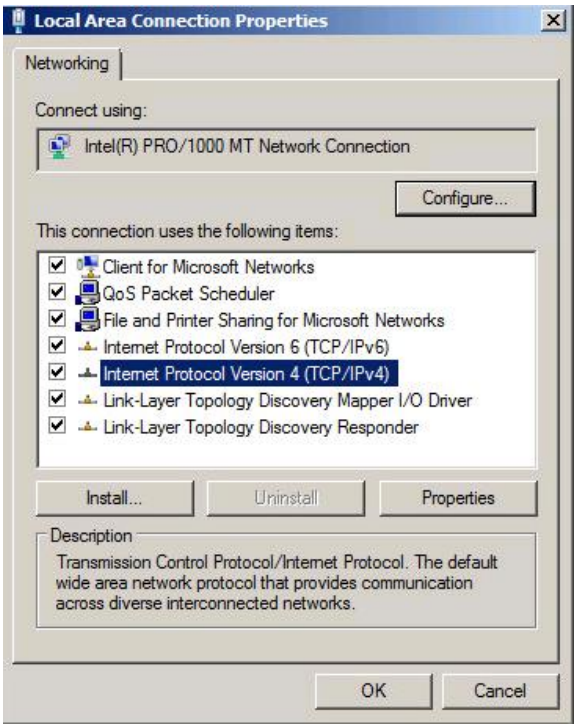

42. Select the Local Area Connection.

43. Click Change settings of this connection in the menu bar.

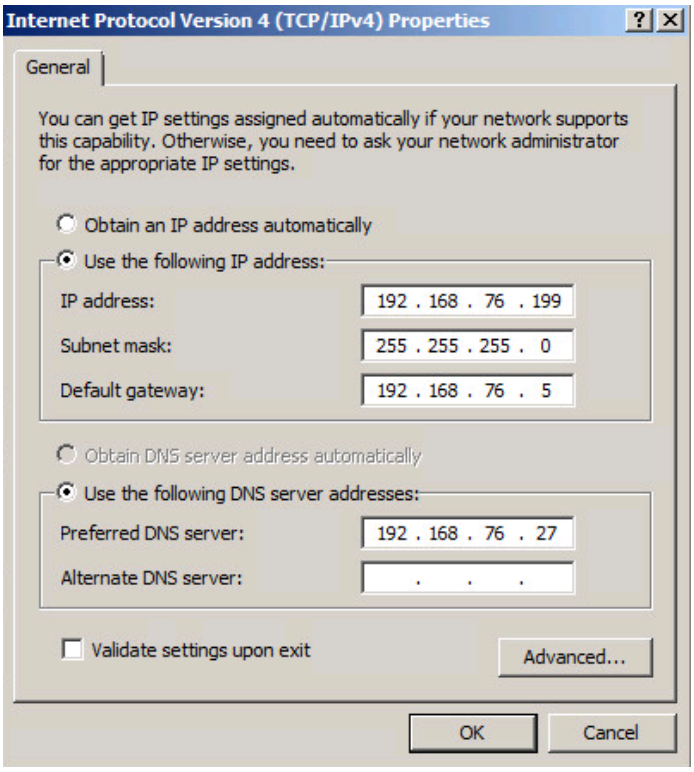



44. Select Internet Protocol Version 4 (TCP/IPv4).

45. Click Properties.

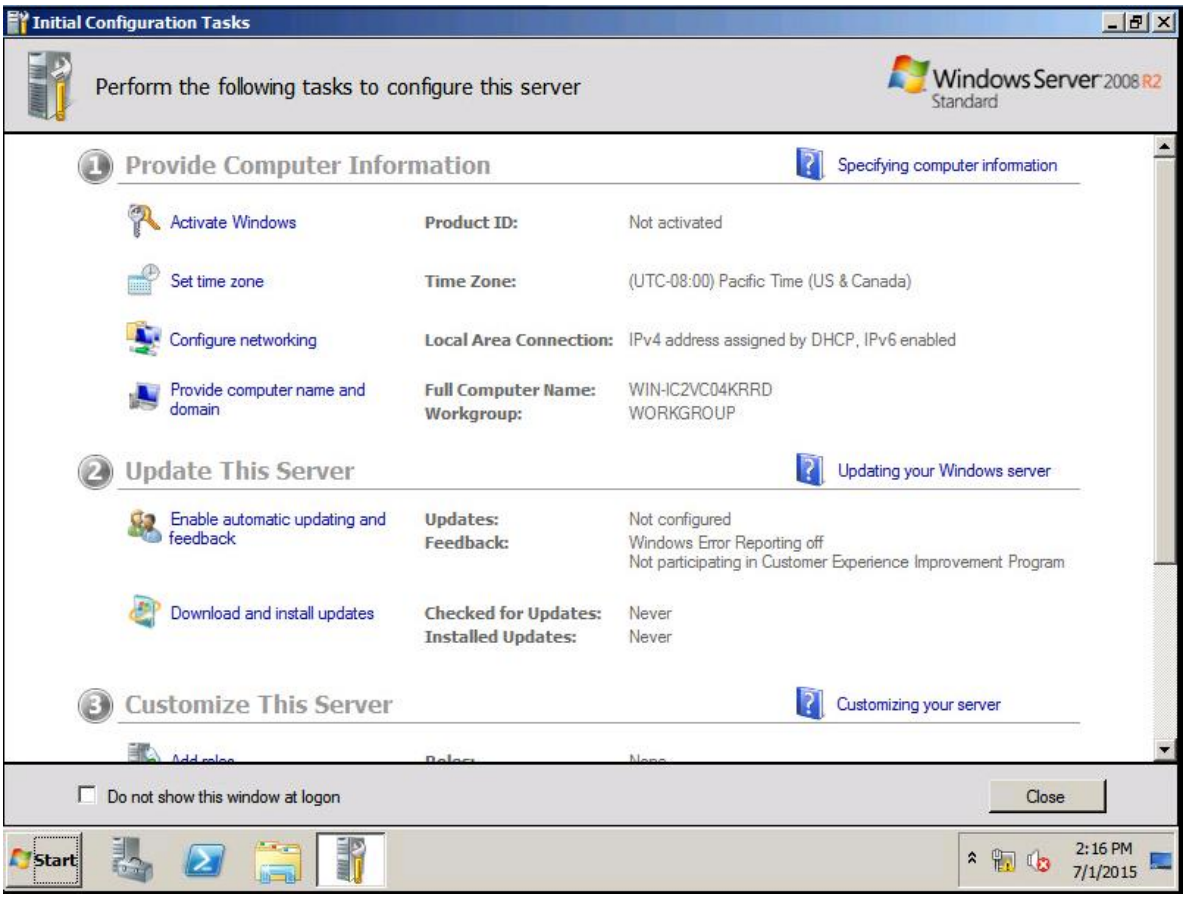



46. Enter <<>> as the IP Address.
47. Enter <<>> as  the Subnet mask.
48. Enter <<>> as the Default Gateway.
49. Enter <<>> as the Preferred DNS Server.
50. Click OK.




51. Click Close.
52. Close the Network Connections Window.
53. Configure the Microsoft Windows Server system as required to meet your best practices:

— Service Packs
— Virus Scanner
— Enable Remote Desktop
— Disable Windows Firewall
— Other tools and settings



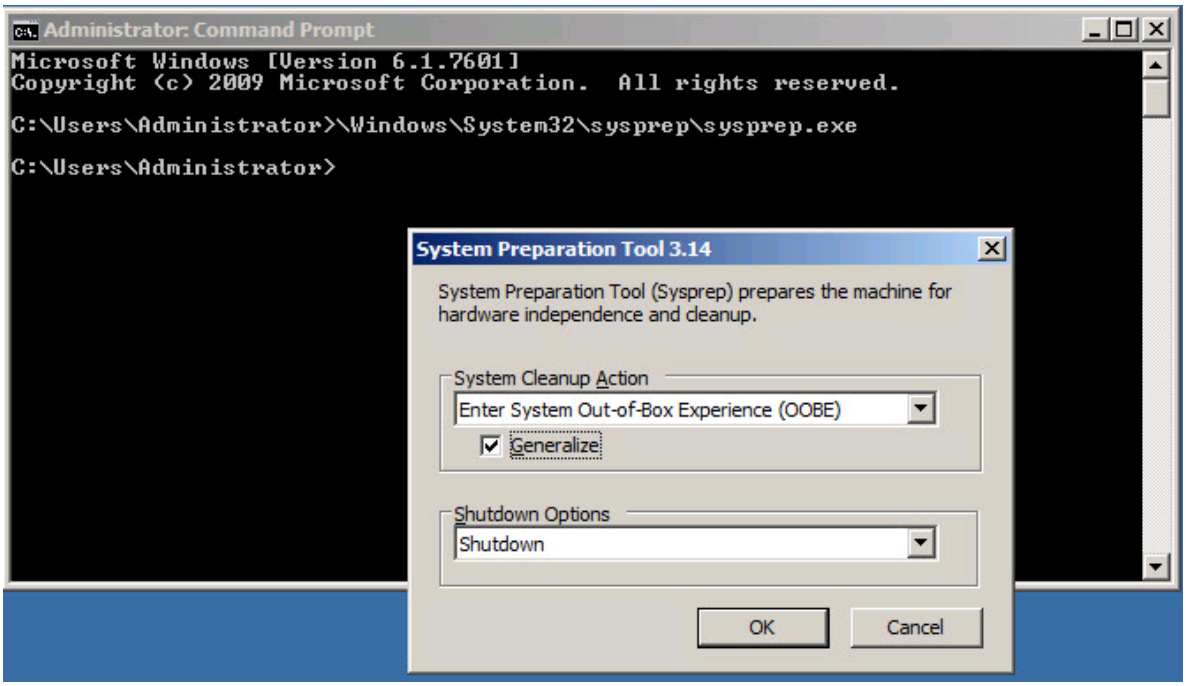

54. Open a CMD window.

55. Enter  \Windows\system32\sysprep\syspre.exe.

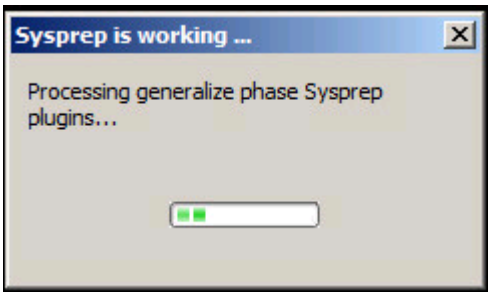
56. Click the checkbox for Generalize.

57. Select Shutdown for the Shutdown Option.

58. Click OK.




59. Sysprep removes all the information specific to the Virtual Machine.




60. Shutdown the system.

## Migrate the Virtual Machine into a Virtual Machine Template

Migrate the virtual machine into a virtual machine template that is used for future virtual machine deployments. To migrate a virtual machine into a template, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click Hosts and Clusters.
4. Click the virtual machine.
5. Click Actions > All vCenter Actions.

6. Click Convert to Template.

# Install and Configure Management Tools

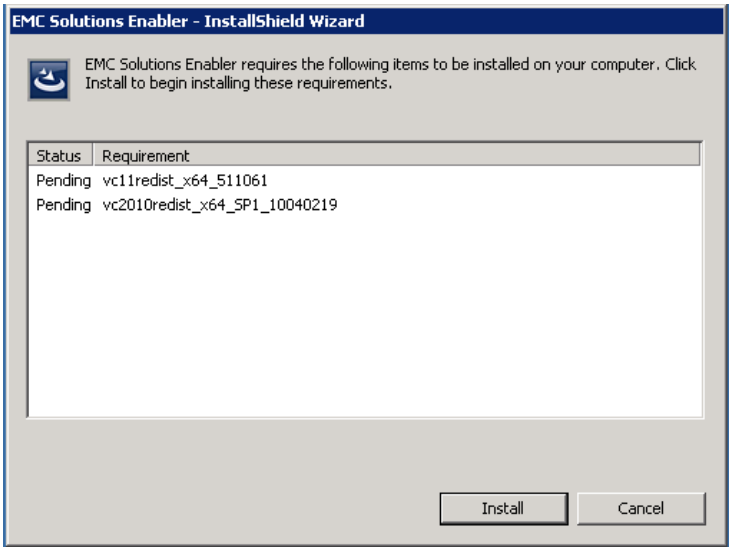
When the infrastructure components are installed, additional management tools can be installed and configured.

The tools described in the following sections are the EMC Solution Enabler SMI Option and the Cisco UCS Performance Manager. Both tools are required to monitor the utilization of the components and identify upcoming bottlenecks.

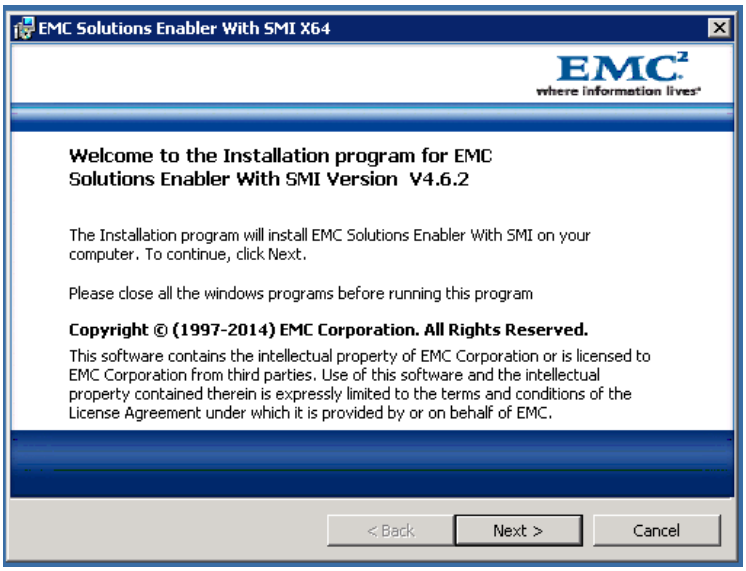
## Install and Configure EMC Solution Enabler SMI Module

The EMC Solution Enabler with SMI software can be loaded from the EMC web site. To install and configure the EMC Solution Enabler SMI Module, complete the following steps:

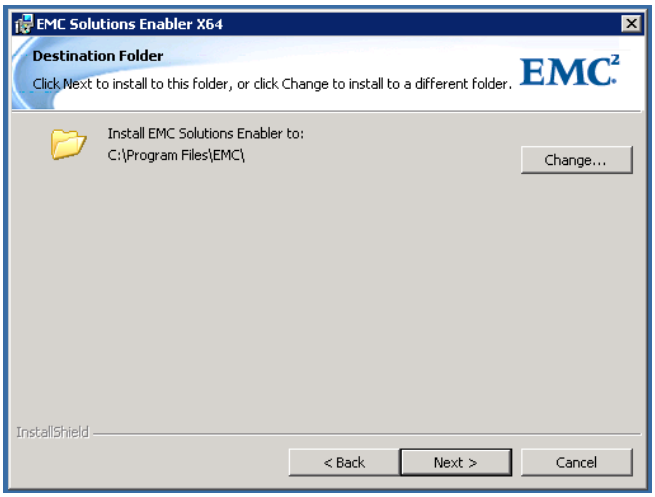
1. Log in to Windows Server in the Management POD.
2. Open a File Browser and navigate to the location of the installation source.
3. Double-click the se76226-WINDOWS-x64-SMI.exe file.
4. The Installation procedure will automatically install the packages required prior to install the EMC Solution Enabler.
5. Click Install.




6. Click Next.

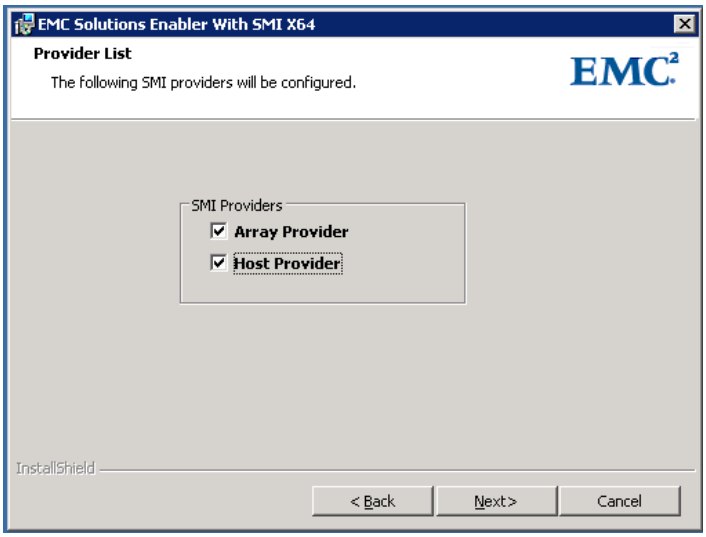



7. Click Next.

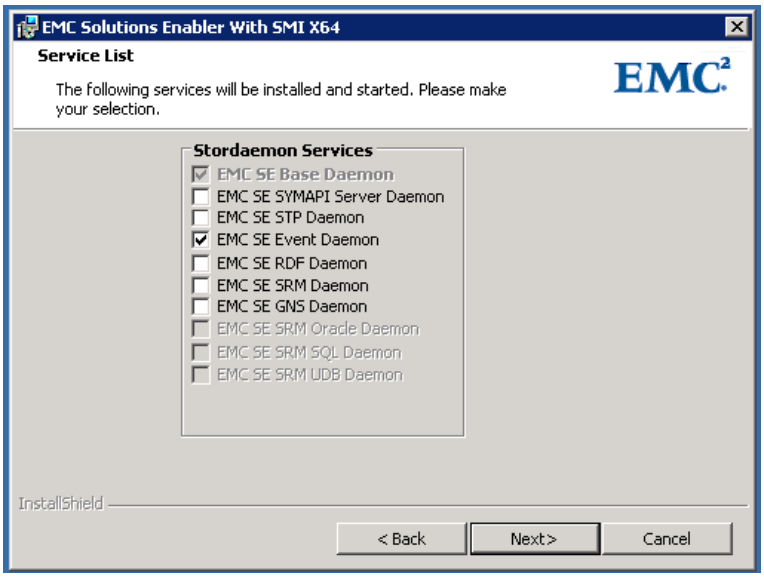



8. Select both SMI Providers.

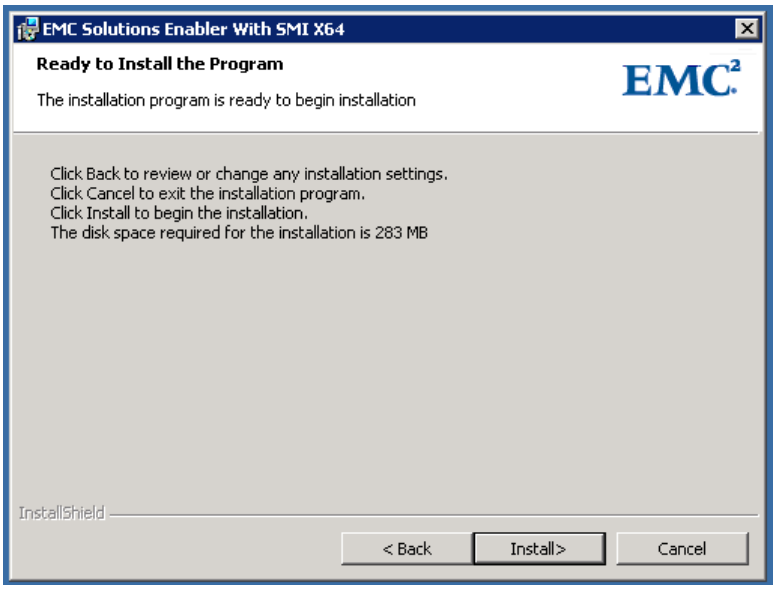
9. Click Next.



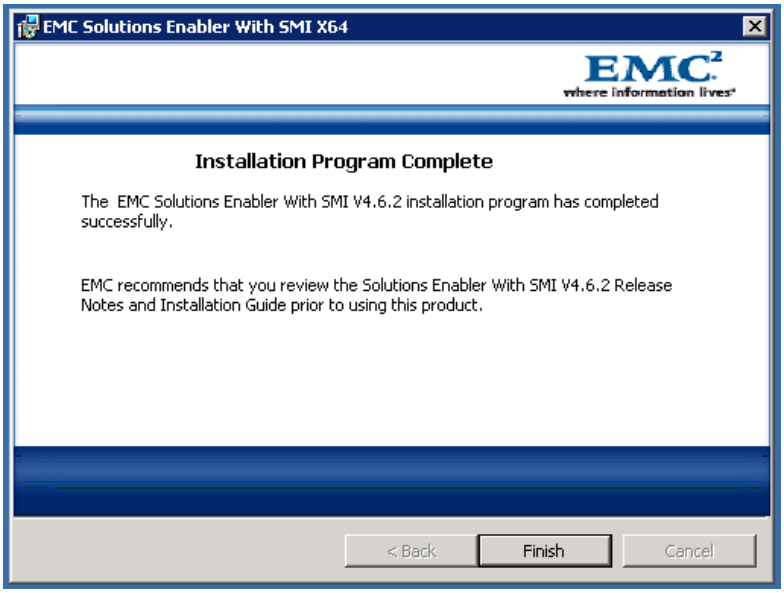

10. Click Next.




11. Click Install.

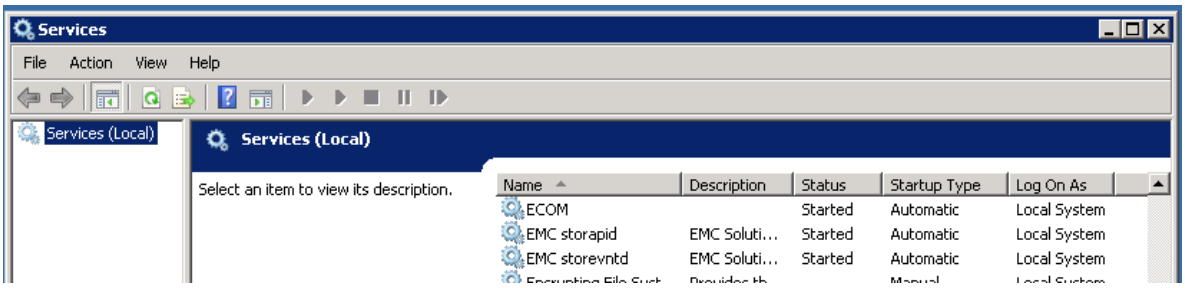



12. Click Finish.




13. Open the windows Services Manager.

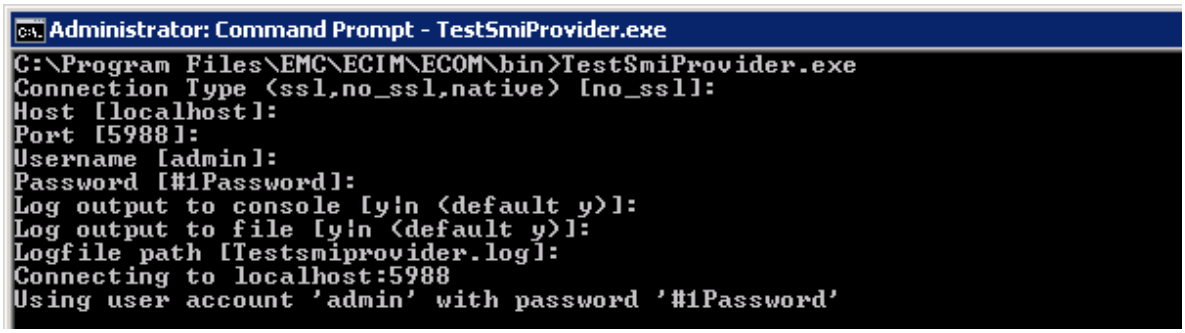
14. Check that the Service ECOM is Started and Startup Type is Automatic.




15. Open a CMD Window.

16. Start C:\Program Files\EMC\ECIM\ECOM\TestSmiProvider.exe.

17. Accept all defaults until the menu is reached.

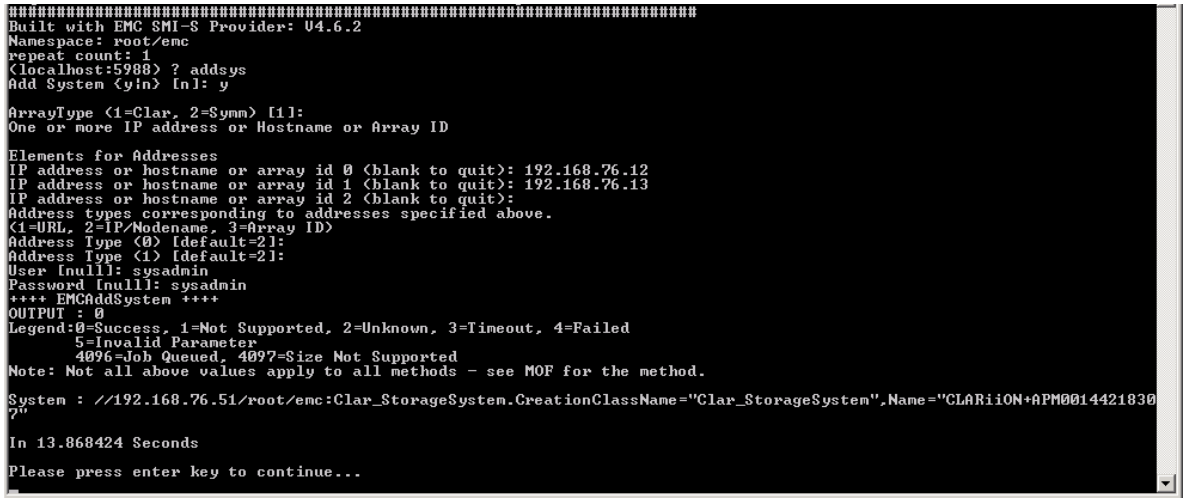





18. Enter addsys.
19. Enter 1 for CLARiiON / VNX.
20. Enter the IP Address of Storage Processor A <<var_vnx1_spa_ip>>.
21. Enter the IP Address of Storage Processor B <<var_vnx1_spb_ip>>.
22. Hit Enter.
23. Use Address Type 2.

24. Enter <<var_vnx_user>> as the User.

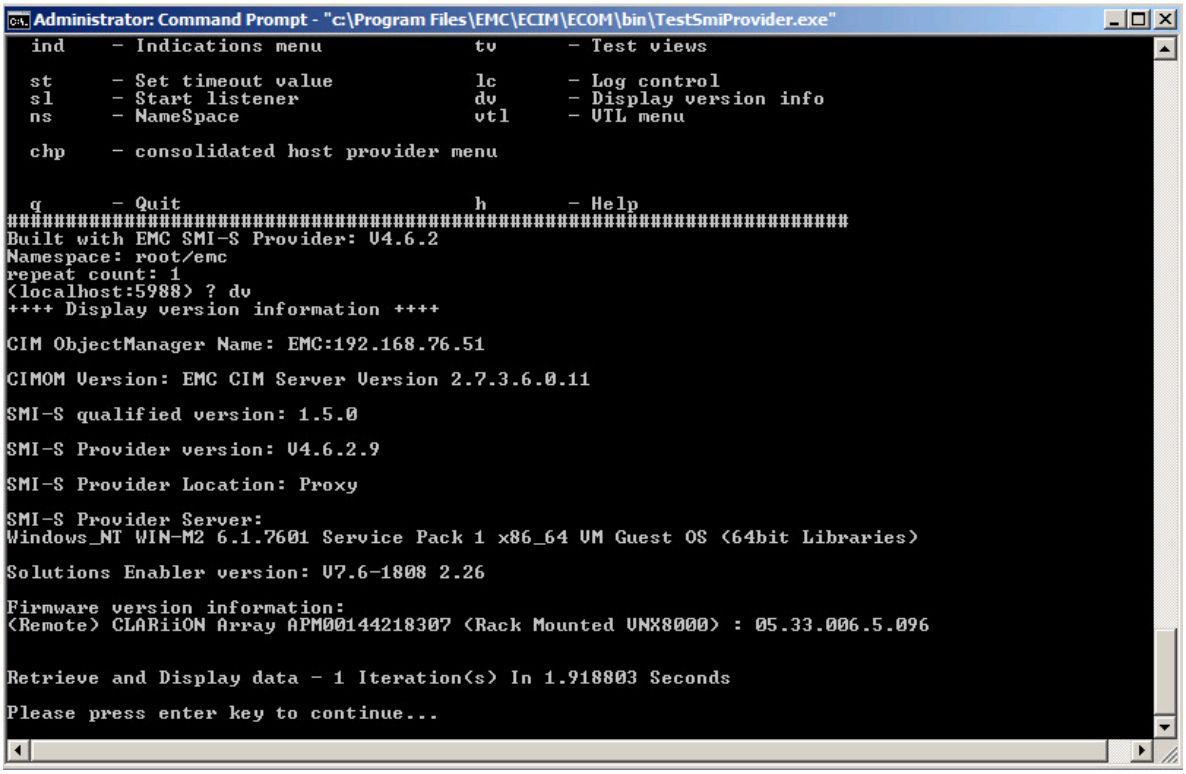
25. Enter <<var_mgmt_passwd>> as the Password.




26. The OUTPUT must be 0.

27. Press Enter.

28. Enter dv and press Enter.

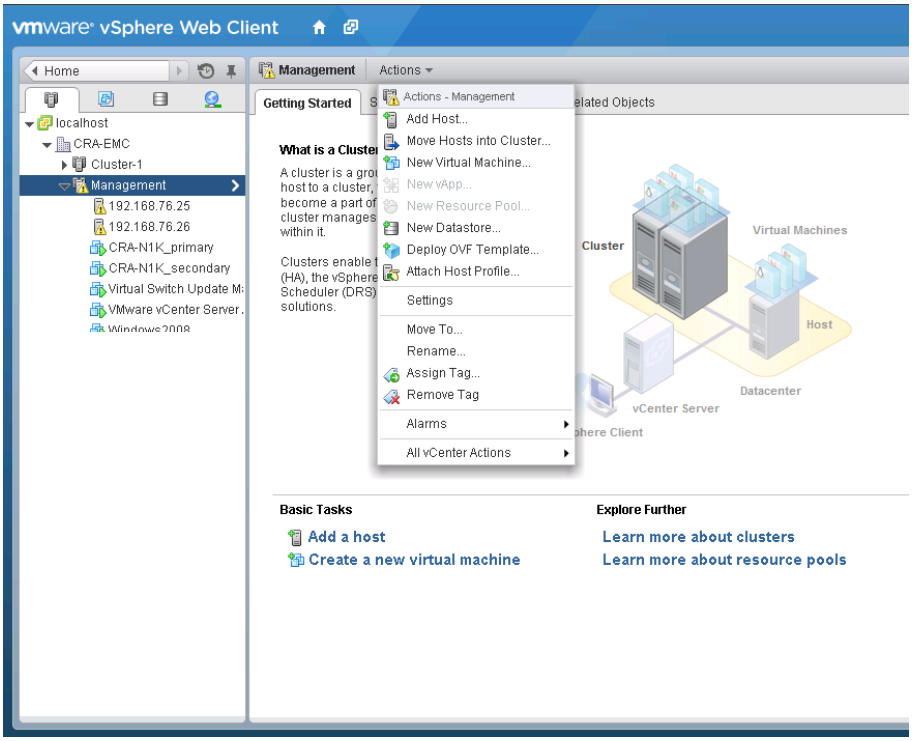


29. Make sure that the EMC VNX you have connected is listed with a Firmware version.
30. Press Enter.
31. Press q.
32. Close the CMD.

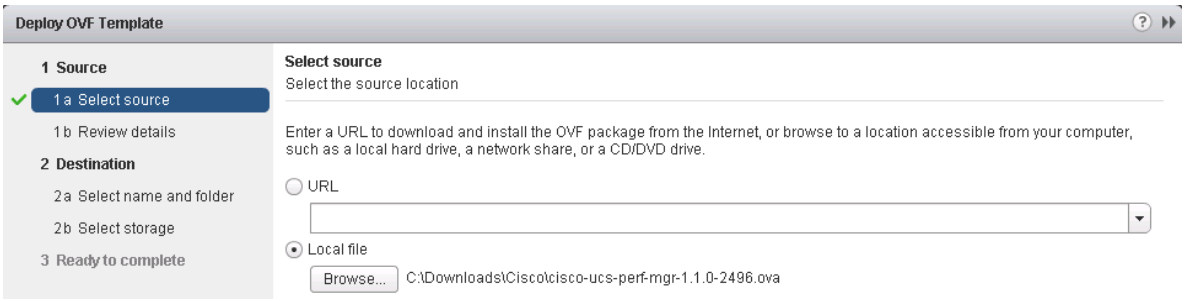
## Install and Configure Cisco UCS Performance Manager

The Cisco UCS Performance Manager appliance OVA file can be loaded from the Cisco web site. To install the Cisco UCS Performance Manager, complete the following steps:

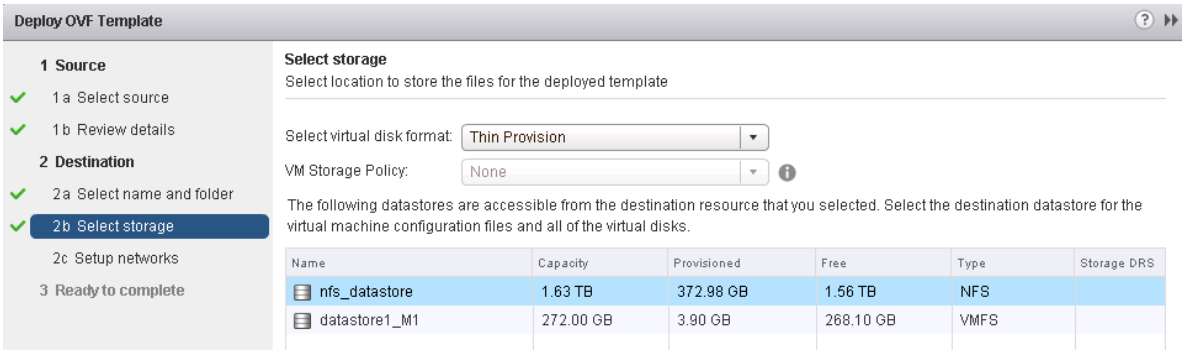
1. Log in to the vSphere Web Client.
2. Click Hosts and Clusters in the Home Screen.
3. Click the <<var_vc_mgmt_cluster_name>>.
4. Click Actions and select Deploy OVF Template.



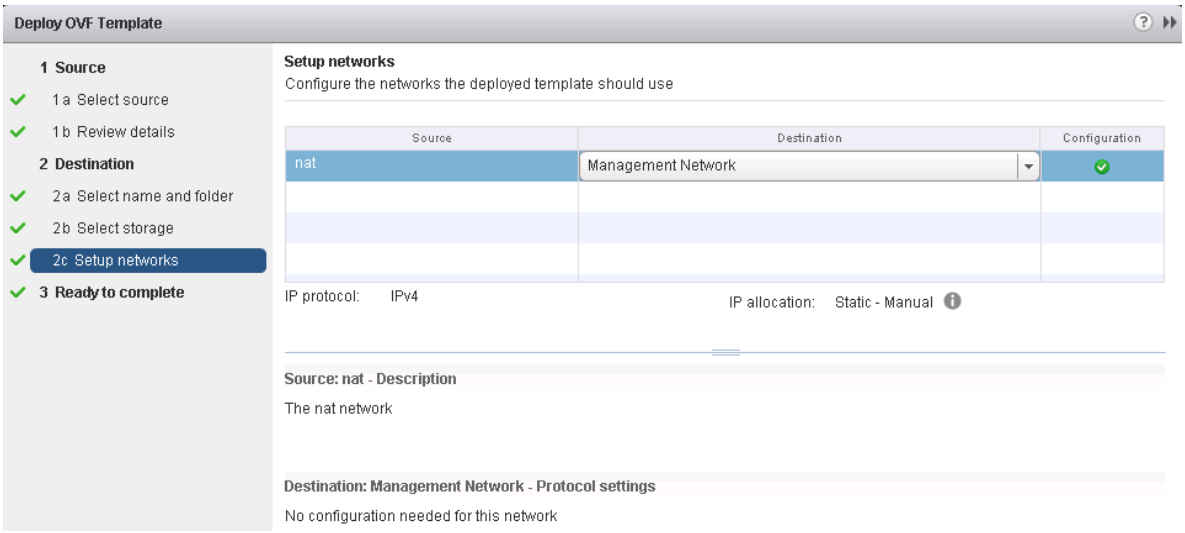

5. Click Browse and select the Cisco UCS Performance Manager OVA file.
6. Select the requires Nexus1000v-vsum file.




7. Review the Details.
8. Click Next.
9. Enter <<var_vc_ucspm_vm_name>> as the name.
10. Select <<var_vc_datacenter_name>> as destination.
11. Click Next.
12. Select <<var_vc_mgmt_datastore_1>> as the Storage.
13. Click Next.

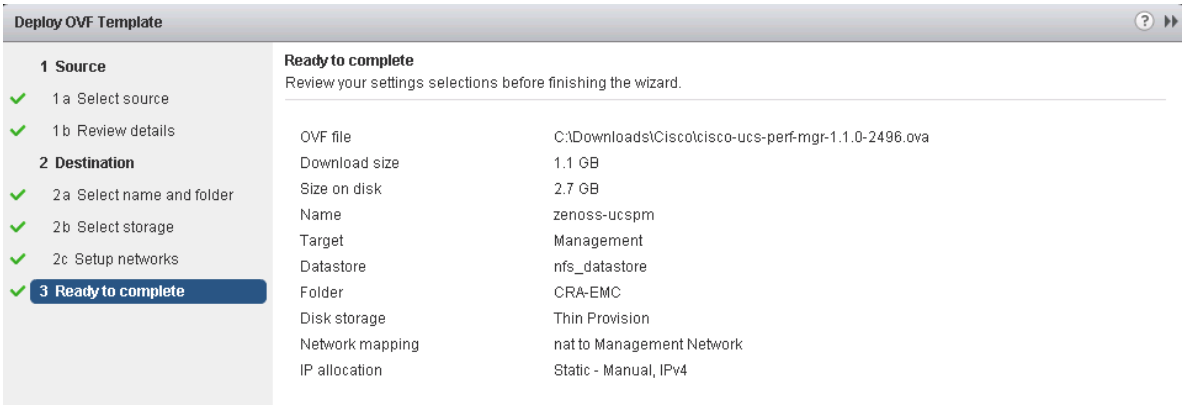



14. Select <<var_esx_mgmt_network>> as the Destination for the Source.
15. Click Next.




16. Review the information.

17. Click Finish.

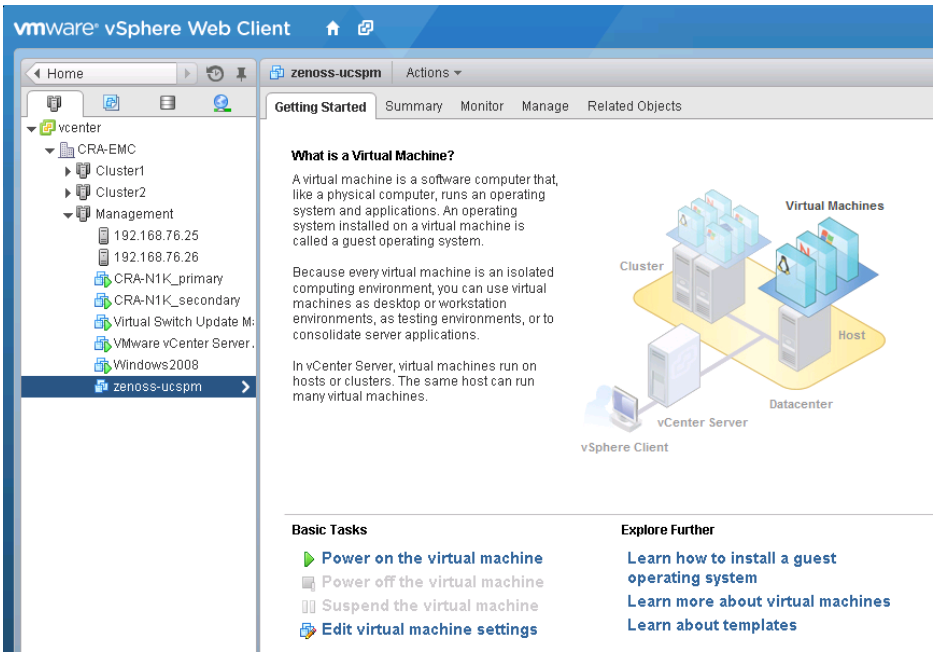



18. Select Hosts and Clusters in the Home screen.

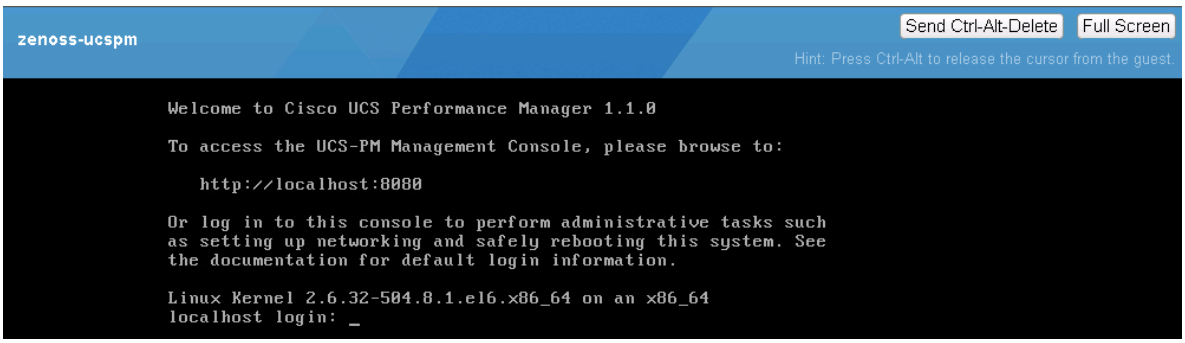
19. Open Management Cluster.

20. Select <<var_vc_ucspm_vm_name>> Virtual Machine.

21. Power On the VM.




22. Open the VM Console from the Actions menu.

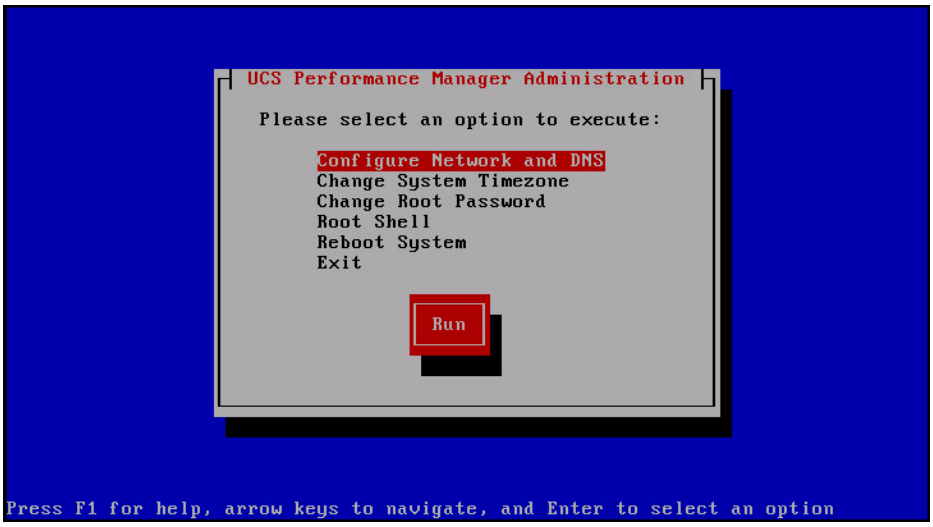



23. Logon as root with the password specified in the Cisco UCS Performance Manager Installation Guide.

24. The system will automatically ask for a new password. Please use <<var_mgmt_passwd>> as the new password for the user root.

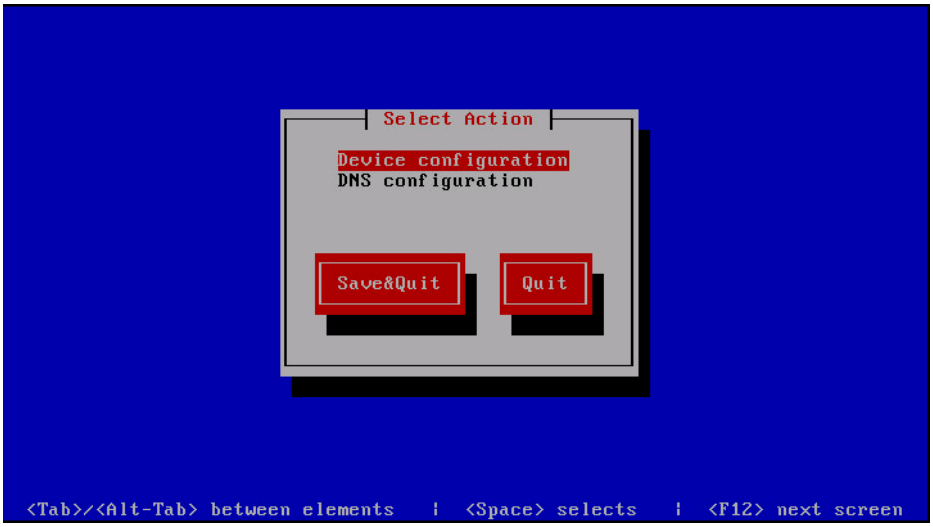
25. Select Configure Network and DNS.

26. Hit Enter.



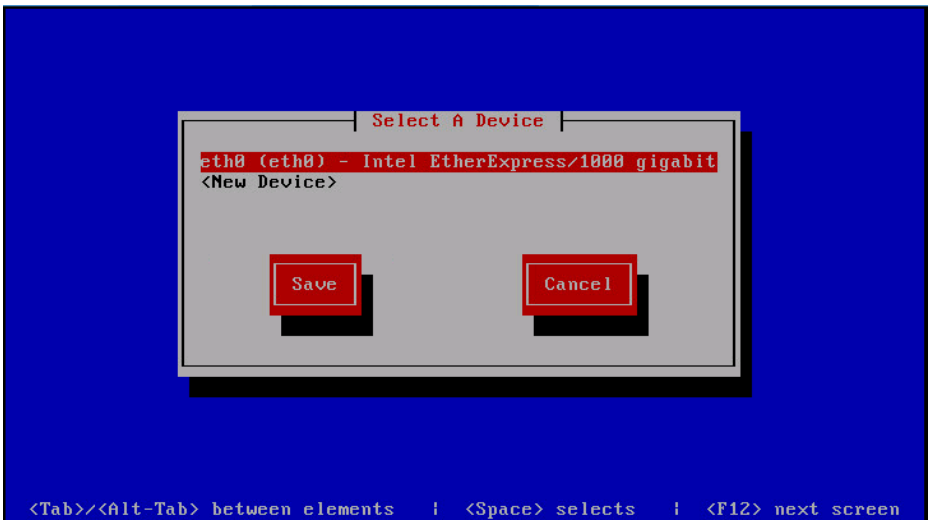

27. Select Device Configuration.

28. Hit Enter.

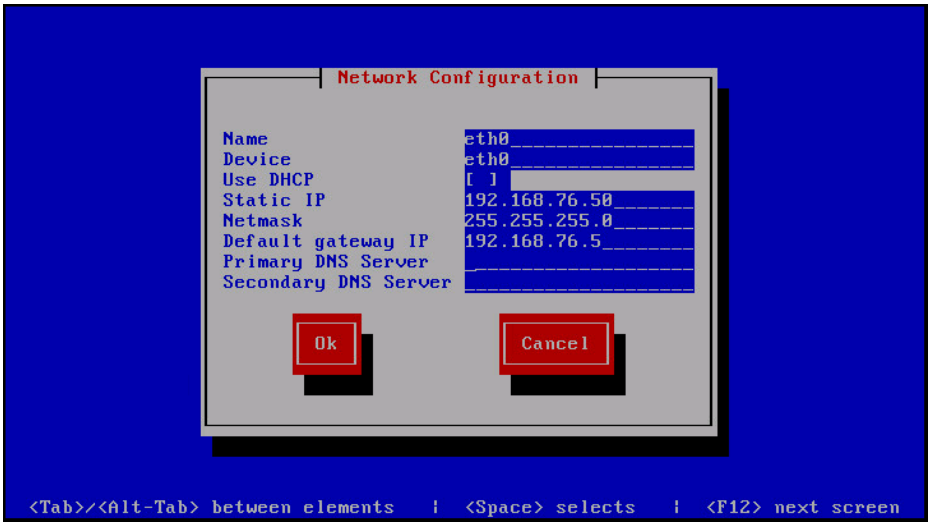



29. Select eth0.

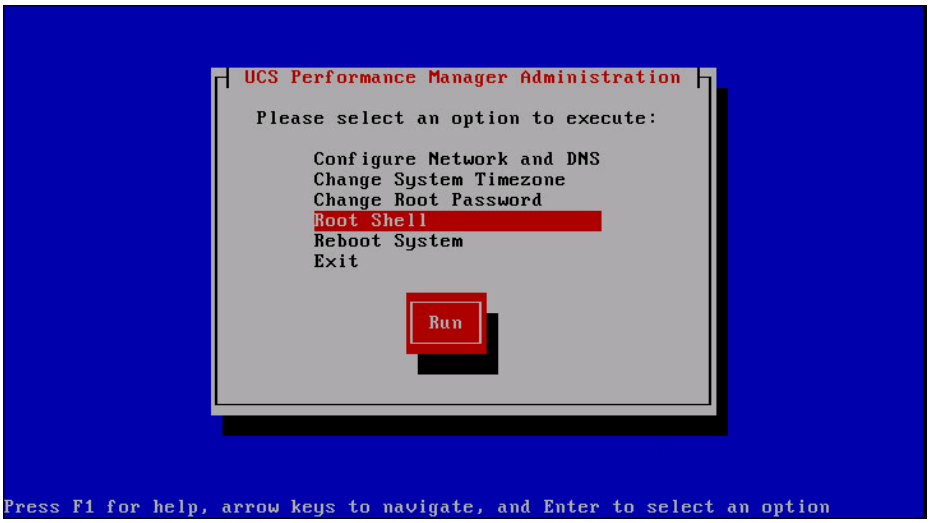
30. Hit Enter.




31. Unselect Use DHCP.
32. Enter <<var_ucspm_ip>> as the Static IP.
33. Enter <<var_mgmt_mask>> as the Netmask.
34. Enter <<var_mgmt_gw>> as the Default GW IP.
35. Enter the primary and secondary DNS Server as required.
36. Select OK, hit Enter.




37. Select Save, hit Enter.
38. Select Save&Quit, hit Enter.
39. Select Root Shell, hit Enter.




40. Restart the network services:

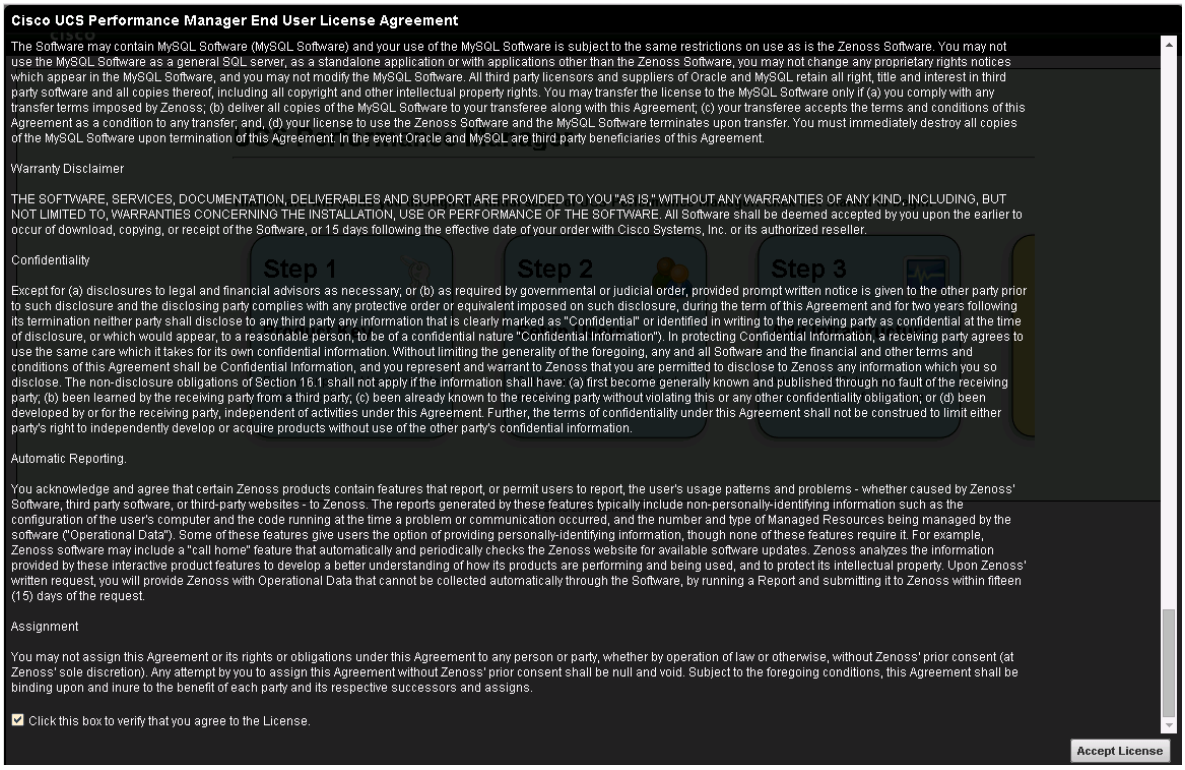
```
# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Determining if ip address 192.168.76.50 is already
in use for device eth0...
                                                           [  OK  ]
# exit
```

41. Select Exit, hit Enter.

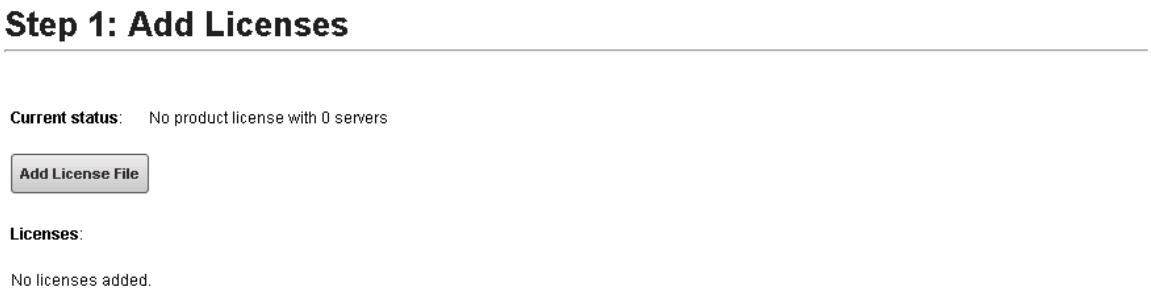
42. Open http://<<var_ucspm_ip>>:8080/ in a web browser.

43. Scroll down on the EULA page, click the checkbox in the lower left corner.

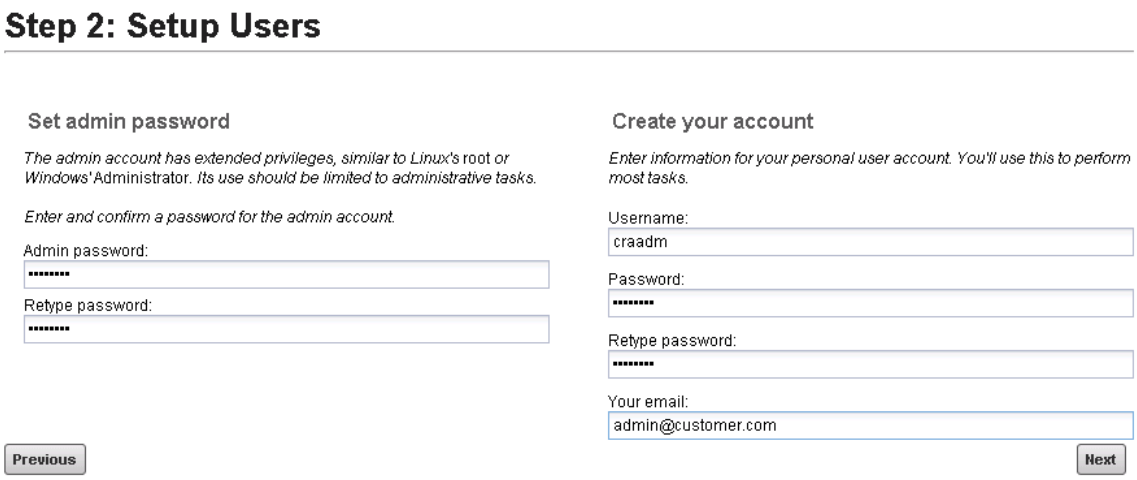
44. Click Accept License.




45. Click Add License File and select the License file you have received from Cisco.
46. Click Next.




47. Enter <<var_mgmt_passwd>> as the Admin password.
48. Enter valid information to create your account as shown below.
49. Click Next.



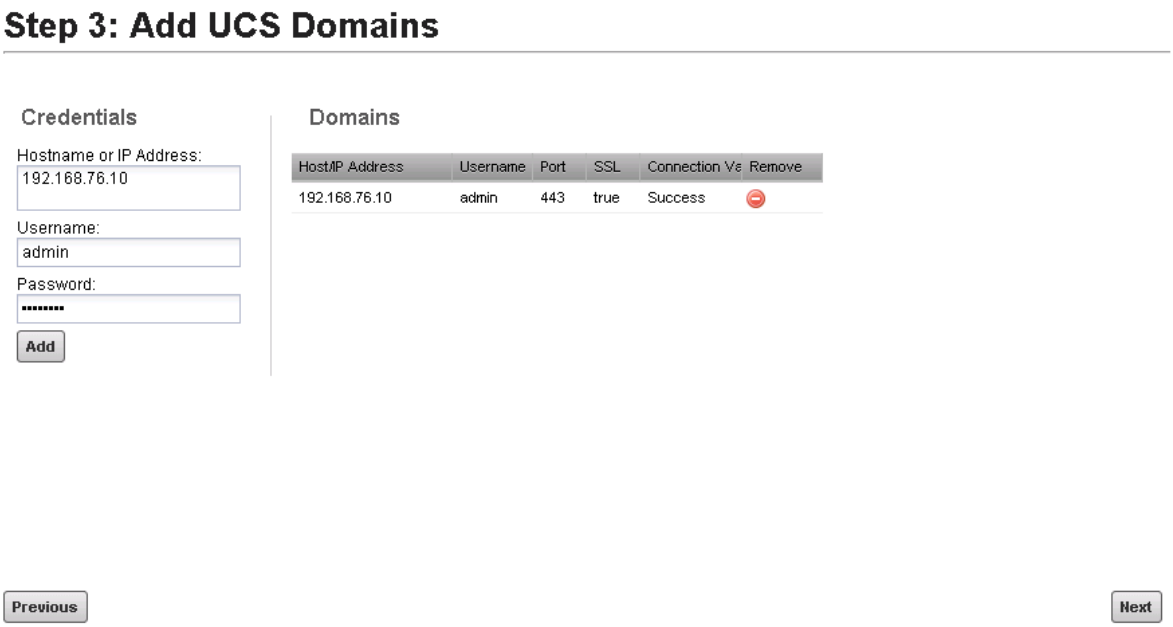

50. Enter <<var_ucsm1_ip>> as the IP address.

51. Enter admin as User.

52. Enter <<var_mgmt_passwd>> as the Password.

53. Click Add.

54. Click Next.

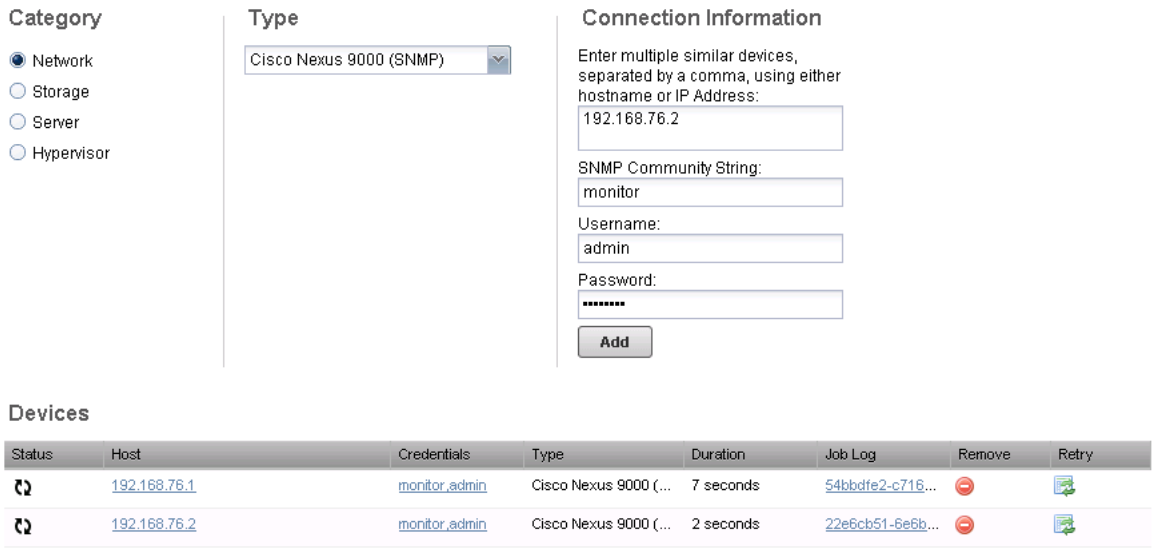



55. To add the Cisco Nexus 9000 switches, click Network.

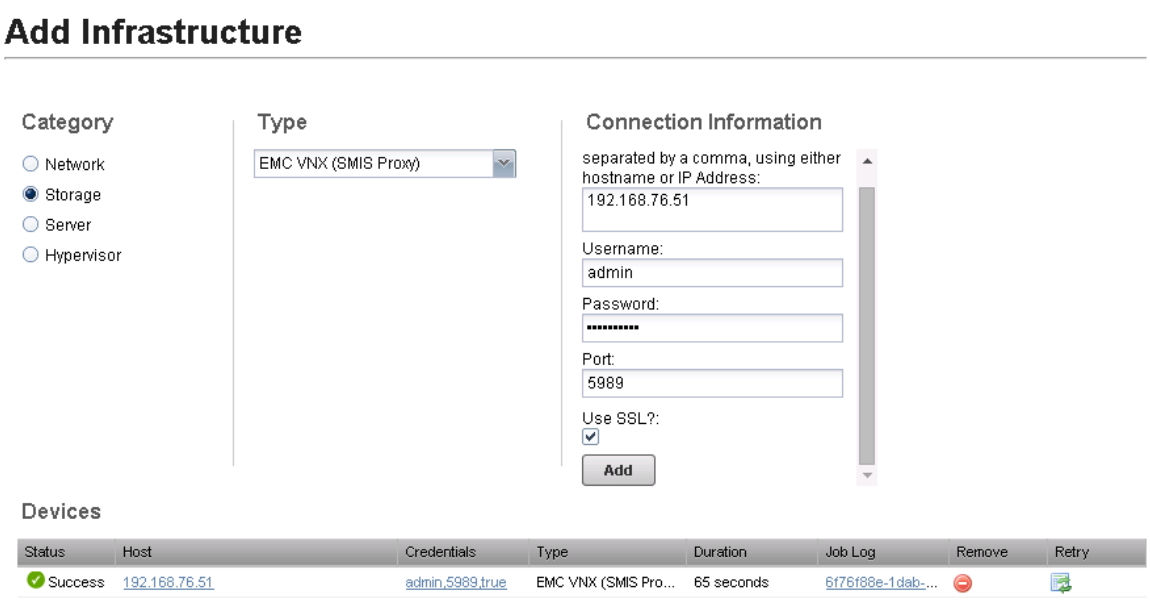
56. Select Cisco Nexus 9000 (SNMP) from the drop-down menu.

57. Enter <<var_nexus_a_ip>> and <<var_nexus_b_ip>> as the IP Address.
58. Enter <<var_snmp_ro_string>> as the SNMP Community String.
59. Enter admin as the Username.
60. Enter <<var_mgmt_passwd>> as the Password.
61. Click Add.

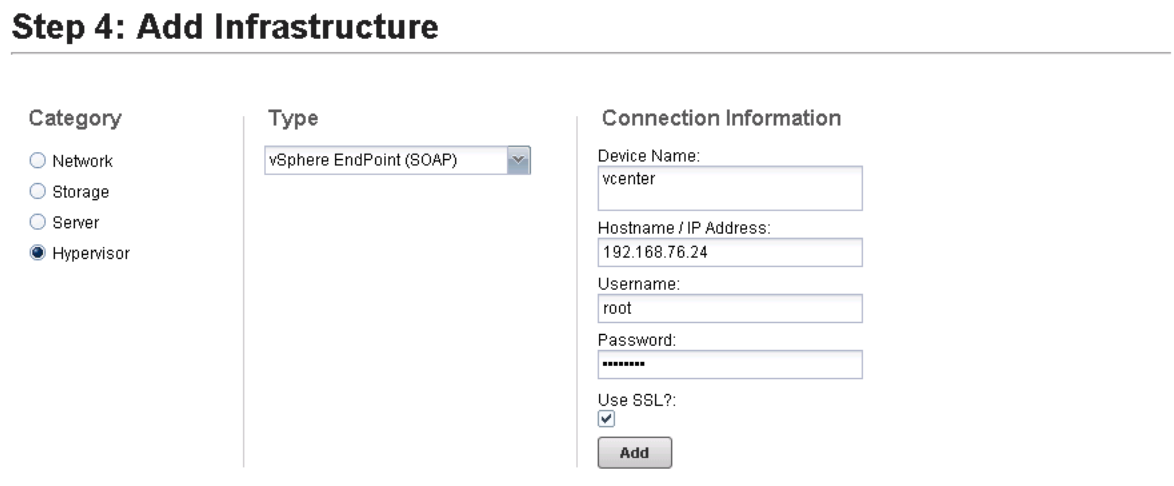
## Step 4: Add Infrastructure



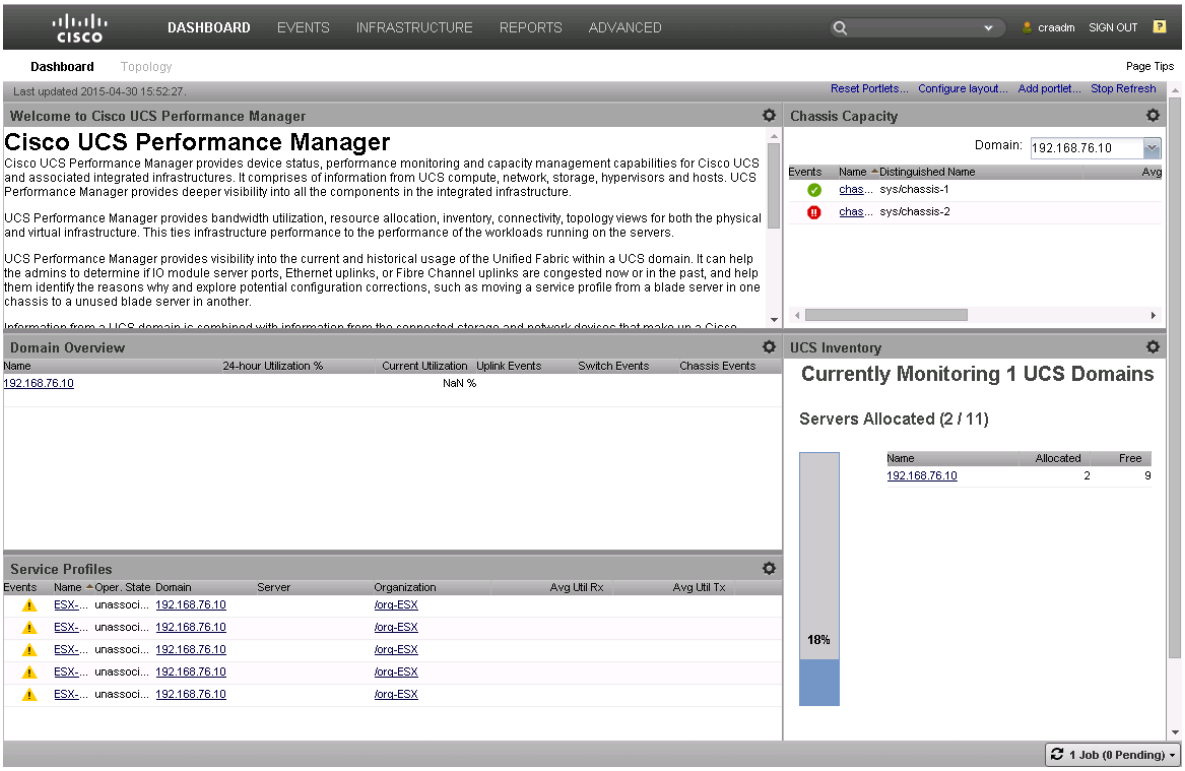

62. To add the VNX Storage, Click Storage.
63. Select EMC VNX (SMIS Proxy) from the drop-down menu.
64. Enter <<var_emc-smis_ip>> as the IP Address.
65. Enter admin as the Username.
66. Enter <<var_mgmt_passwd>> as the Password.
67. Enter 5989 as the Port.
68. Select Use SSL? checkbox.
69. Click Add.



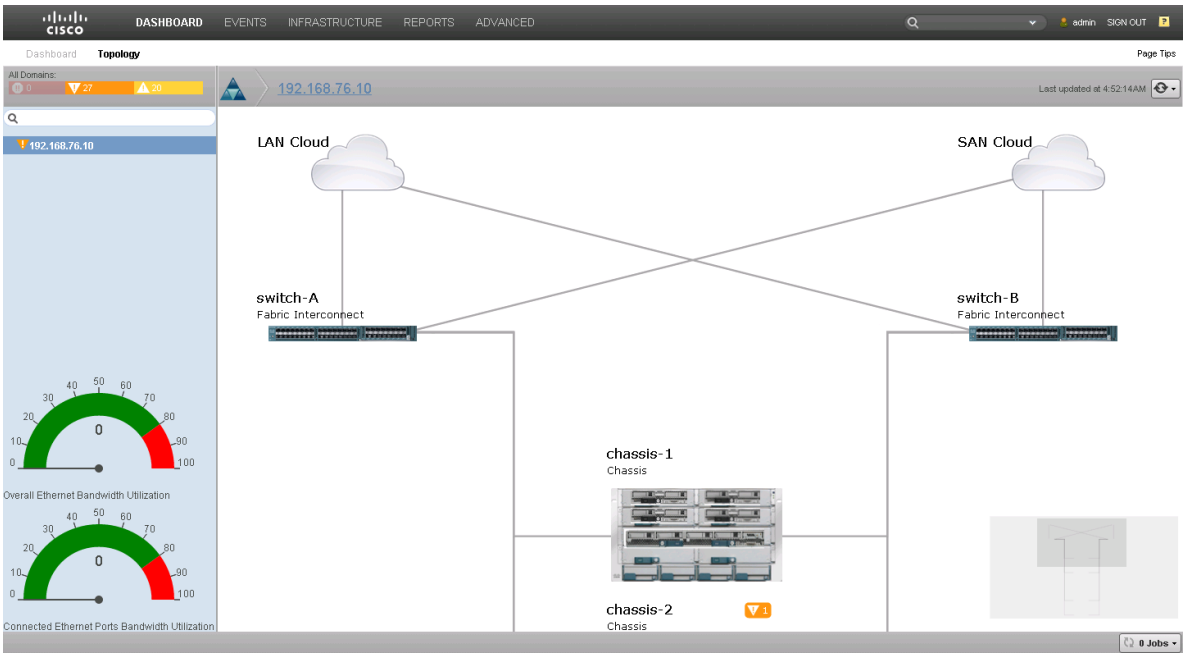

70. To add the vCenter, click Hypervisor.
71. Select vSphere EndPoint (SOAP) from the drop-down menu.
72. Enter vCenter as the Device Name.
73. Enter <<var_vcenter_ip>> as the IP Address.
74. Enter root as the User name.
75. Enter <<var_mgmt_passwd>> as the Password.
76. Click the Use SSL? checkbox.
77. Click Add.




78. Click Finish.



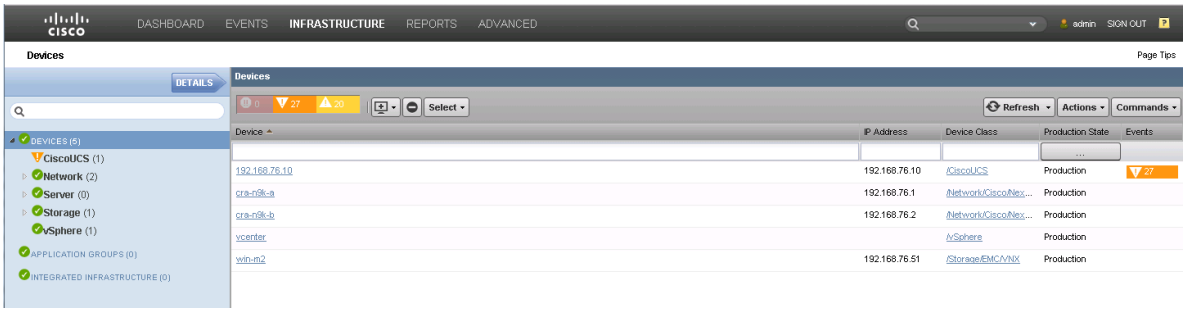

79. Click Topology to view the details.




80. To add additional components, like the Cisco MDS switches, click Infrastructure.

81. Click the  Icon.

82. Select Add Infrastructure.



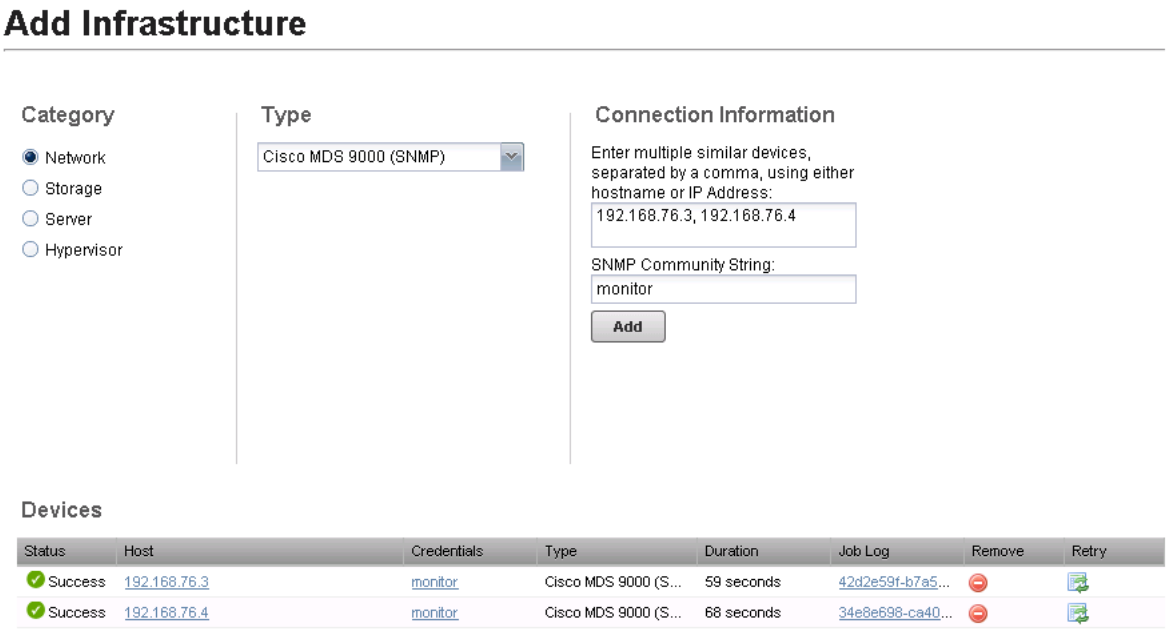

83. To add the Cisco MDS switches, click Network.

84. Select Cisco MDS 9000 (SNMP) from the drop-down menu.

85. Enter <<var_mds-a_ip>> and <<var_mds-b_ip>> as the IP Address.

86. Enter <<var_snmp_ro_string>> as the SNMP Community String.

87. Click Add.

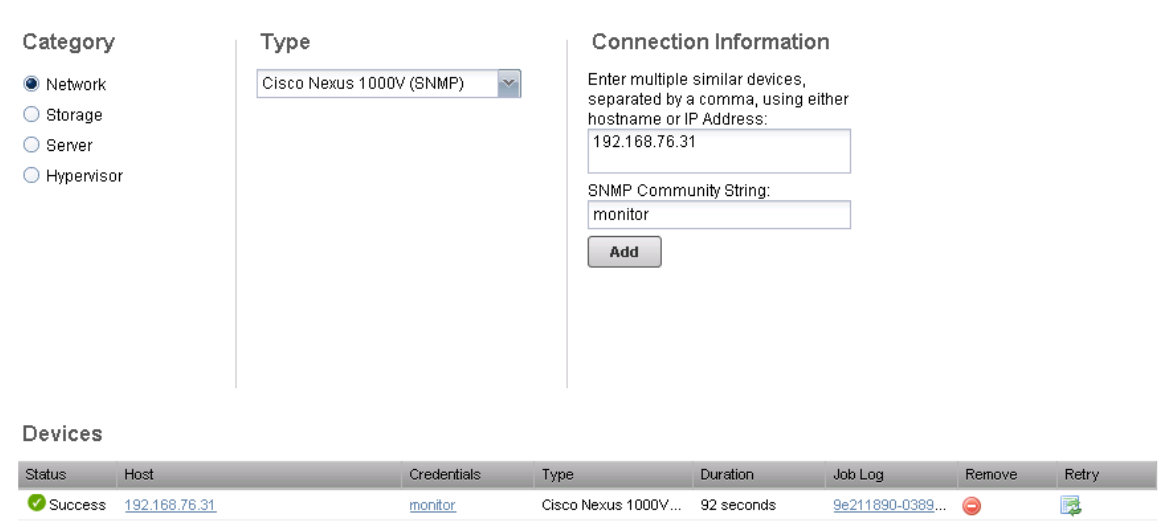



88. To add the Nexus 1000V, select Cisco Nexus 1000V (SNMP).

89. Enter <<var_n1K_vsm_ip>> as the IP Address.

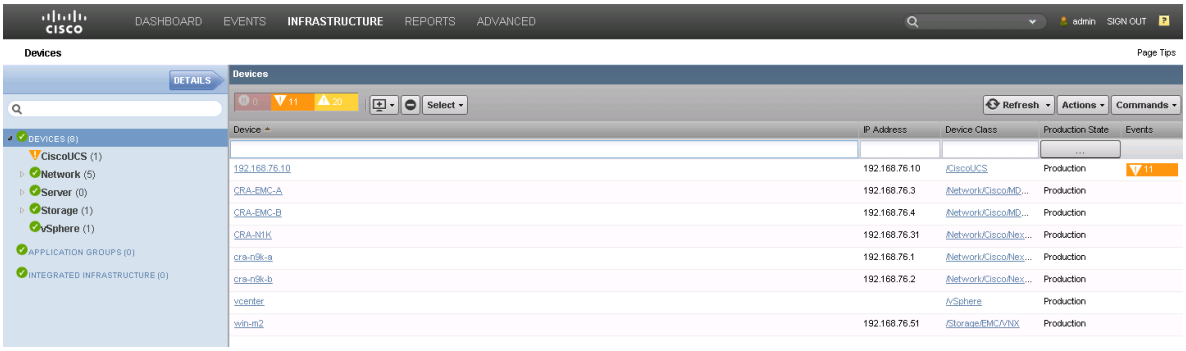
90. Enter <<var_snmp_ro_string>> as the SNMP Community String.

91. Click Add.




92. Click Done.

The two MDS switches and the Cisco Nexus 1000V are listed in the Infrastructure View.




93. Use the Cisco UCS Performance Manager Documentation to add all components you want to have in this tool.

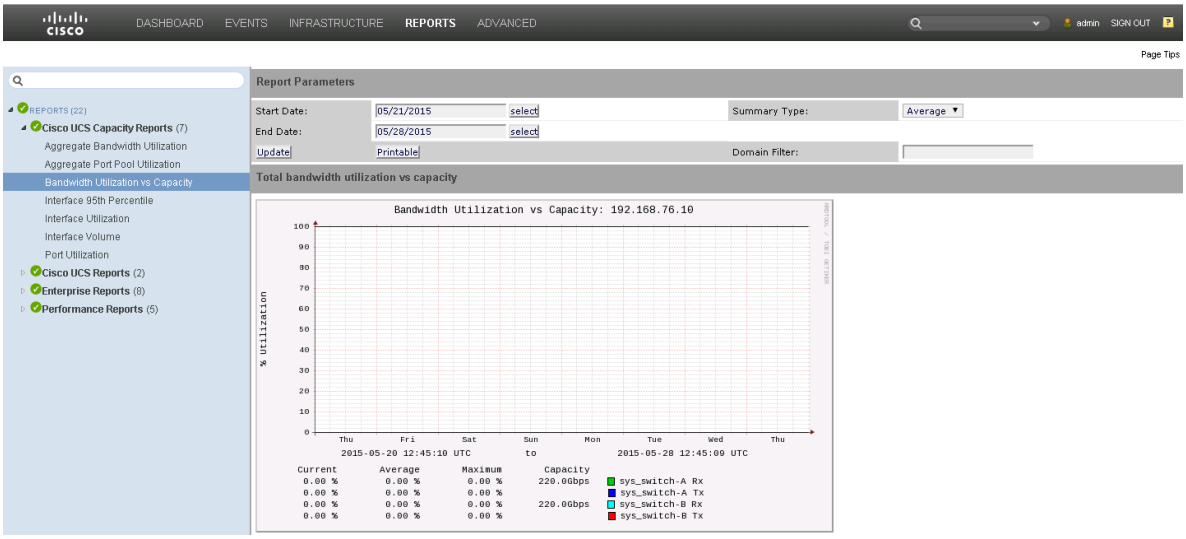
The main reason to have the Cisco UCS Performance Manager installed in this data center architecture is the capability to monitor the port utilization within the Cisco UCS Domain, and between Cisco UCS and the upstream Ethernet and Fibre Channel infrastructure.

Keep in mind that the different SAP HANA use cases require different Ethernet and Fibre Channel capacity, for example, a Virtualized Scale-Up system only required access network and storage access, where a Scale-Out system with enabled SAP HANA System Replication requires in addition to that the internal network and the system replication network.

94. Click Reports.

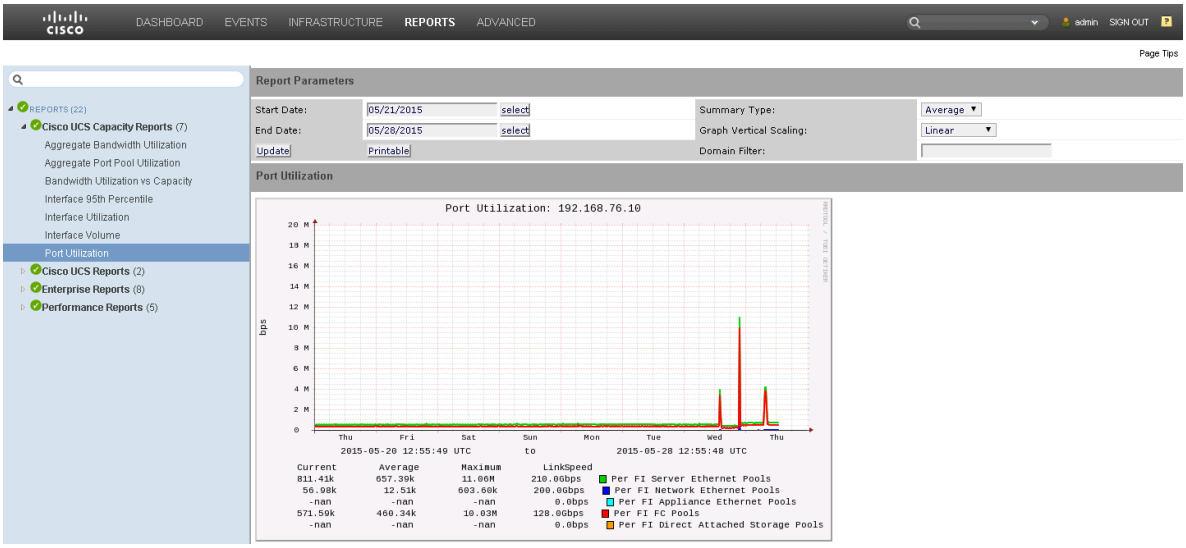
95. Select Cisco UCS Capacity Reports > Bandwidth Utilization vs Capacity.

In this report, the Overall capacity of Fabric A and Fabric B is shown together with the Average and Maximum Utilization. This provides you with an indication about the overall capacity and the load distribution across Fabric A and Fabric B.



96. Select UCS Capacity Reports > Port Utilization.

In this report, the capacity of the Server ports, Ethernet ports and Fibre Channel ports is shown together with the Average and Maximum Utilization. This provides you with an indication about the utilization and the requirements to add more ports of a specific type.



# Reference Workloads and Use Cases

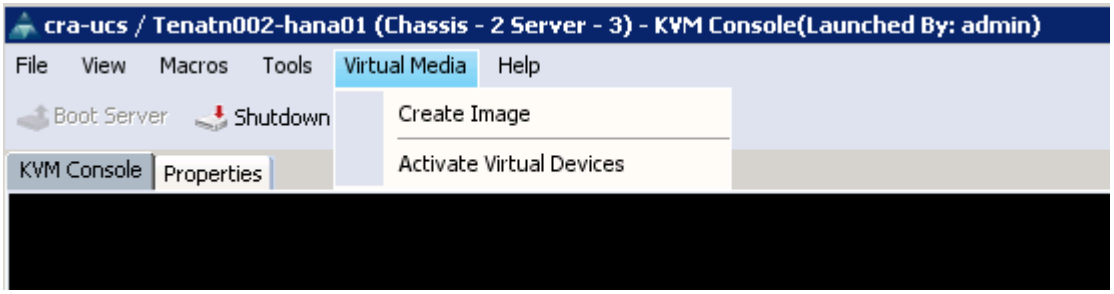
The foundation to deploy one or more workloads and use cases is defined when the Cisco UCS Integrated Infrastructure is up and running. In this CVD, multiple use cases are defined to illustrate the principles and the required steps to configure the Cisco UCS Integrated Infrastructure properly for SAP HANA and other SAP Applications.

## Operating System Installation and Configuration

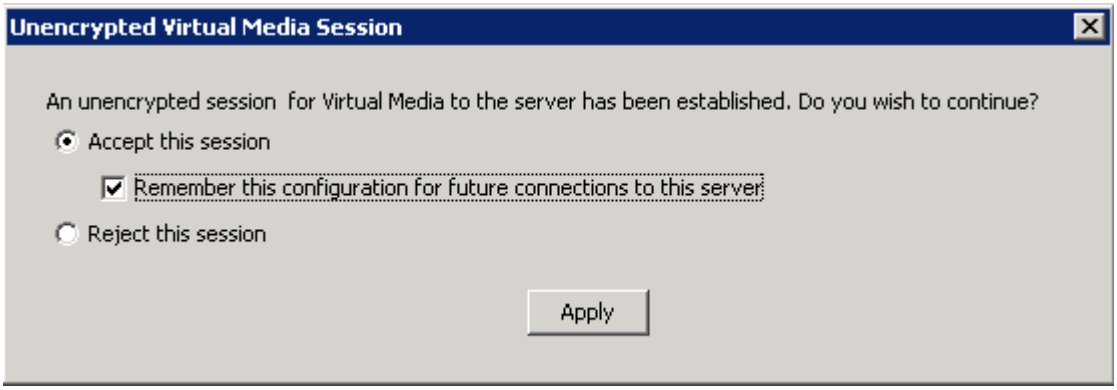
In this section the basic Linux installation and configuration is shown. The tenant or use case specific configuration is documented in the specific use case section.

### RedHat Enterprise Linux 6

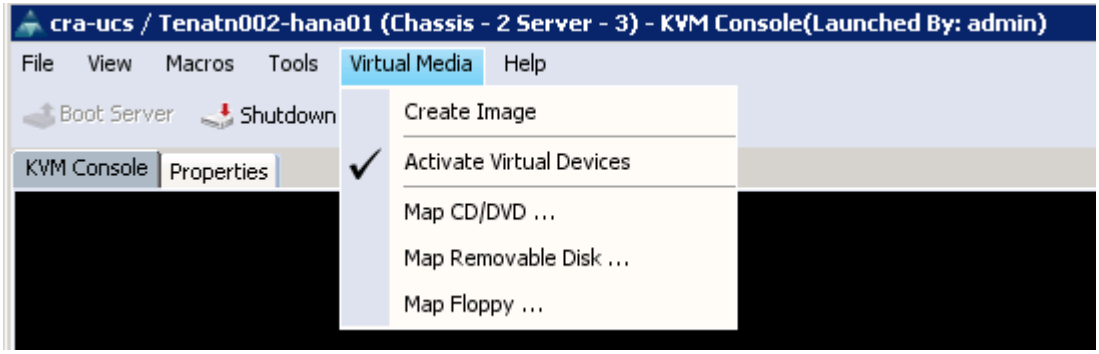
1. Go to the Cisco UCS Manager and select the Service Profile
2. Click KVM Console
3. Click the Menu Virtual Media
4. Select Activate Virtual Devices



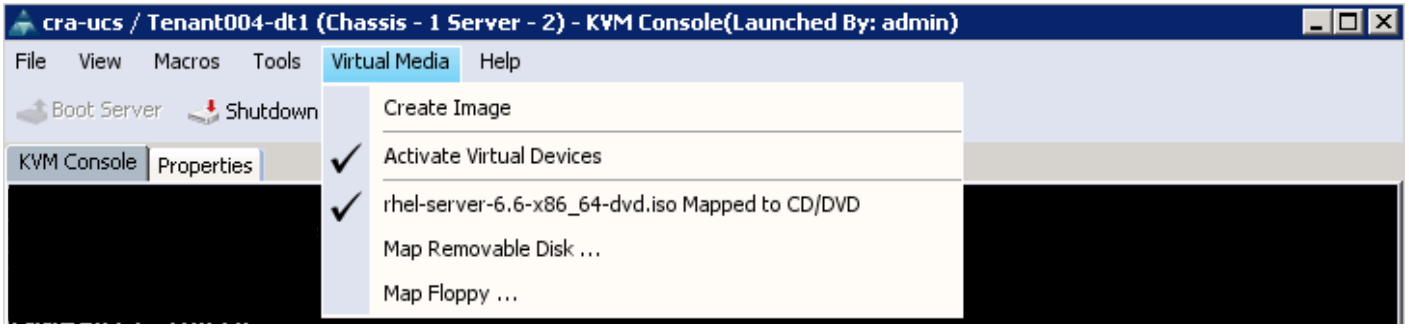

5. In the new Window, Select Accept this Session. If you like you can also select the Check-Box to Remember this setting
6. Click Apply



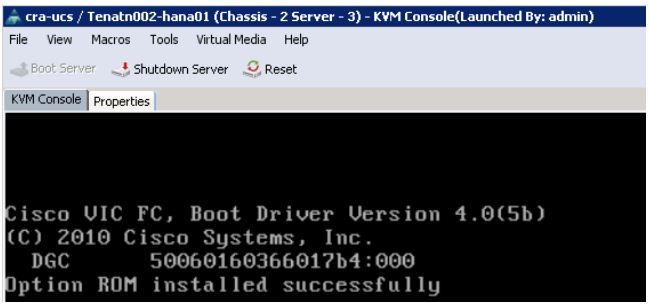

7. Click again on the Menu Virtual Media
8. Select Map CD/DVD...




9. Click Browse, and select the RedHat Enterprise Linux ISO
10. Click Map Device




11. Click Reset to reset the server. This will force the system to scan the SAN and get access to the LUNs on the EMC VNX.



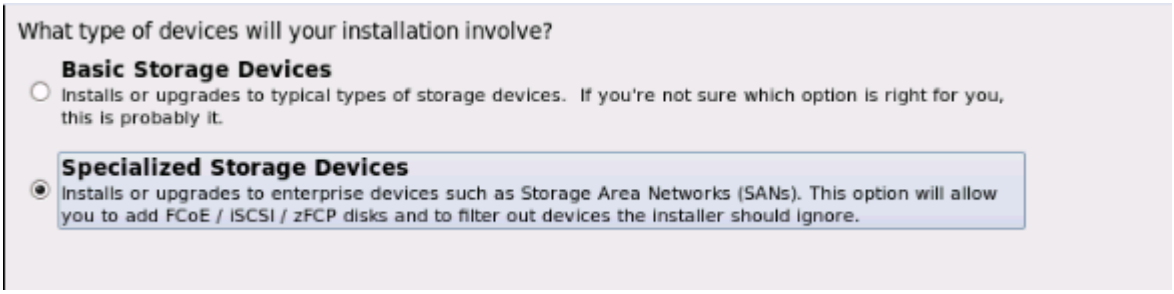

12. The System will automatically boot from the ISO image.




Follow the instructions on the screens and select the settings until the Installation Summary screen appears.

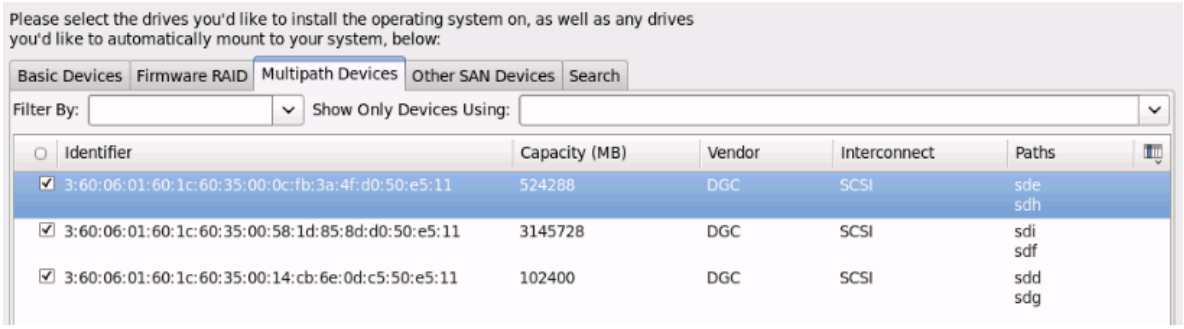
13. Select Specialized Storage Devices.

14. Click Next.




15. Select all devices.

16. Click Next.




17. Click Yes and discard any data.

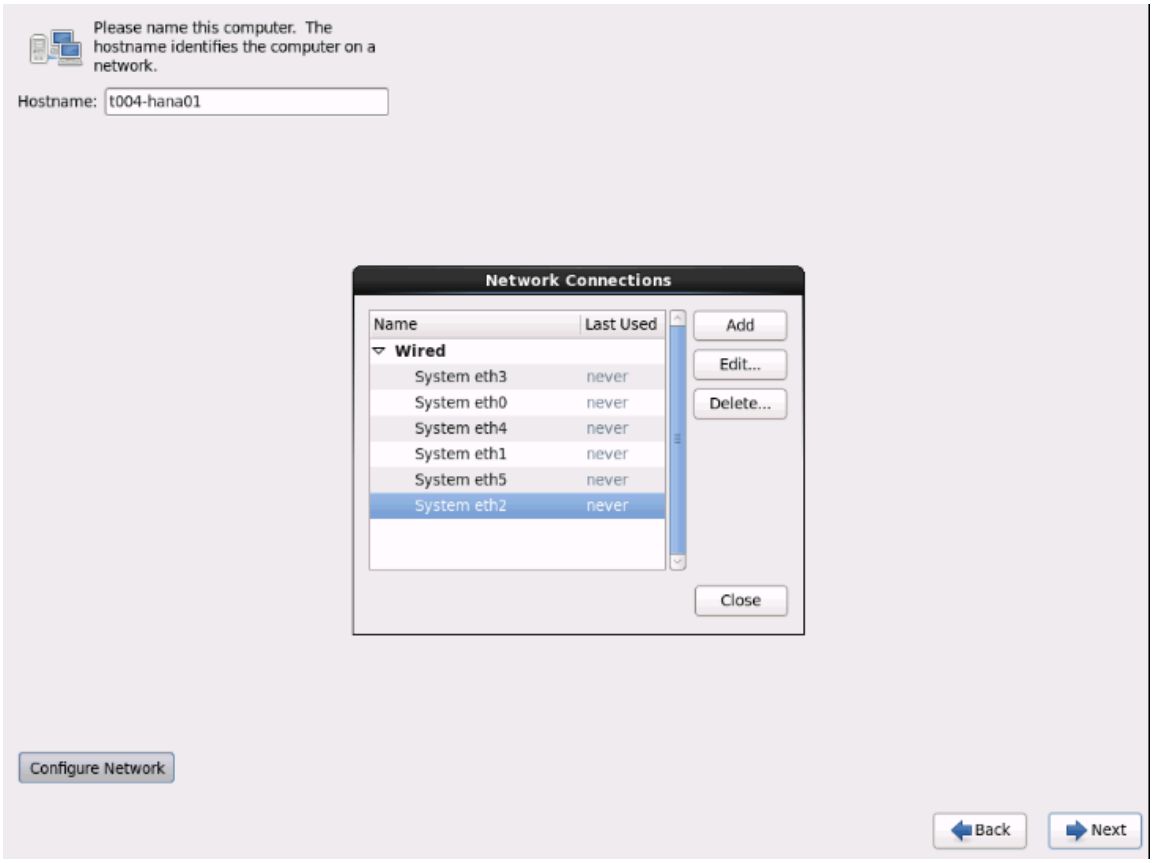



18. Enter <<hana1_hostname>>.

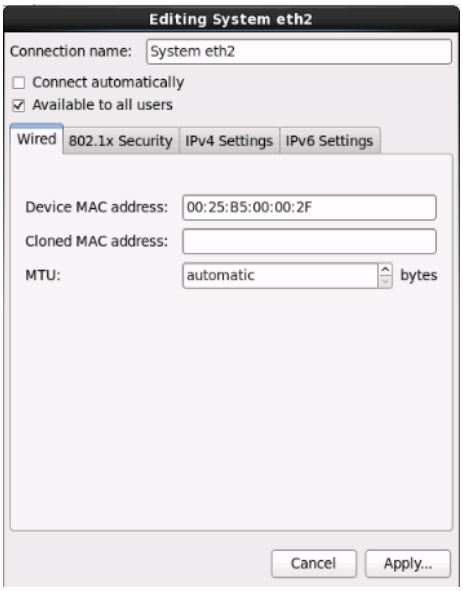
19. Click Configure Network.

20. Select System eth0 (on Cisco UCS C-Series it can also be eth2, please check the MAC address).

21. Click Edit.

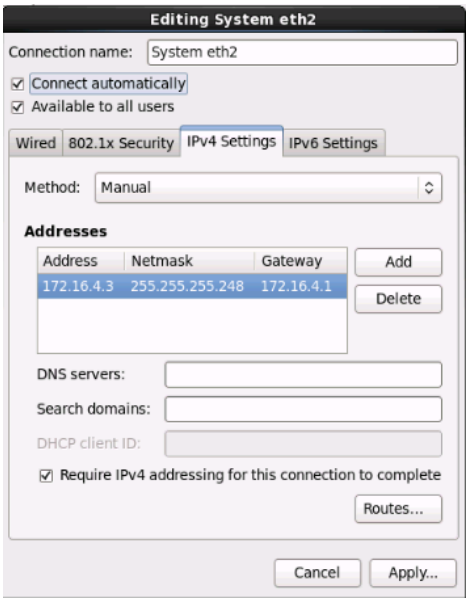



22. Check that the MAC Address is the same as vNIC0 in UCS Manager (Access Network)

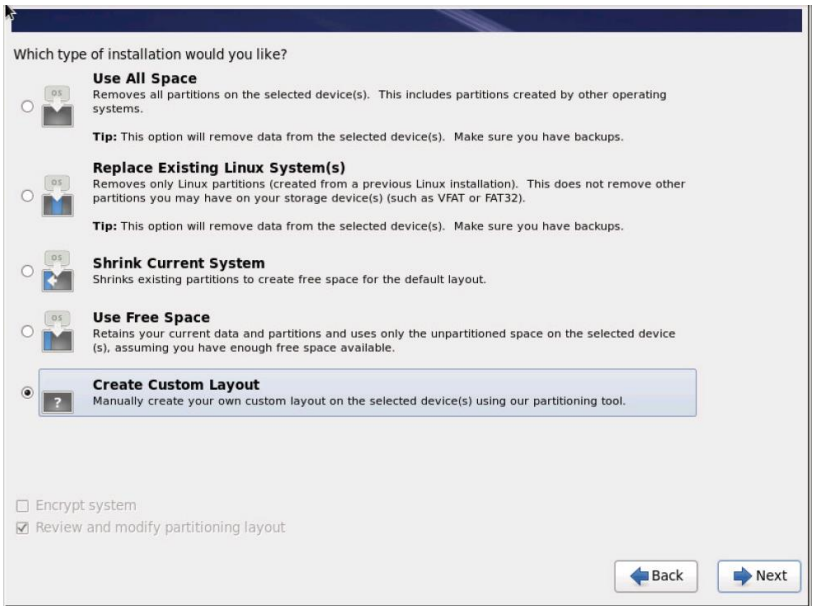



23. Click IPv4 Settings tab

24. Select Manual
25. Click Add
26. Enter <<access_ip>> as the Address
27. Enter <<access_mask>> as the Netmask
28. Enter <<access_gw>> as the Gateway
29. Select Connect automatically
30. Click Apply




31. Click Close
32. Click Next
33. Select the right Time Zone and click Next
34. Use <<var_mgmt_passwd>> as the root password, and click Next
35. Select Create Custom layout for customized disk partitioning and click Next

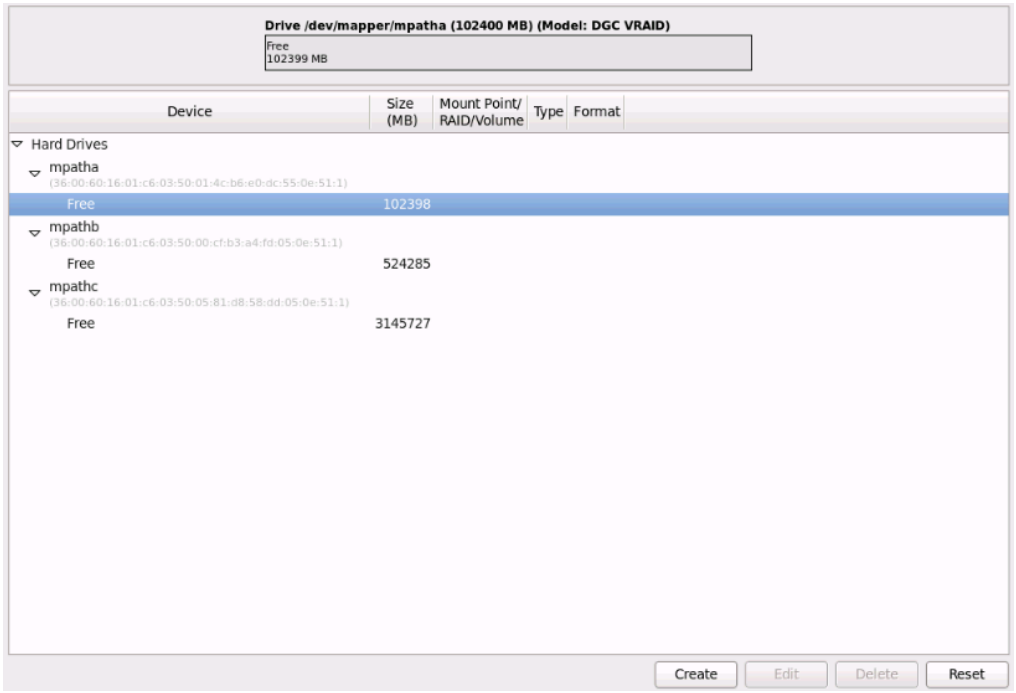





The Storage configuration in this document is only an example. You can also use a LVM based configuration. Please take care that XFS is used for /hana/log and /hana/data as the file system type

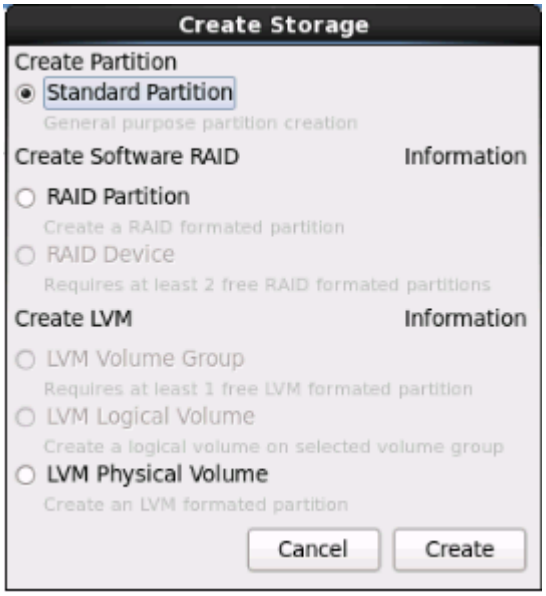
36. Select the device prepared on the storage for the operating system with the size of 100 GB

37. Click Create




38. Select Standard Partition

39. Click Create

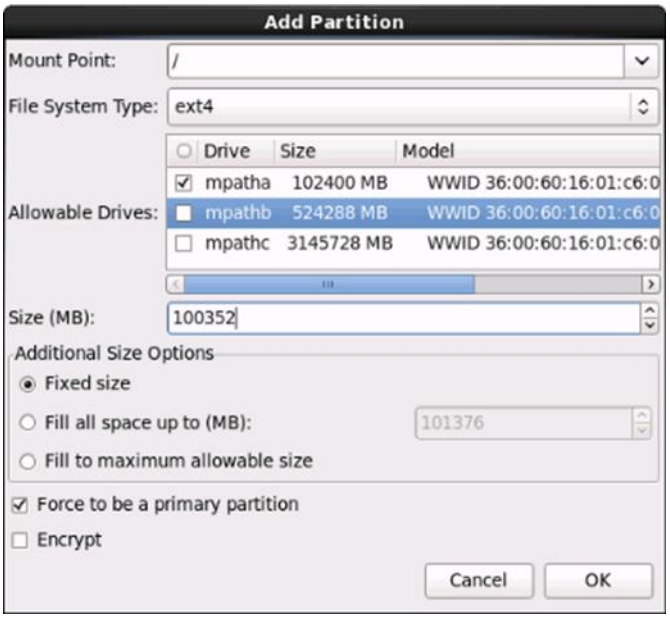



40. Enter / as the Mount Point

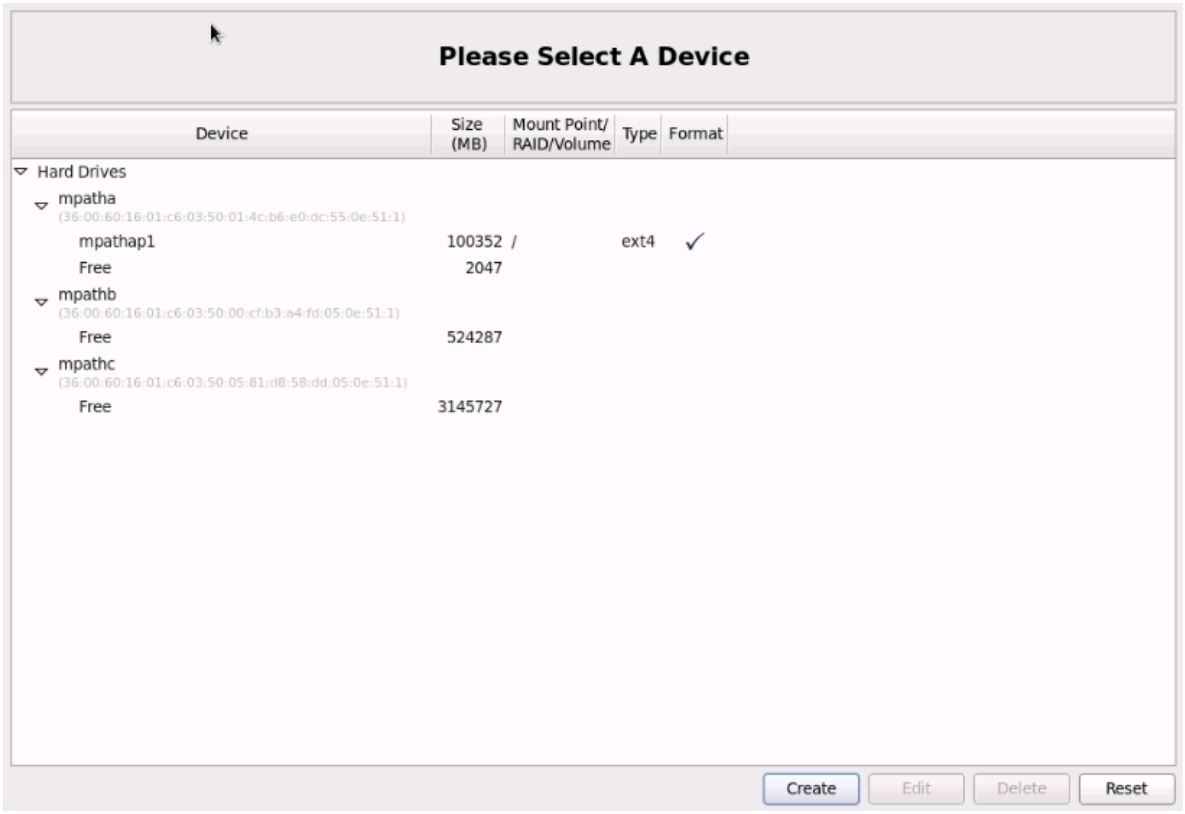
41. Select only the mpath device with the correct size

42. Enter 100352 MB (98 GB) as the Size

43. Click OK

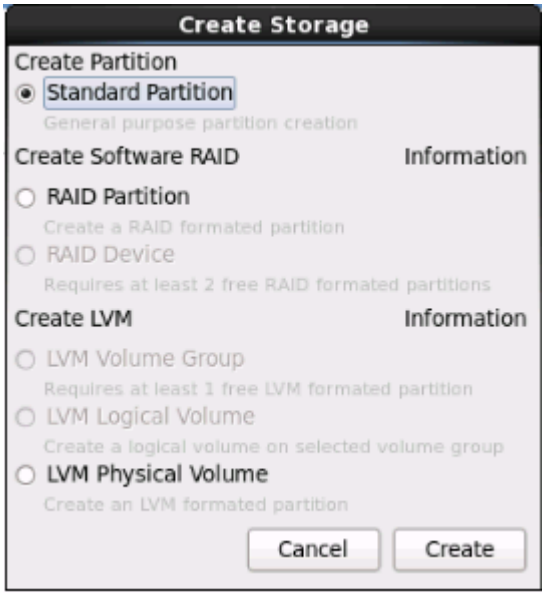



44. Back on the overview click Create




45. Select Standard Partition

46. Click Create

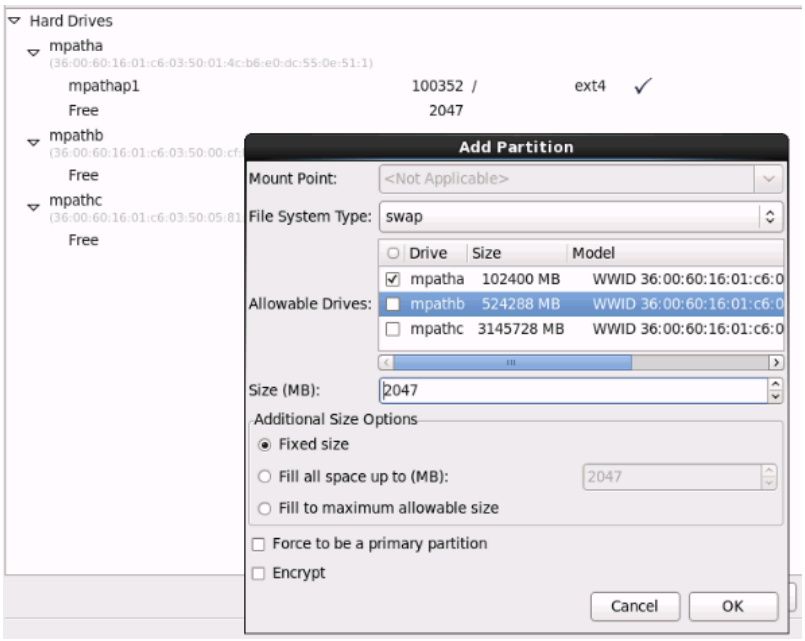



47. Select Swap from the File System Type drop-down menu

48. Select only the mpath device with the correct size

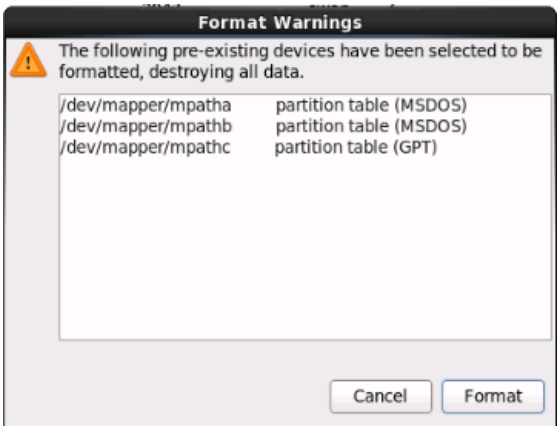
49. Enter 2047 MB as the Size, this is the free space on this device

50. Click OK




51. Back on the disk device overview screen, Click Next

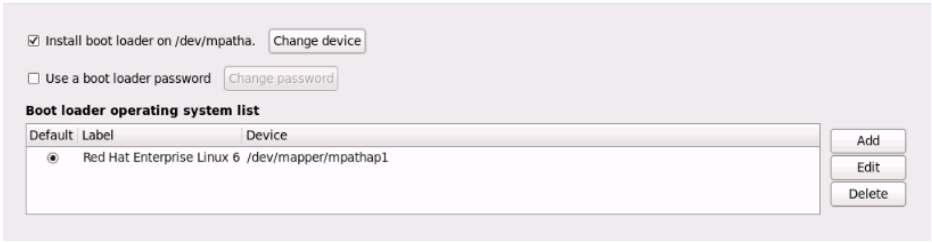
52. Click Format




53. Click Write changes to disk

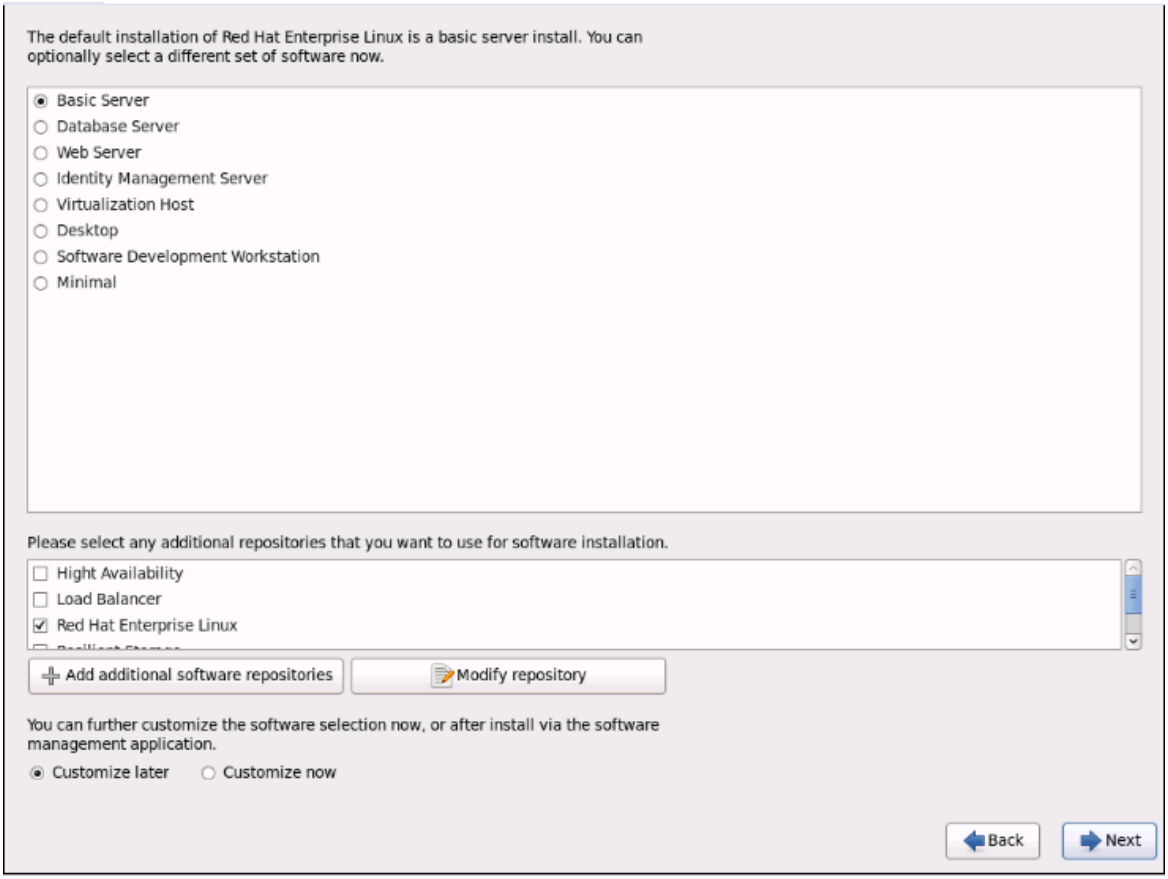



54. On the Boot Loader configuration screen, click Next



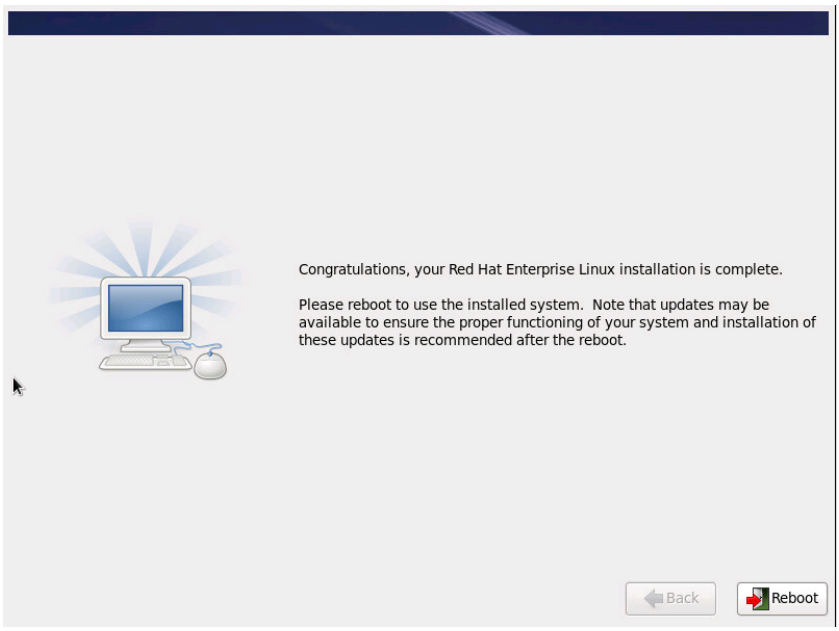

55. Select the installation mode as Basic Server

56. Click Next




57. The installer starts the installation process and wait until it is completed

58. When the installation is completed, the server requires a reboot. Click Reboot




59. Use a SSH client to login to the newly installed system as root

60. Configure DNS

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0 (or eth2)
DNS1=<<ns1_ip>>
DNS2=<<ns2_ip>>
```

The system must have access to the internet to proceed with the next steps!

61. Register the system with Red Hat to get updates

```
subscription-manager register --username <<username>> --force --auto-attach
Password:
The system has been registered with ID: xxxxxxxx-xxxx-xxxx-xxxx-6a06be40e199
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux Server
Status:       Subscribed
```

62. List all the available subscriptions to find the correct Red Hat Enterprise Linux for SAP HANA to allocate to your system:

```
subscription-manager list --available --all
```

```
+-------------------------------------------+
Available Subscriptions
+-------------------------------------------+
Subscription Name: Red Hat Enterprise Linux for SAP HANA
Provides: Red Hat Enterprise Linux 6
Red Hat Enterprise Linux for SAP Hana
Red Hat Enterprise Linux Scalable File System
SKU: SKU123456
Pool ID: e1730d1f4eaa448397bfd30c8c7f3d334bd8b
Available: 6
Suggested: 1
Service Level: Premium
Service Type: L1-L3
Multi-Entitlement: No
Ends: 01/01/2022
System Type: Physical
```

63. The SKU and Pool ID depend on the Red Hat Enterprise Linux for SAP HANA product type that corresponds to your system version and product type. Take note of the pool IDs of Red Hat Enterprise Linux for SAP HANA that correspond to your system version and product type.

```
subscription-manager subscribe –pool=<Pool_Id>
```

64. Your subscription-manager 'Release' field must be set to 6Server in order to receive the latest version of Red Hat Enterprise Linux during the installation. Set the field by using the command:

```
subscription-manager release --set=6Server
```

65. Disable all existing repositories

```
subscription-manager repos --disable "*"
```

66. Enable the Red Hat Enterprise Linux, Red Hat Enterprise Linux for SAP HANA and Red Hat Scalable Filesystem (xfs) repositories

```
subscription-manager repos --enable rhel-6-server-rpms \
  --enable rhel-sap-hana-for-rhel-6-server-rpms \
  --enable rhel-scalefs-for-rhel-6-server-rpms
```

67. Install all security updates to the system

```
yum -y install yum-security

yum --security update

yum -y update kernel kernel-firmware

yum -y groupinstall base

yum -y install xfsprogs
```

68. Check the availability of the NTP-server with utilities

service ntpd stop

ntpdate <<var_ntp_server>>

service ntpd start

69. Check if the ntp service is enabled

chkconfig | grep ntpd

ntpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

ntpdate 0:off 1:off 2:off 3:off 4:off 5:off 6:off

chkconfig ntpd on

70. The ntpdate service script adjusts the time according to the ntp server every time when the system comes up. This happens before the regular ntp service is started and ensures an exact system time even if the time deviation is too big to be compensated by the ntp service.

echo <<var_ntp_server>> >> /etc/ntp/step-tickers

chkconfig ntpdate on

71. Install dependencies in accordance with the SAP HANA Server Installation and Update Guide and the numactl package if the benchmark HWCCT is used :

```
yum install libicu xulrunner expect cairo graphviz iptraf krb5-libs.i686 nfs-
utils lm_sensors openssl098e openssl PackageKit-gtk-module libcanberra-gtk2 xauth
compat-libstdc++-33 libgomp tuned icedtea-web compat-sap-c++
```

72. Disable SELinux:

```
# sed -i 's/^SELINUX=enforcing/SELINUX=disabled/g' /etc/sysconfig/selinux

# sed -i 's/^SELINUX=permissive/SELINUX=disabled/g' /etc/sysconfig/selinux
```

73. Disable kdump Service:

```
service kdump stop
```

```
chkconfig kdump off
```

74. Sysctl.conf: The following parameters must be set in /etc/sysctl.conf

```
# Parameters for HANA
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.ip_local_port_range=40000 61000
net.ipv4.neigh.default.gc_thresh1=256
net.ipv4.neigh.default.gc_thresh2=1024
net.ipv4.neigh.default.gc_thresh3=4096
net.ipv6.neigh.default.gc_thresh1=256
net.ipv6.neigh.default.gc_thresh2=1024
net.ipv6.neigh.default.gc_thresh3=4096
kernel.shmmax=137438953472
kernel.shmall=33554432
# Next line modified for SAP HANA Database on 2014.11.05_18.49.07
kernel.shmmni=524288
kernel.msgmni=32768
kernel.sem=1250 256000 100 8192
kernel.sysrq=1
vm.swappiness=60
# Next line modified for SAP HANA Database on 2014.11.05_18.49.07
vm.max_map_count=102000000
vm.memory_failure_early_kill=1
fs.file-max=20000000
fs.aio-max-nr=458752
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

75. Compat-sap-c++ Install the most important package compat-sap-c++ from the RHEL for SAP HANA. At the time of this lab installation the tuned-profiles-sap-hana where available in the version 0.2.9.19-13 and requires the same version for the tuned package. Please check at the time of the installation which version to install – you can try “yum install tuned-profiles-sap-hana*” and check the dependencies:

```
yum install tuned-profiles-sap-hana tuned

yum install resource-agents-sap-hana

tuned-adm profile sap-hana
```

76. Add the following line into /etc/modprobe.d/sunrpc-local.conf, Create the file, if it does not exist:

```
sunrpc.tcp_max_slot_table_entries = 128
```

77. For compatibility reasons, four symbolic links are required:

```
ln -s /usr/lib64/libssl.so.0.9.8e /usr/lib64/libssl.so.0.9.8
ln -s /usr/lib64/libssl.so.1.0.1e /usr/lib64/libssl.so.1.0.1
ln -s /usr/lib64/libcrypto.so.0.9.8e /usr/lib64/libcrypto.so.0.9.8
ln -s /usr/lib64/libcrypto.so.1.0.1e /usr/lib64/libcrypto.so.1.0.1
```

78. Transparent Hugepages in the file /boot/grub/grub.conf add the kernel command line argument:

```
transparent_hugepage=never
```

79. Create User-Group sapsys:

```
groupadd –g 401 sapsys
```

80. Disable abrt service which handles application crashes:

```
chkconfig abrtd off
chkconfig abrt-ccpp off
service abrtd stop
service abrt-ccpp stop
```

81. Disable core file creation. To disable core dumps for all users, open /etc/security/limits.conf, and add the line:

```
* soft core 0
* hard core 0
```

82. Edit the /boot/grub/menu.lst and append the below parameter to the kernel line per SAP Note:

```
intel_idle.max_cstate=0
```

83. Adopt the multipath.conf information

```
defaults {
checker_timeout         60
user_friendly_names     no
}
# ALUA Configuration
#devices {
#        device {
```

```
#                vendor                  "DGC"
#                product                 ".*"
#                product_blacklist      "LUNZ"
#                path_grouping_policy    group_by_prio
#                prio                    emc
#                hardware_handler        "1 alua"
#                features                "1 queue_if_no_path"
#                no_path_retry           60
#                path_checker            emc_clariion
#                failback                immediate
#                flush_on_last_del       yes
#                fast_io_fail_tmo        off
#                dev_loss_tmo            120
#        }
#}
# Active/Passive Configuration
devices {
        device {
                vendor                    "DGC"
                product                   ".*"
                product_blacklist         "LUNZ"
                features                  "0"
                hardware_handler          "1 emc"
                path_selector             "round-robin 0"
                path_grouping_policy      group_by_prio
                failback                  immediate
                rr_weight                 uniform
                no_path_retry             5
                rr_min_io                 1000
                path_checker              emc_clariion
                prio                      emc
                flush_on_last_del         yes
                fast_io_fail_tmo          off
                dev_loss_tmo              120
        }
}
```

84. Reboot the system:

```
Reboot
```



**Distributed installation of HANA fails after updating package libssh2 to version 1.4.2-1.el6_6.1.x86_64.**

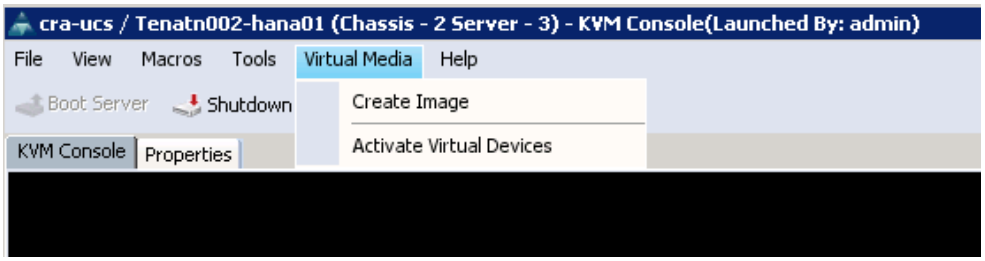
Version 1.4.2-1.el6_6.1.x86_64 triggers an incompatibility with different libssl and libcrypto versions. Please downgrade libssh2 to version libssh2-1.4.2-1.el6.x86_64. More detailed information can be found in the following Red Hat Knowledgebase Article: https://access.redhat.com/solutions/1370033 (Red Hat customer portal login required)

**HANA fails to start after updating package nss-softokn-freebl to version 3.14.3-17**

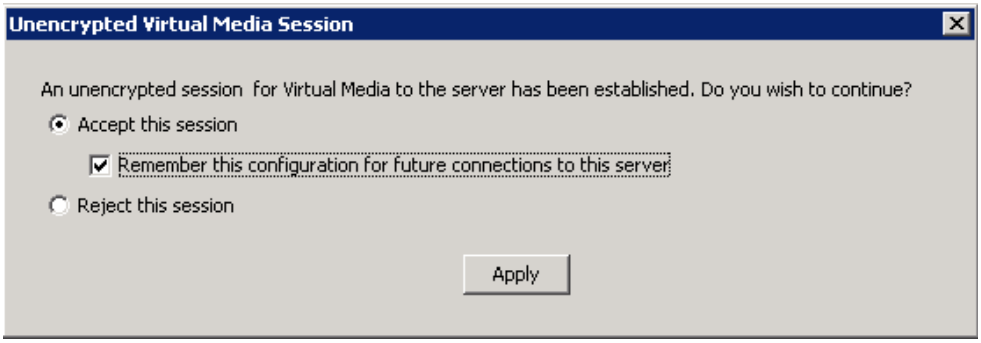
Version 3.14.3-17 of package nss-softokn-freebl triggers a bug in GlibC that hinders HANA to start. Please update to glibc-2.12-1.149.el6_6.4 or newer and nss-softokn-freebl to 3.14.3-19.el6_6 or newer in order to resolve the problem. More detailed information can be found in the following Red Hat Knowledgebase Article: https://access.redhat.com/solutions/1236813 (Red Hat customer portal login required).

## SUSE Linux Enterprise 11

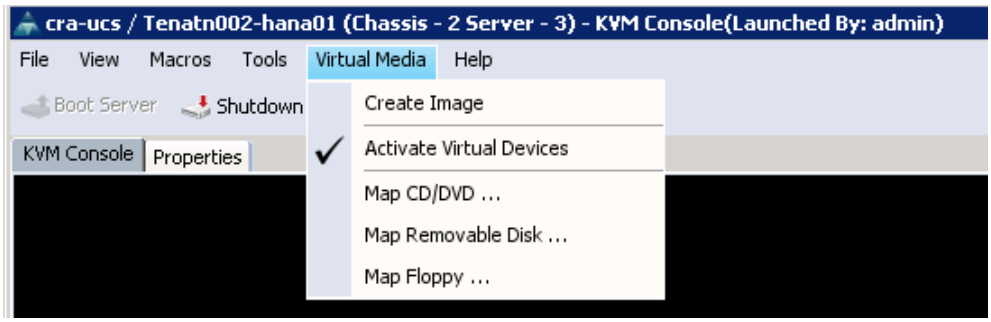
1. Go to the Cisco UCS Manager and select the Service Profile
2. Click KVM Console
3. Click the Menu Virtual Media
4. Select Activate Virtual Devices




5. In the new Window, Select Accept this Session. If you like you can also select the check box to Remember this setting
6. Click Apply

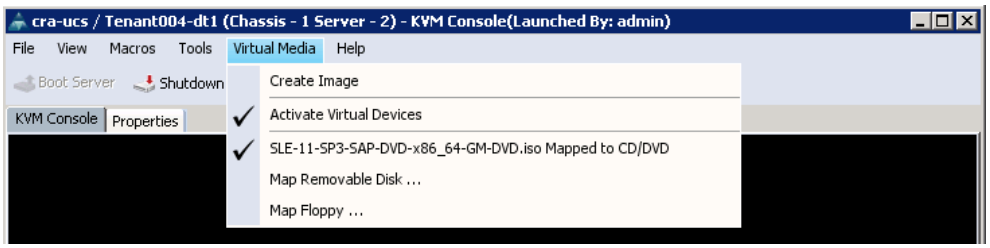



7. Click again on the Menu Virtual Media
8. Select Map CD/DVD...

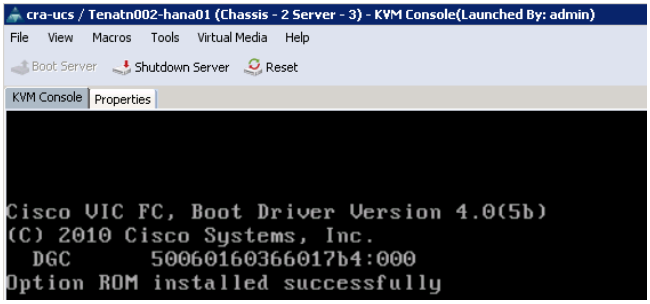



9. Click Browse, and select the Suse Linux Enterprise ISO

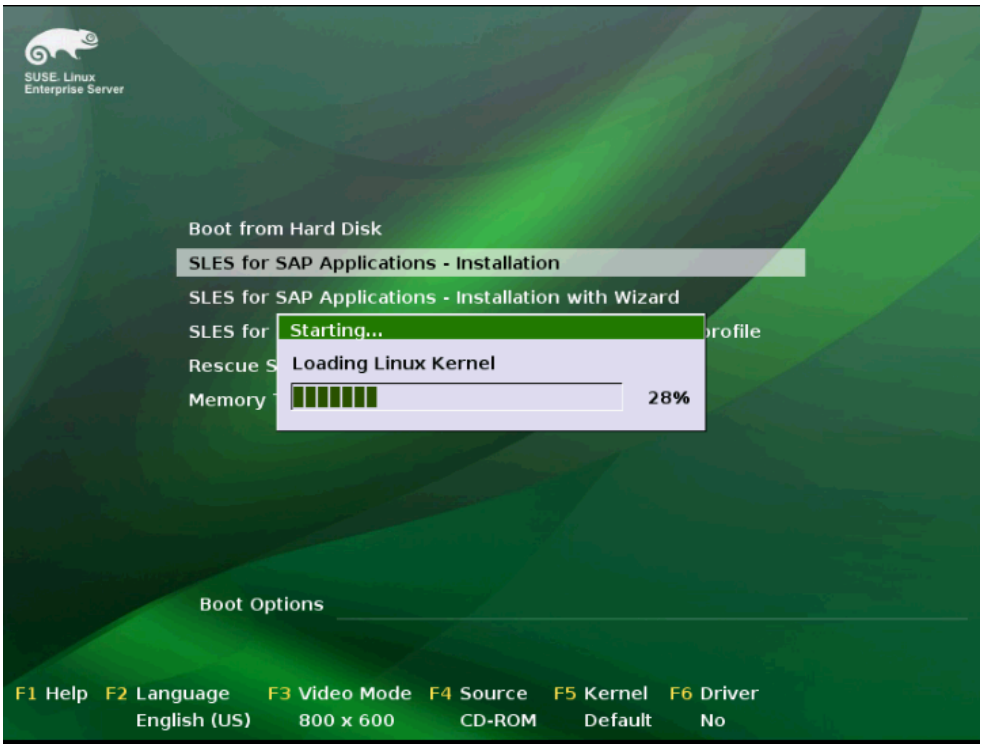
10. Click Map Device




11. Click Reset to reset the server. This will force the system to scan the SAN and get access to the LUNs on the EMC VNX.



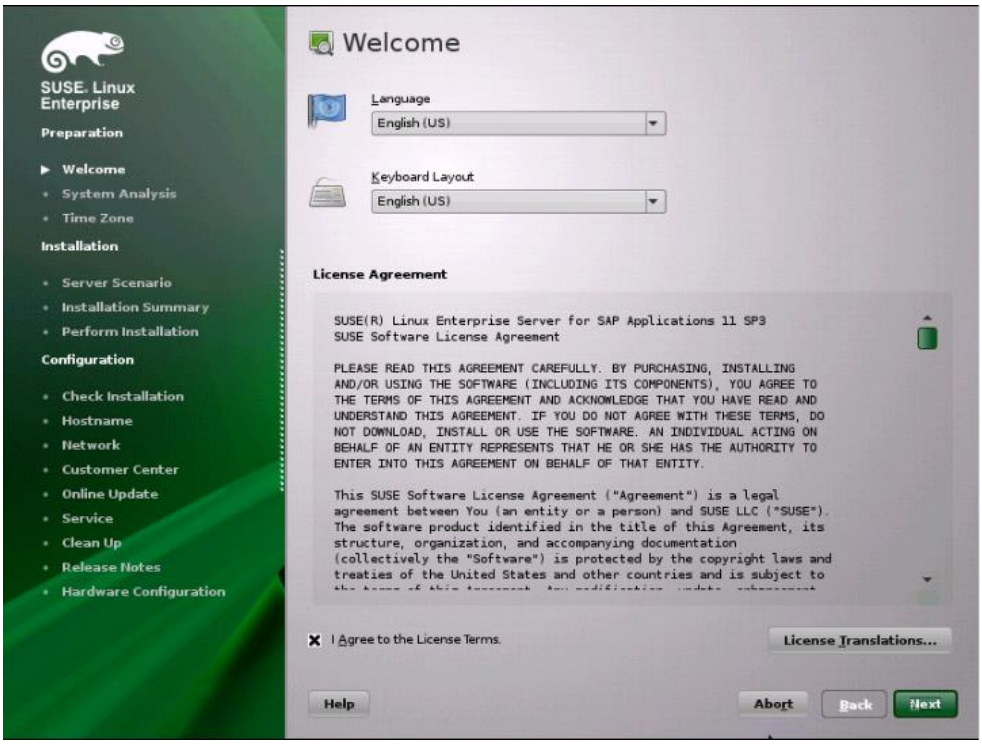

12. The System will automatically boot from the ISO image



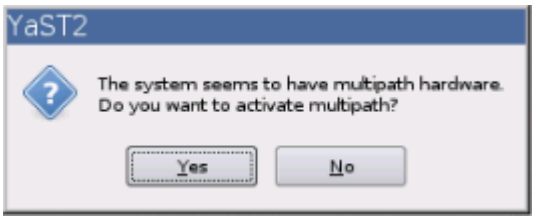

13. Follow the instructions on the screens and select the settings that fits best for you until the Installation Summary Screen.

    The best way to interact with the system is through keyboard short-cuts. You can see that some letters are marked with underline, i.e. I Agree ... or Next.

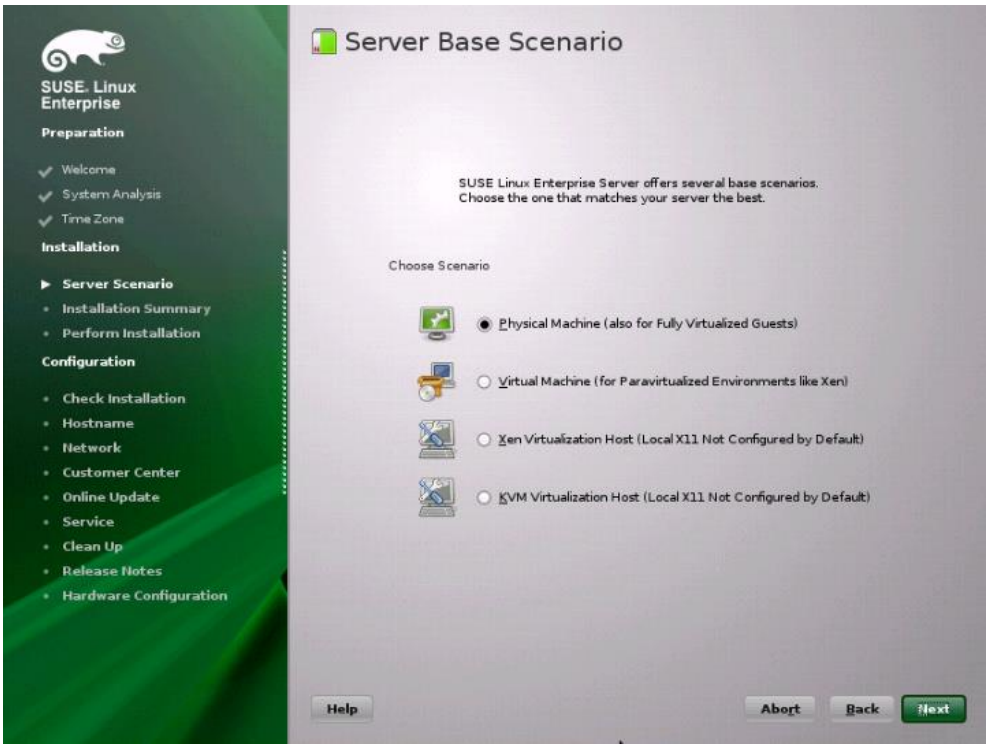
    You can now use the ALT key together with the letter that is underlined to activate this option or to go to the next screen. As shown in the next screen ALT+A marks the check-box to Agree the License Terms and with ALT+N you can go to the Next screen.

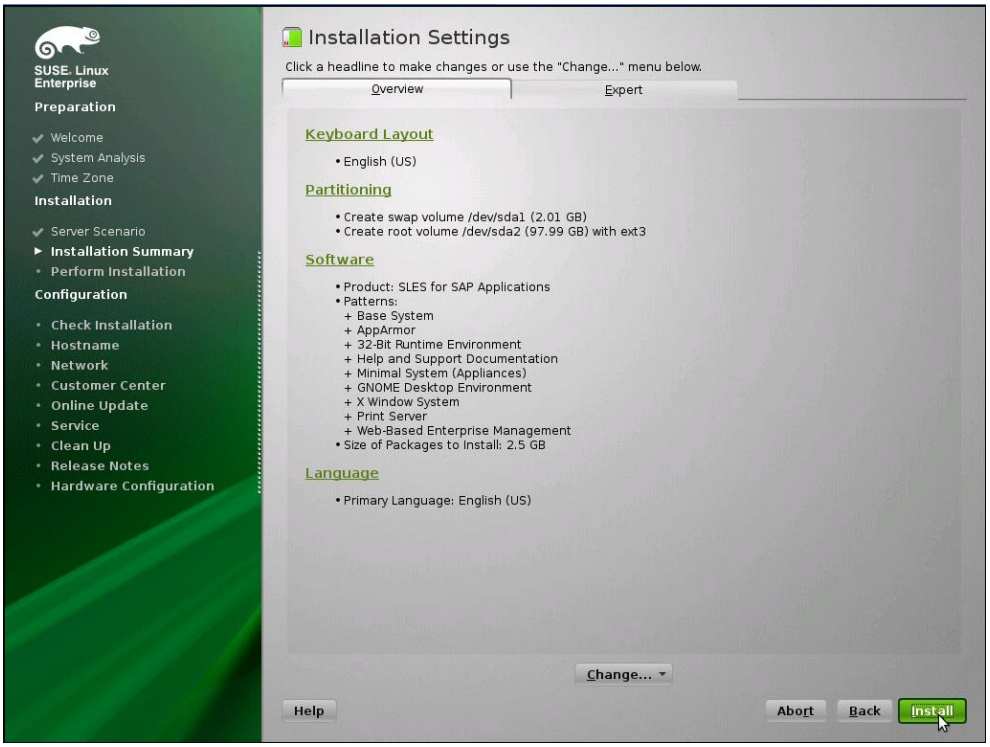



14. As multipathed disk devices are used please answer the following question with Yes (ALT+Y).




15. Set the Server Base Scenario to Physical Machine in case you install the linux system on the Service Profile or within a VMware virtual machine.




16. Click Change.

17. Select Partitioning

18. Select the disk (UUID) created to host the operating system.
    In case you do not have the UUID at hand. Please go to a free command shell (ALT+STRG+F2) and run multipath –ll | egrep “DGC|size”. This shows a list of the UUIDs and in the next line the size of the LUN.

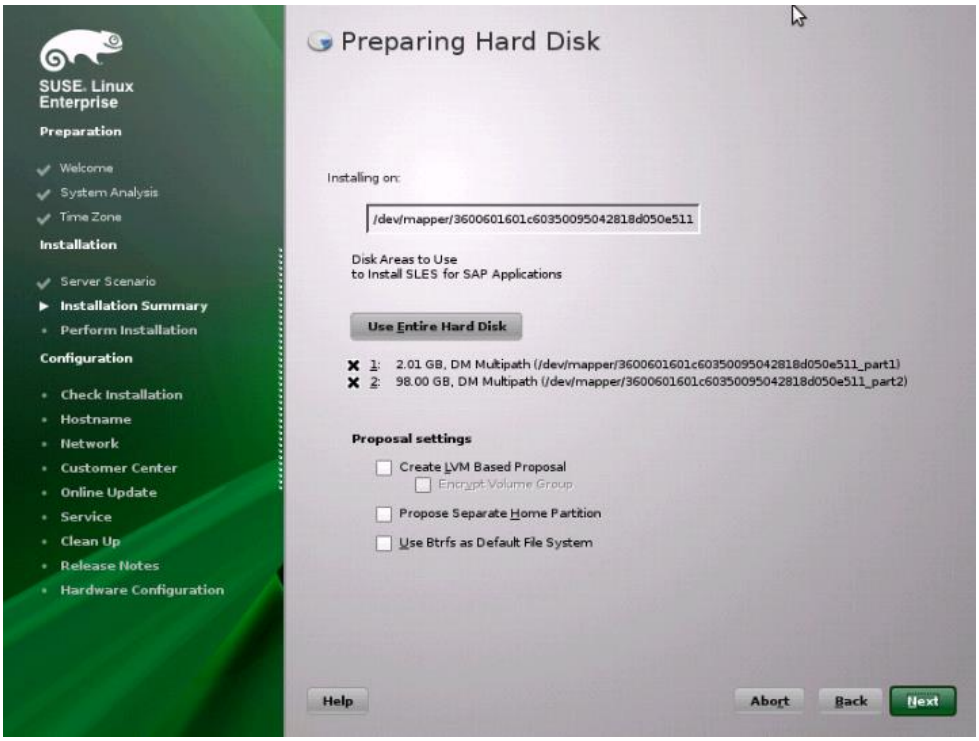
```
/ # multipath -ll |egrep "DGC|size"
3600601601c60350055181ee8d250e511 dm-1 DGC     ,VRAID
size=200G features='1 queue_if_no_path' hwhandler='1 emc' wp=rw
3600601601c6035000a43a9f0ed350e511 dm-2 DGC     ,VRAID
size=6.0T features='1 queue_if_no_path' hwhandler='1 emc' wp=rw
3600601601c60350095042818d050e511 dm-0 DGC     ,VRAID
size=100G features='1 queue_if_no_path' hwhandler='1 emc' wp=rw
3600601601c60350053ebfb71d350e511 dm-3 DGC     ,VRAID
size=160G features='1 queue_if_no_path' hwhandler='1 emc' wp=rw
/ #
```

19. Press ALT+STRG+F7 to go back to the installation screen




20. Click Next

21. Select “Use Entire Hard Disk”, we do not use a LVM based proposal. You can use this if you prefer to use Logical Volume Manager of if this is your datacenter default.

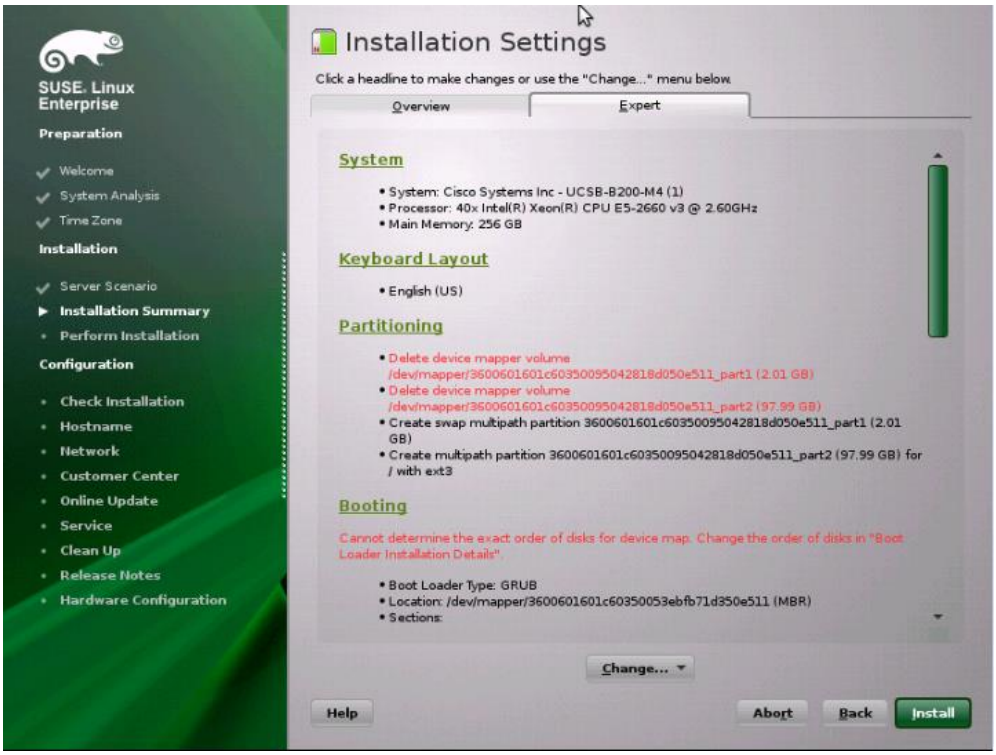



22. Click Next

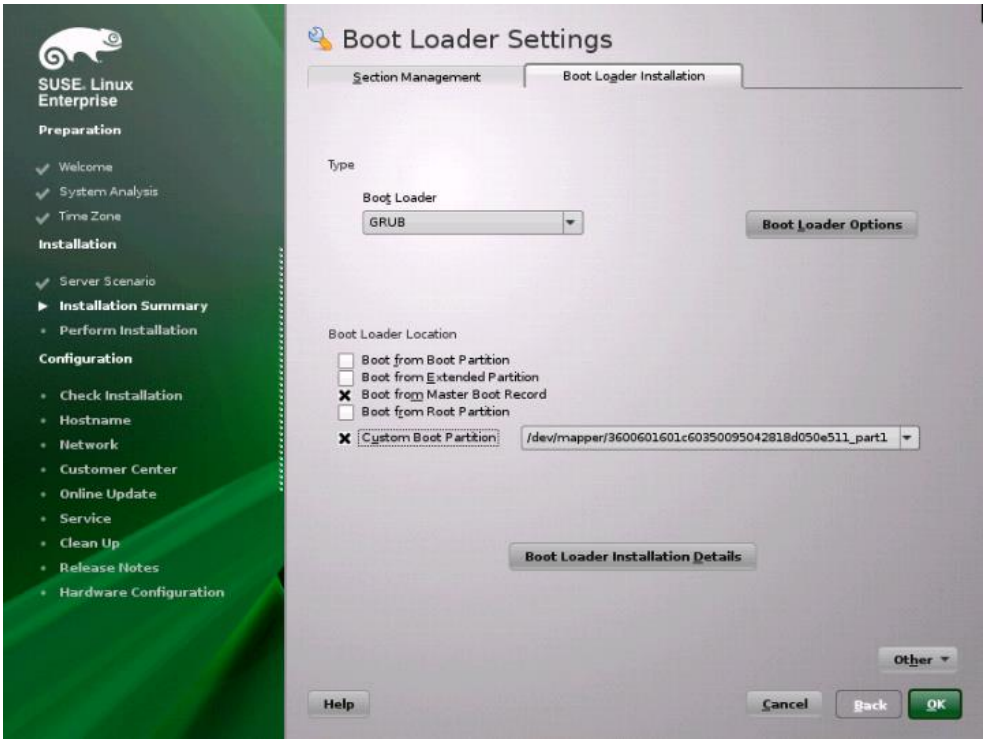


The configuration of the Boot system is very important and you should follow the steps very carefully. If not done the installed operating system will not boot as the bootloader is installed on the wrong disk and points to the wrong disk.

23. Click the Expert View tab or use ALT-E



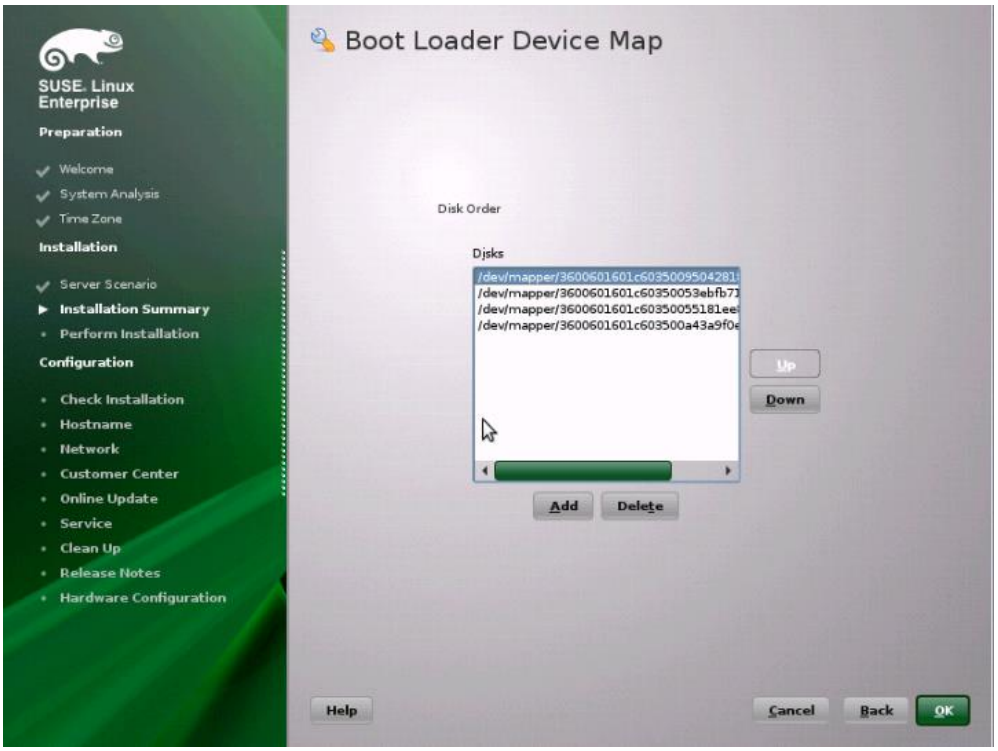

24. Click Chance and select Boot and Click the “Boot Loader Installation” tab



25. Select Customer Boot Partition, take care that the correct partition is selected.

26. Click “Boot Loader Installation Details”

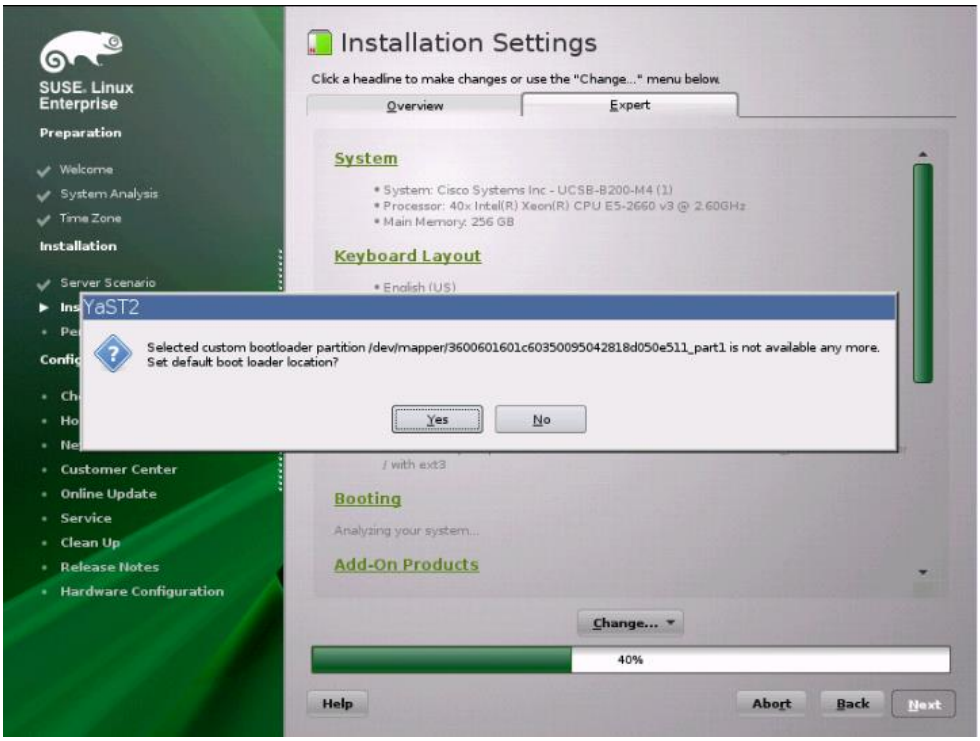
27. Take care that the boot disk is the first (top of list) in the disk list




28. Click OK

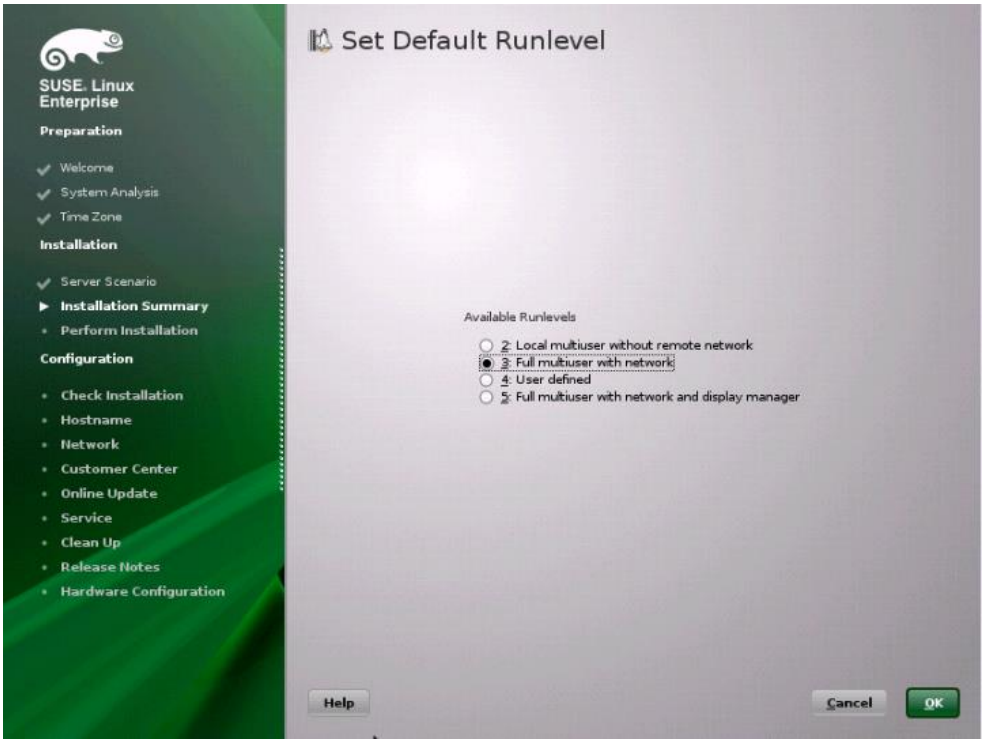
29. Back on the Boot Loader Settings screen, click OK

30. The System will come up with an information window, click Yes

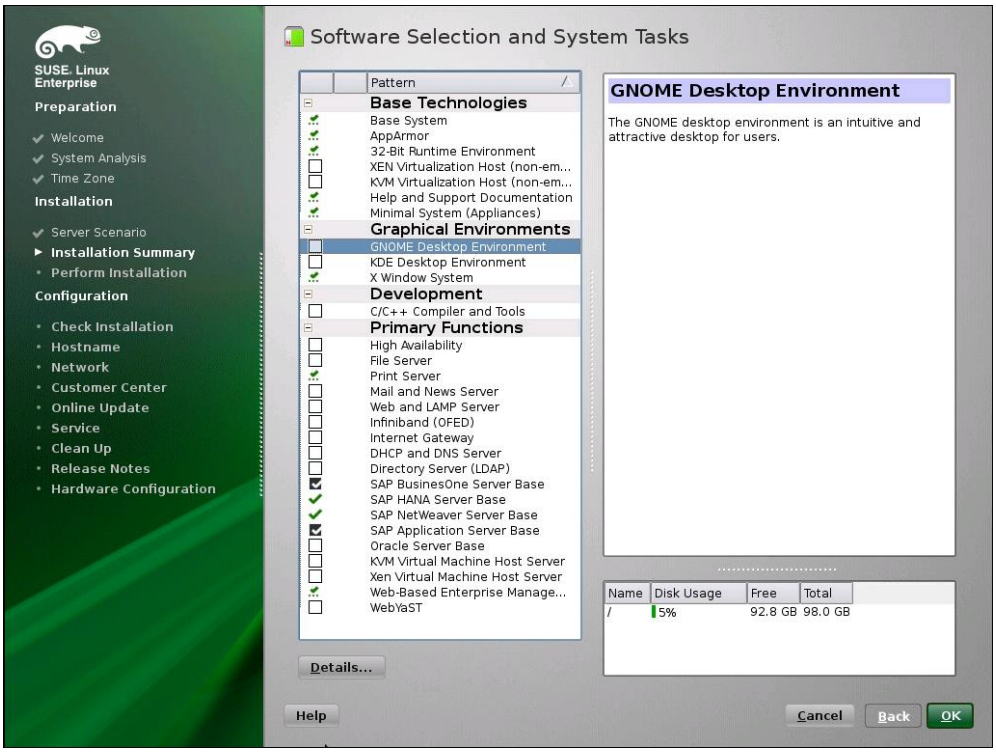



31. Click Change and select Default Runlevel

32. Select 3: Full multiuser with network, click OK



33. Click Change and select Software.
34. Unselect GNOME Desktop Environment.
35. Select SAP HANA Server Base.
36. Click OK.
37. Click Accept.




38. Click Install.
39. On the Confirm Installation Window, click Install.
40. SUSE Enterprise Linux installation will start and after the packages are installed the system automatically reboots.
41. After the reboot, enter <<var_mgmt_passwd>> as the Password.
42. On the Network configuration screen, click Disable in the Firewall section.
43. Click Network Interfaces.
44. Select eth0 (or eth2 on a C-Series server).
45. Click Edit.

46. Select Static assigned IP Address.

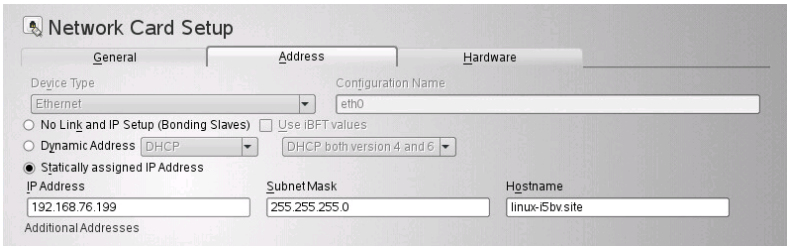
47. Enter <<var_mgmt_temp_ip>> as the IP Address – This IP Address is only temporarily used.



Please take care that the system has access to the internet or an Suse Update server to install the patches.

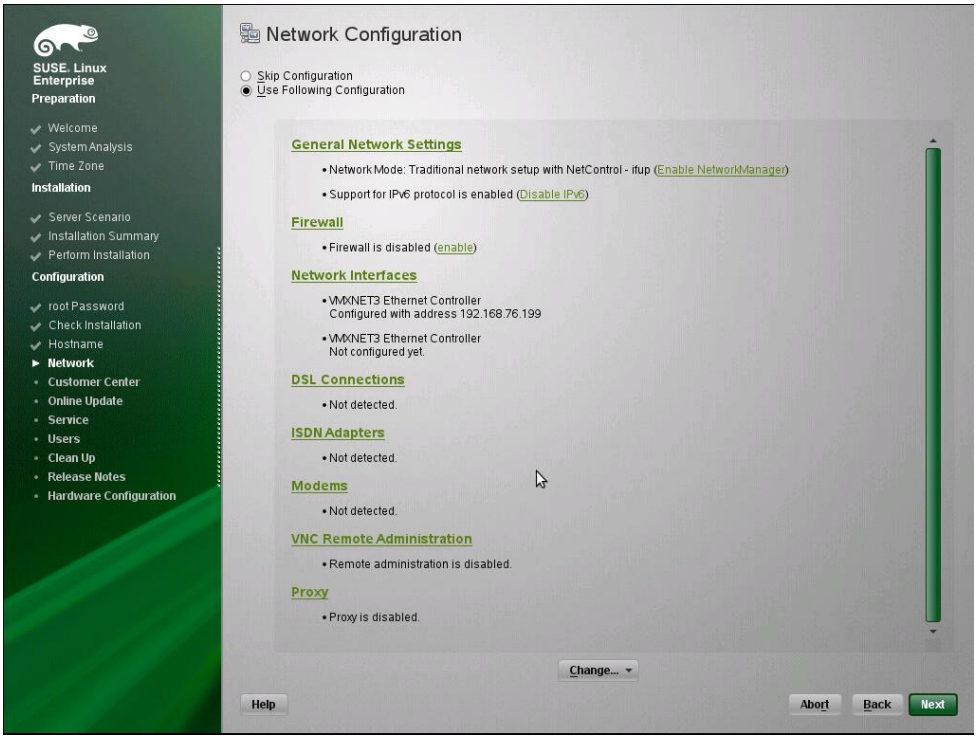
48. Enter <<var_mgmt_mask>> as the Subnet Mask.

49. Click Next.

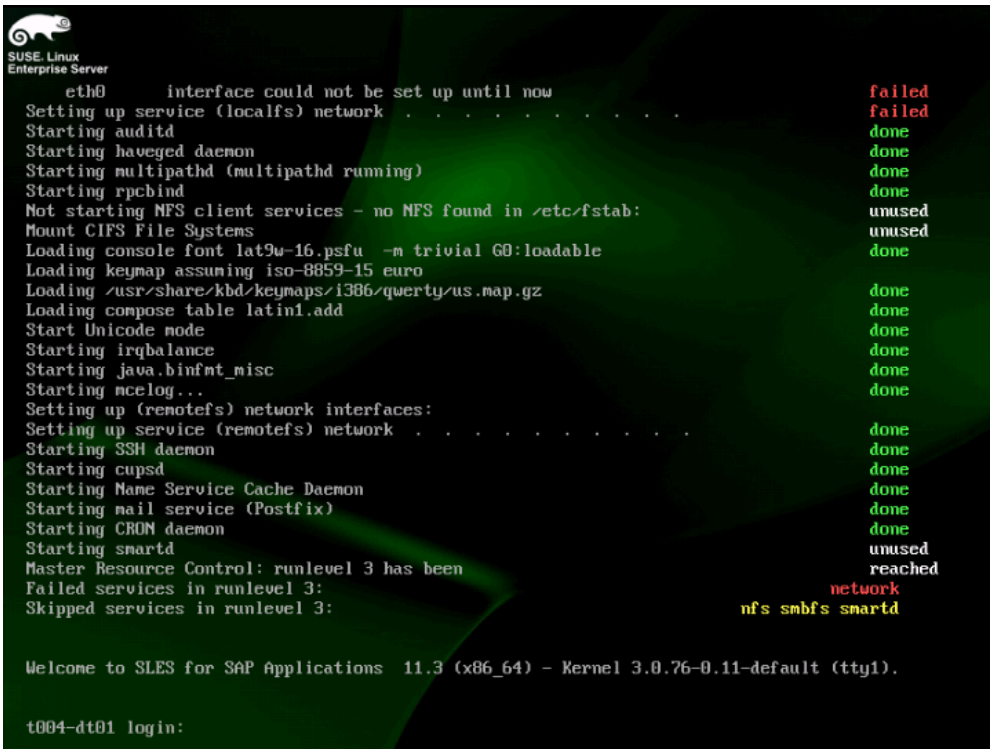



50. Click OK.

51. From the Network Configuration Screen, click Next.




52. Skip the Network Test and follow the instructions on the following screens until the configuration is finished.




53. Use the KVM console or a SSH client to log in to the installed system with the user root and the password <<var_mgmt_passwd>>.

54. Register the System at SUSE to get latest Patches.

The system must have access to the internet to proceed with this step.

suse_register -i -r -n -a email= <<email_address>> -a regcode-sles=<<registration_code>>

55. Update the system with the following command:

The system must have access to the internet to proceed with this step!

```
zypper update
```

56. Follow the on screen instructions to complete the update process. Reboot the server and login to the system again.

57. Configure the Network Time Protocol:

```
vi /etc/ntp.conf
server <<var_global_ntp_server_ip>>
fudge <<var_global_ntp_server_ip>> stratum 10
keys /etc/ntp.keys
trustedkey 1
```

58. Create User-Group sapsys:

```
groupadd –g 401 sapsys
```

59. It is recommended to disable Transparent Huge Pages and the swappiness on the system:

```
vi /etc/init.d/after.local

#!/bin/bash
# (c) Cisco Systems Inc. 2014
echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status
# set sappiness to 30 to avoid swapping
echo "Set swappiness to 30 to avoid swapping"
echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status
```

60. Based on different SAP Notes multiple entries in /etc/sysctl.conf are required:

```
vi /etc/sysctl.conf

#SAP Note 1275776
vm.max_map_count = 2000000
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
net.ipv4.tcp_slow_start_after_idle = 0
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
```

```
net.ipv4.tcp_wmem = 65536 262144 16777216

net.ipv4.tcp_no_metrics_save = 1

net.ipv4.tcp_moderate_rcvbuf = 1

net.ipv4.tcp_window_scaling = 1

net.ipv4.tcp_timestamps = 1

net.ipv4.tcp_sack = 1

sunrpc.tcp_slot_table_entries = 128

# Memory Page Cache Limit Feature SAP Note 1557506

vm.pagecache_limit_mb = 4096

vm.pagecache_limit_ignore_dirty = 1
```

61. Edit boot loader configuration file /etc/sysconfig/bootloader. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

```
intel_idle.max_cstate=0
```

62. Append the intel_idle.max_cstate=0 processor.max_cstate=0 value to the kernel's parameter line in /boot/grub/menu.lst – 3.0.xxx-x.xx is the placeholder for your Kernel patch version:

```
vi /boot/grub/menu.lst


title SLES for SAP Applications - 3.0.XXX-X.XX

root (hd0,0)

kernel /boot/vmlinuz-3.0.XXX-X.XX-default root=/dev/sda2 resume=/dev/sda1
splash=silent showopts intel_idle.max_cstate=0 processor.max_cstate=0

initrd /boot/initrd-3.0.XXX-X.XX-default
```

63. Reboot the server:

```
reboot
```

## Virtualized SAP HANA Scale-Up System (vHANA)

This is a common deployment methodology of SAP HANA in a private and public cloud model. Reference SAP and VMware for the actual limitations for virtualized SAP HANA on VMware ESXi before you start the deployment.

To deploy vHANA, complete the following high-level steps:

1. Create the access VLAN on Cisco Nexus 9000, Cisco UCS, and Cisco Nexus1000V.

2. Check the Space on the VMware datastore and create a new one if required.

3. Deploy the Virtual Machine from the VM Template.
4. Create VMDKs for SAP HANA.
5. Install SAP HANA.
6. Test the connection to the SAP HANA database.

## Workload Definition

This vHANA system is defined as requiring the SAP HANA system having a size of 256GB main memory, it is for non-production, and must run on Red Hat Enterprise Linux.

## Requirements

For a virtualized SAP HANA database, the only network that is required is the access network. Storage is provided through VMDKs. To access the installation sources for SAP HANA and other applications, the access to the NFS share on the EMC VNX storage is also configured; this can be temporary only until all applications are installed. All other networks are optional. For this use case, no optional network is used. This is the first system for a tenant, so no existing network definition can be used. Since this is for non-production, the relaxed storage requirements apply. The following configuration is required:

Network: 1x Access Network with >=100Mbit/sec

1x NFS-Access Network (to access the installation sources)

Storage: 256GB for /hana/log, 384GB for /hana/data, 256GB for /hana/shared

An average of 50 MB/sec throughput can be used as the baseline. Dependent on the use case it can be less (default analytics) or much more (heavy Suite on HANA)

Memory: 256GB

CPU: 30 vCPUs, as we use Ivy Bridge CPUs in the Lab

## Create VLANs

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

1. On each Cisco Nexus 9000, enter the configuration mode:

```
config terminal
```

2. From the configuration mode, run the following commands:

```
vlan <<var_t001_access_vlan_id>>
name T001-Access
```

3. Add the VLAN to the VPC Peer-Link:

```
interface po1
switchport trunk allowed vlan <<var_t001_access_vlan_id>>
```

4. Add the VLAN to the Port Channels connected to the Cisco UCS:

```
interface po13,po14
switchport trunk allowed vlan <<var_t001_access_vlan_id>>
```

5. Add the VLAN to the data center uplink

```
interface po99
switchport trunk allowed vlan add <<var_t001_access_vlan_id>>
```

6. Save the running configuration to start-up:

```
copy run start
```

7. Validate the configuration:

```
#show vpc
…
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,2031,2034,3001

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
11   Po11   up     success     success                    76,177,199,
                                                          2031,2034
12   Po12   up     success     success                    76,177,199,
                                                          2031,2034
13   Po13   up     success     success                    76,177,199,
                                                          2031,2034,3
                                                          001
14   Po14   up     success     success                    76,177,199,
                                                          2031,2034,3
                                                          001
…

show vlan id 3001
VLAN Name                             Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
3001 Tenant001-Access                 active    Po1, Po13, Po14, Po99, Eth1/1
                                                Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                Eth1/9, Eth1/10, Eth1/15
                                                Eth1/16, Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3001 enet         CE

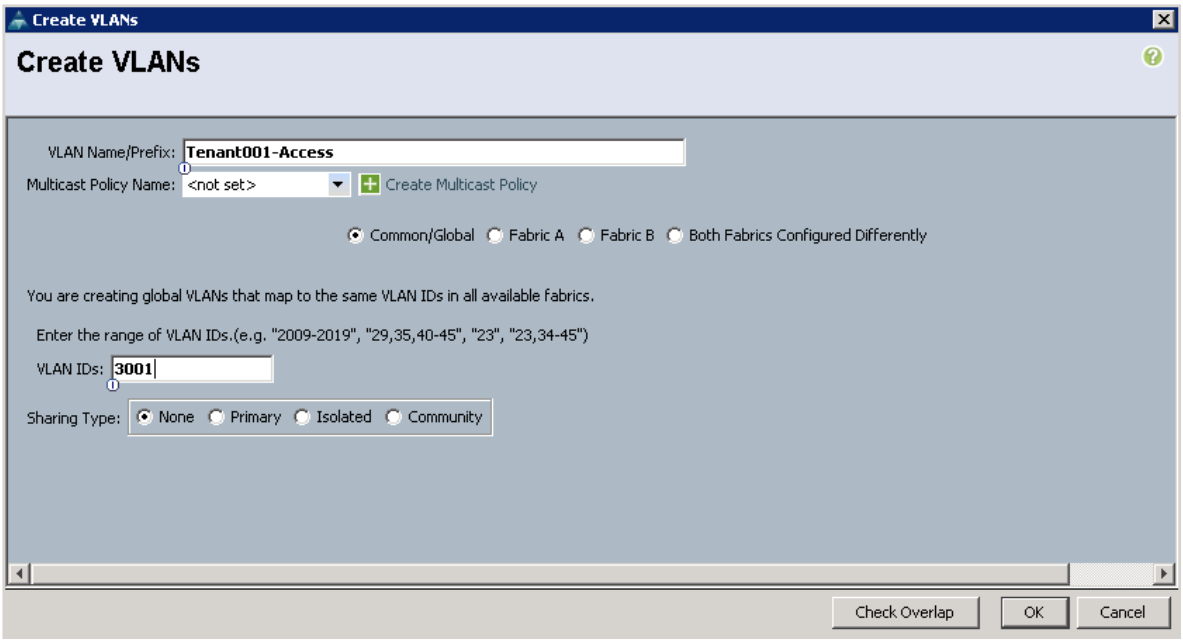
Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

## Create VLAN in Cisco UCS

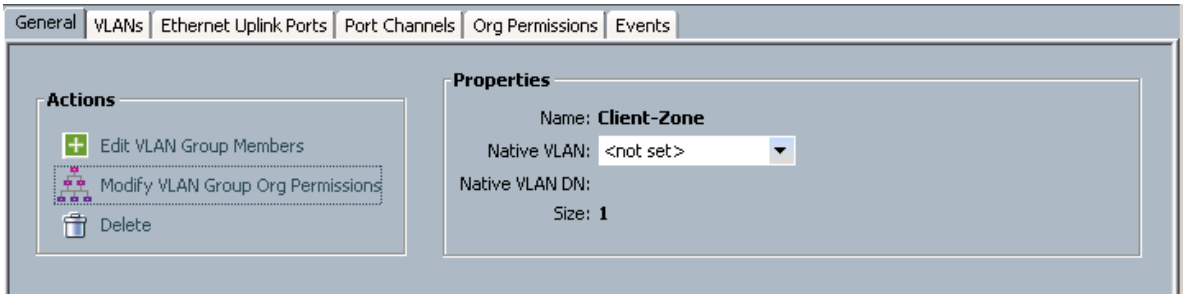
To create a VLAN in Cisco UCS, complete the following steps:

1. Log on to Cisco UCS Manager.
2. Go to LAN Tab > LAN Cloud > VLANs.
3. Right-Click > Create VLANs.
4. Enter <<var_ucs_t001_access_vlan_name>> as the VLAN Name.
5. Enter <<var_t001_access_vlan_id>> as the VLAN ID.
6. Click OK.
7. Click OK.

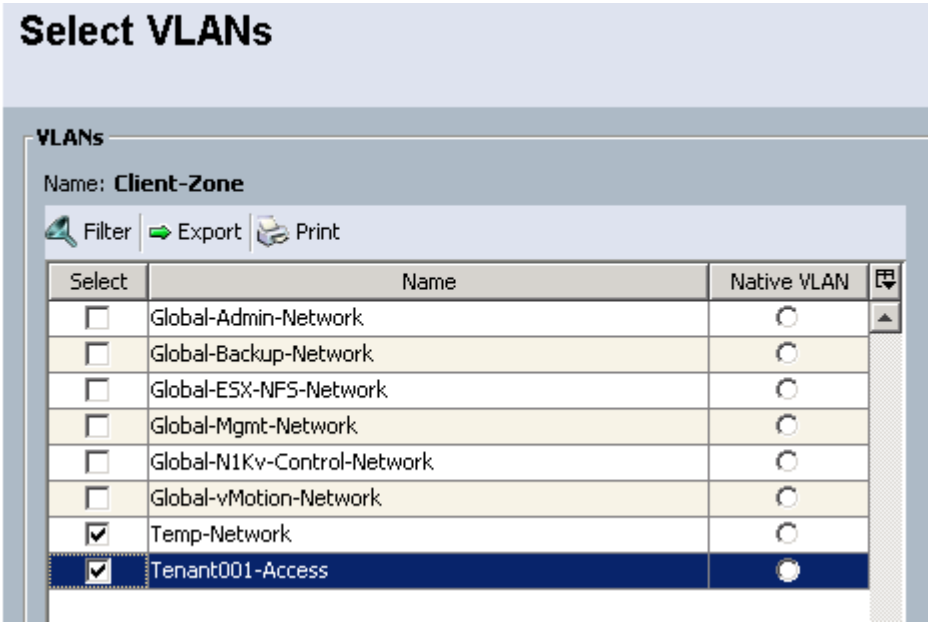



8. Go to LAN Tab > LAN Cloud > VLAN Groups.
9. Select VLAN group Client-Zone.
10. Click the Info Icon 

on the right side of the list.
11. Click Edit VLAN Group Members.




12. Select <<var_ucs_t001_access_vlan_name>>.
13. Click Finish.



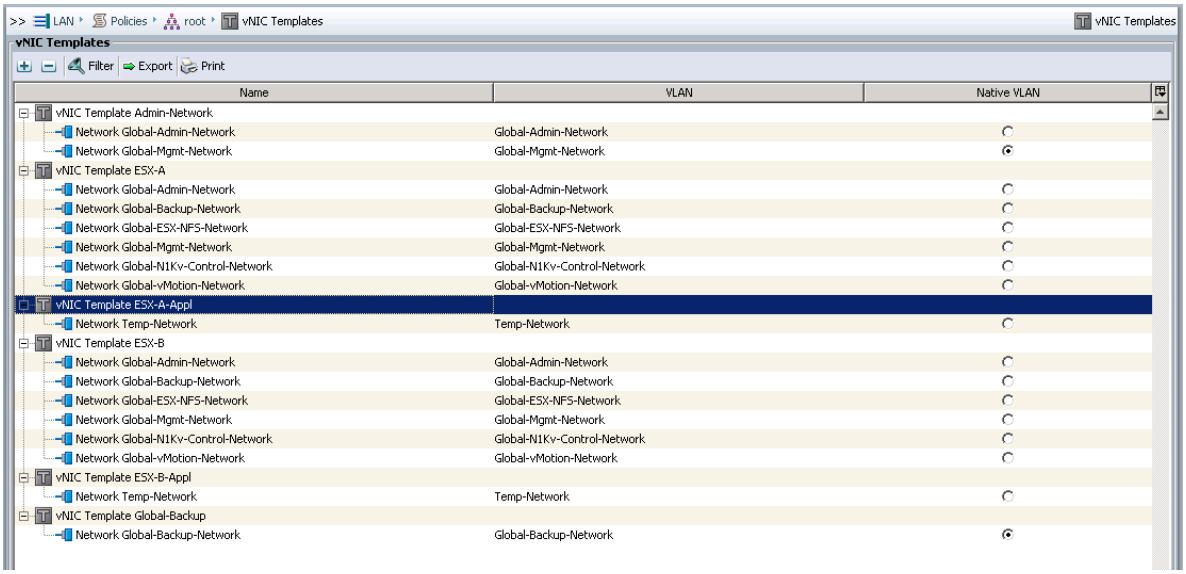

14. Click OK.

15. Go to LAN Tab > Policies > root > vNIC Templates.

16. Select vNIC <<var_ucs_esx_a_appl_vnic_name>> on the right pane.

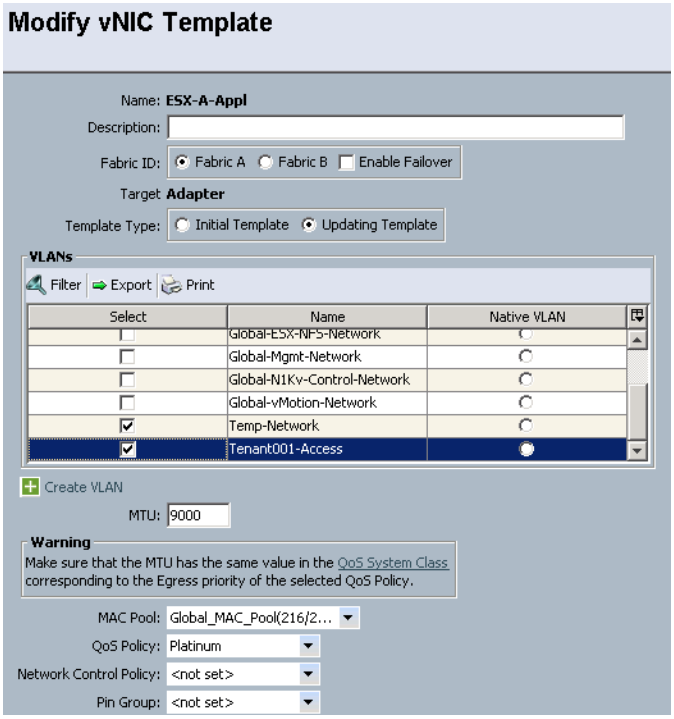
17. Click the Info Icon  on the bottom of the list.



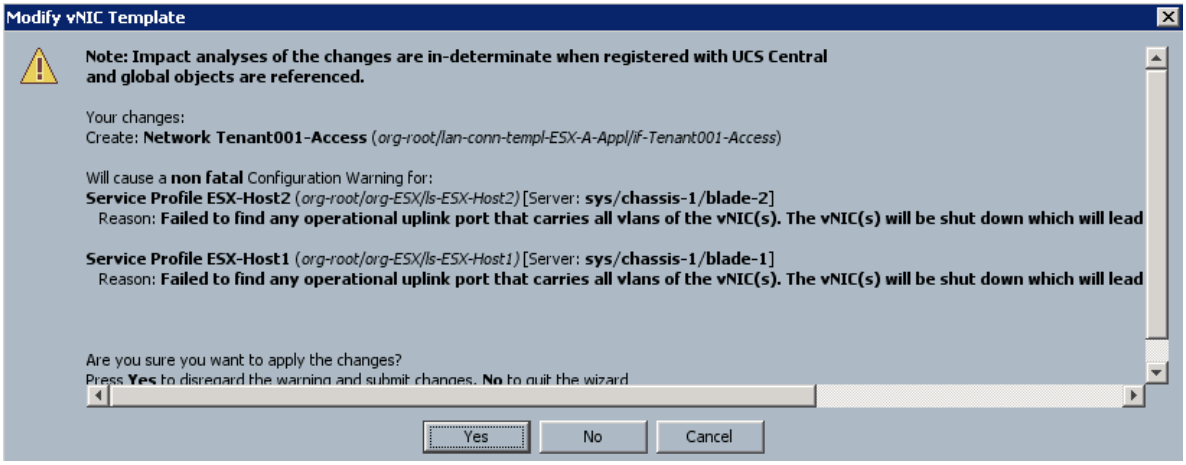



18. Select <<var_ucs_t001_access_vlan_name>>.

19. Click OK.




20. Click Yes.




21. Click OK

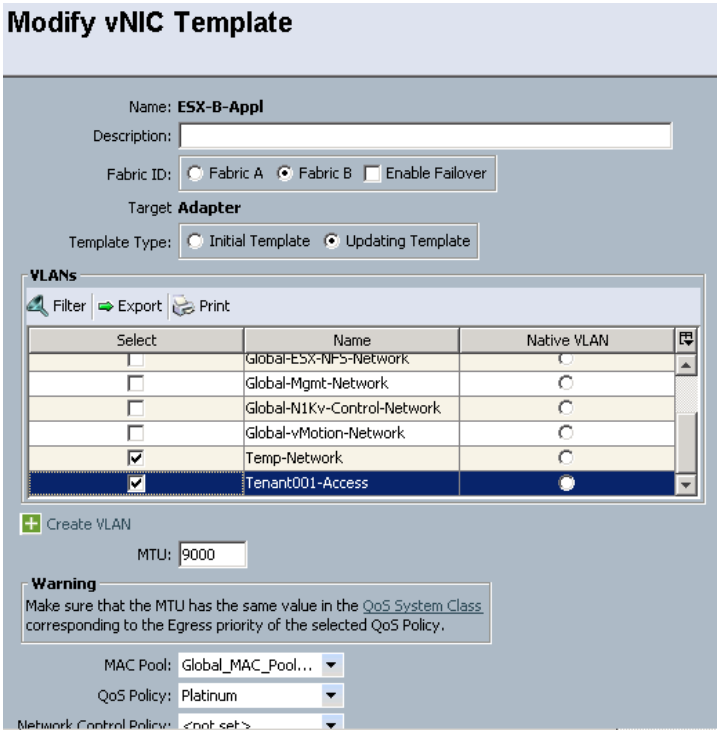
22. Select vNIC <<var_ucs_esx_b_appl_vnic_name>>.

23. Click the Info Icon 

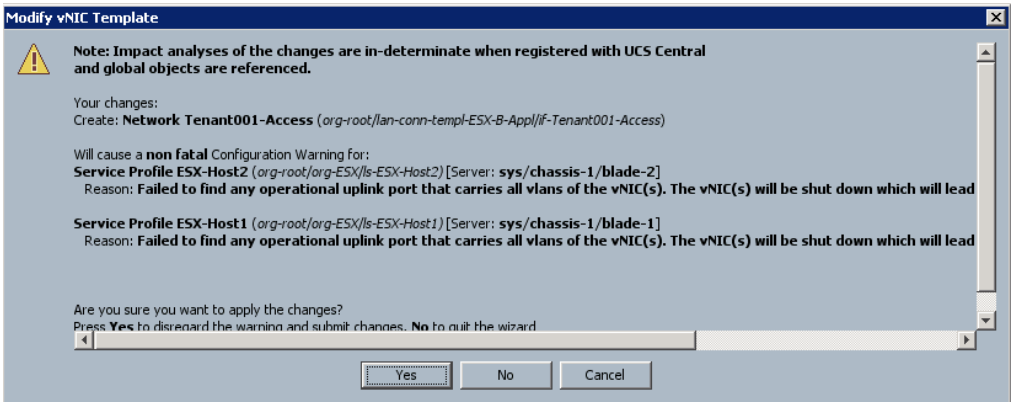
.

24. Select <<var_ucs_t001_access_vlan_name>>.

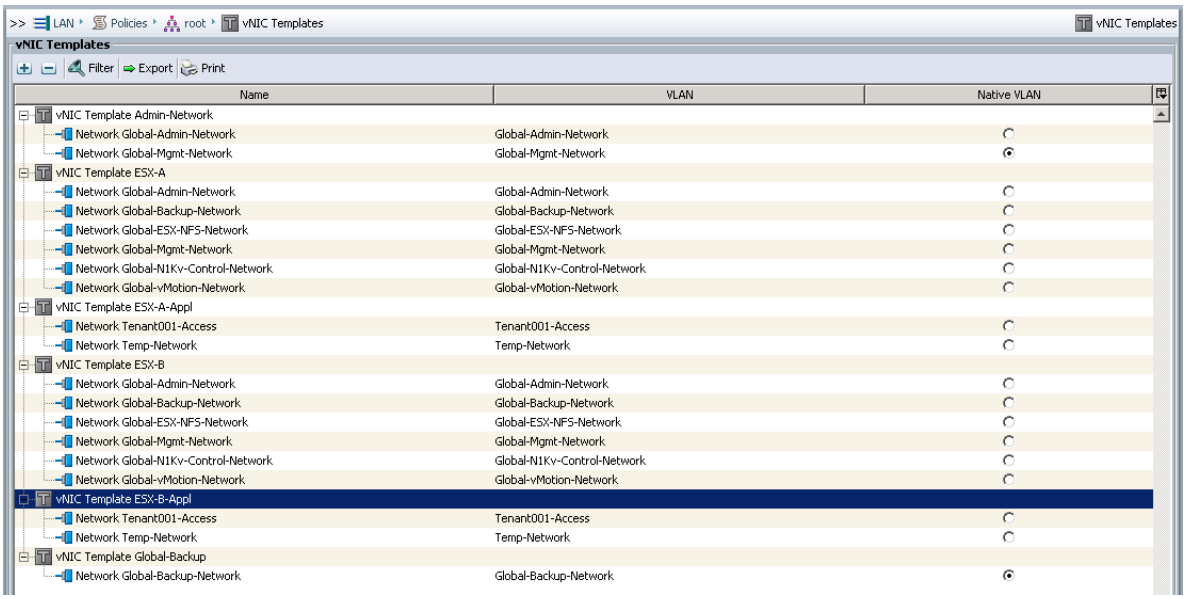
25. Click OK.




26. Click Yes.




27. Click OK.




## Create VLAN and Port-Profile on Cisco Nexus1000V

To create a VLAN and Port-Profile, complete the following steps:

1. Create VLAN:

```
vlan <<var_t001_access_vlan_id>>
 name <<var_ucs_t001_access_vlan_name>>
 no shut
 exit
```

2. Create Port-Profile for Tenant 001 access traffic:

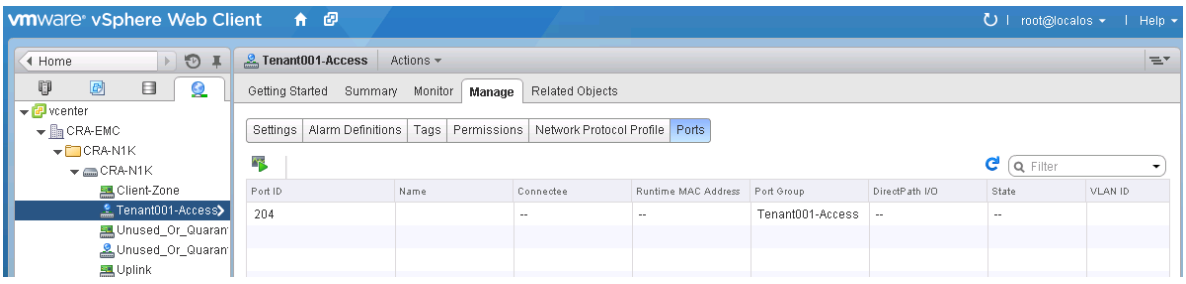
```
port-profile type vethernet <<var_ucs_t001_access_vlan_name>>
 vmware port-group
 switchport mode access
 switchport access vlan <<var_t001_access_vlan_id>>
 no shutdown
 port-binding static auto expand
state enabled
```

3. Validate Port-Profile on the Cisco Nexus1000V:

```
CRA-N1K(config)# show port-profile name <<var_ucs_t001_access_vlan_name>>


port-profile Tenant001-Access
```

```
type: Vethernet
description:
status: enabled
max-ports: 32
min-ports: 1
inherit:
config attributes:
 switchport mode access
 switchport access vlan 3001
 no shutdown
evaluated config attributes:
 switchport mode access
 switchport access vlan 3001
 no shutdown
assigned interfaces:
port-group: Tenant001-Access
system vlans: none
capability l3control: no
capability iscsi-multipath: no
capability vxlan: no
capability l3-vservice: no
port-profile role: none
port-binding: static auto expand
```




4. Add Access VLAN to the Client-Zone Port-Profile on the Cisco Nexus1000V:

```
port-profile type ethernet Client-Zone
switchport trunk allowed vlan add <<var_t001_access_vlan_id>>
no shutdown
exit
```

5. Validate Port-Profile on the Cisco Nexus1000V:

```
CRA-N1K(config)# show port-profile name Client-Zone

port-profile Client-Zone
 type: Ethernet
 description:
 status: enabled
 max-ports: 512
 min-ports: 1
 inherit:
 config attributes:
  mtu 9000
  switchport mode trunk
  switchport trunk allowed vlan 2,3001
  switchport trunk native vlan 2
  channel-group auto mode on mac-pinning
  no shutdown
 evaluated config attributes:
  mtu 9000
  switchport mode trunk
  switchport trunk allowed vlan 2,3001
  switchport trunk native vlan 2
  channel-group auto mode on mac-pinning
  no shutdown
 assigned interfaces:
  port-channel3
  port-channel4
```

```
 Ethernet3/2
 Ethernet3/4
 Ethernet4/2
 Ethernet4/4
port-group: Client-Zone
system vlans: none
capability l3control: no
capability iscsi-multipath: no
capability vxlan: no
capability l3-vservice: no
port-profile role: none
port-binding: static


CRA-N1K(config)#
```

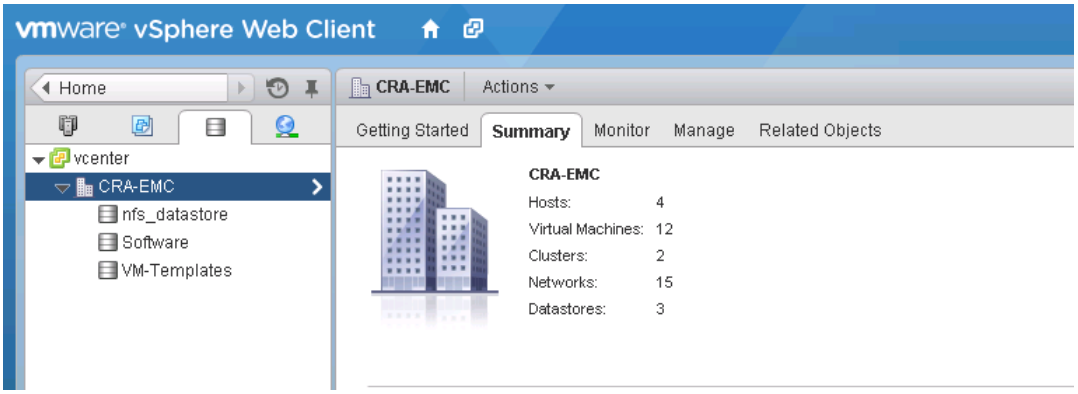
6. Save the running configuration as the startup-configuration:

```
copy run start
```

## Check Available VMware Datastore and Available Capacity

To create and check space on the VMware Datastore, complete the following steps:

1. Log in to the VMware vSphere Web Client and click the Storage Icon in the Home screen. Check the available datastores in the VMware data center you want to deploy in the new virtual machine.




With a new deployment, the list of existing datastores is short. In this solution, there are three defined datastores. The datastore nfs_datastore is the main datastore in the management PoD. The software

datastore hosts the ISO files and installation sources. The VM-Templates datastore hosts the virtual machine templates.

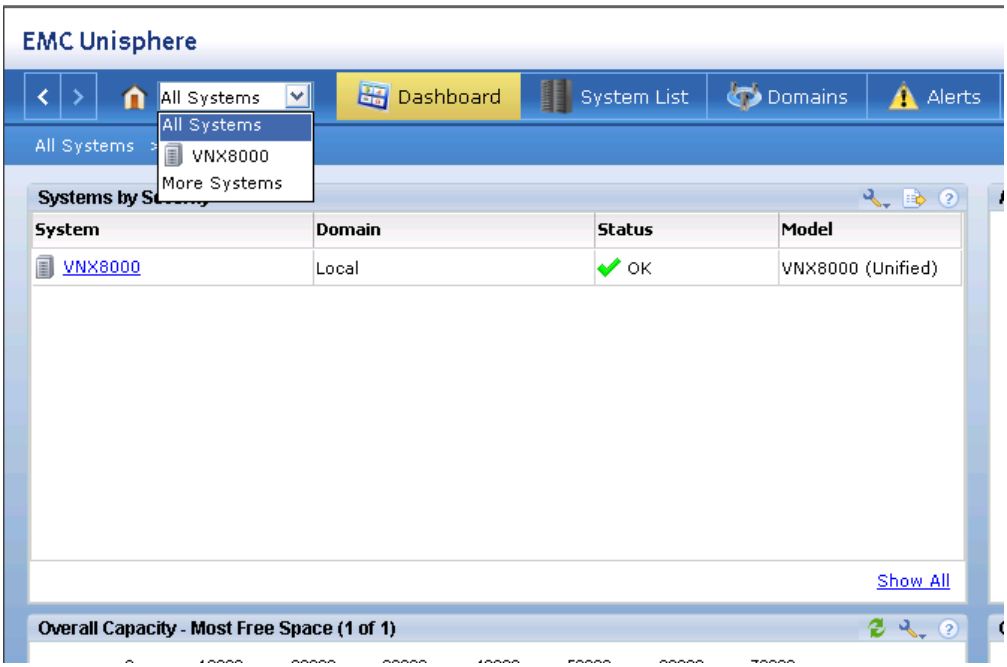
## Create a New Datastore

### Configure Storage Pool for SAP HANA Applications

To create a storage pool and carve LUNs for the datastore, complete the following steps:

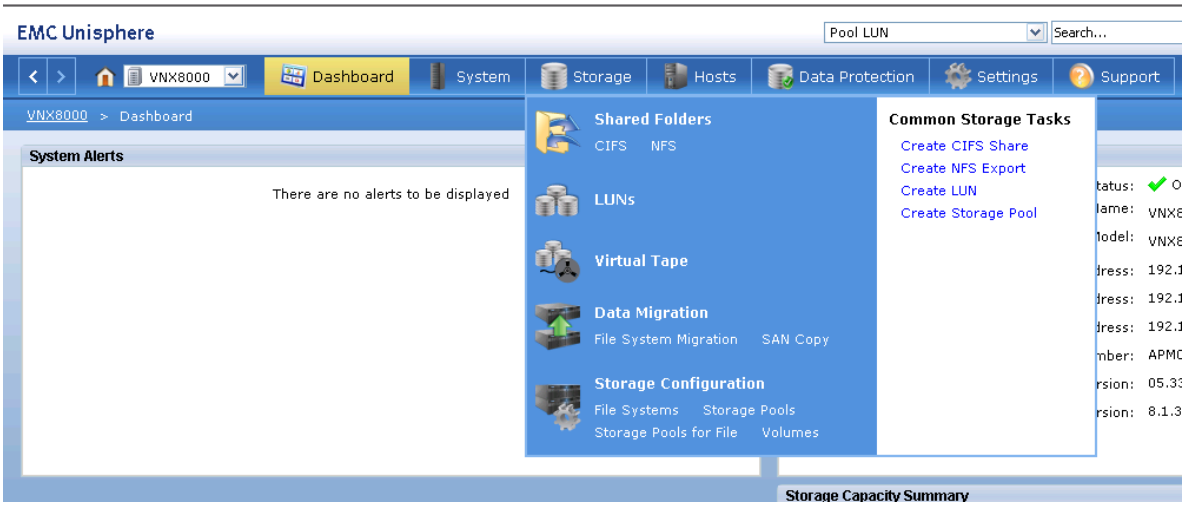
1. Open a Web Browser and connect to EMC VNX Unisphere.

2. From the drop-down menu select the VNX <<var_vnx1_name>>.

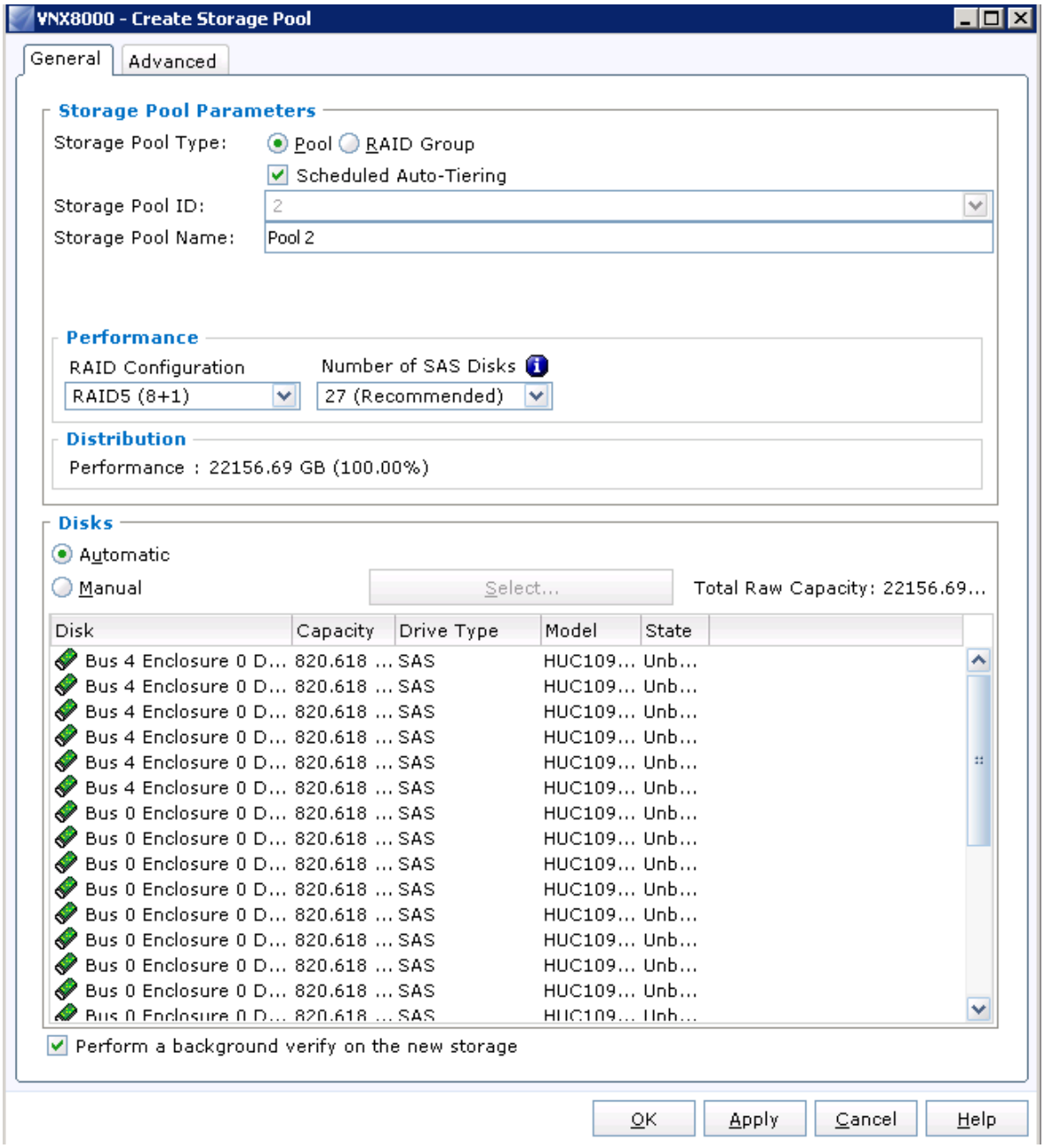



3. Click the Storage.

4. Select Storage Configuration > Storage Pools.

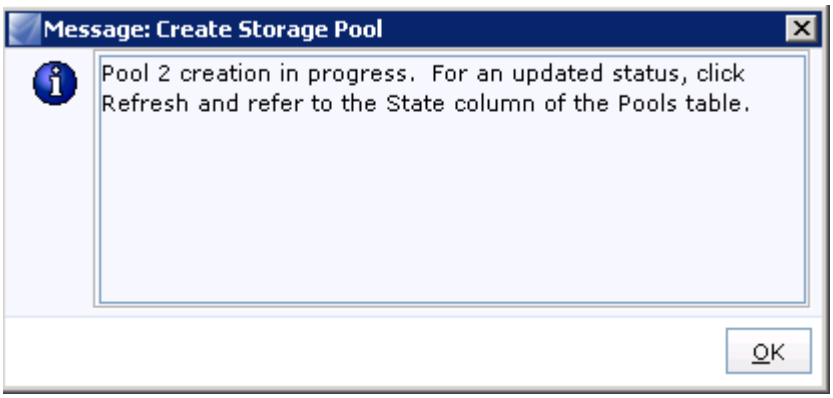


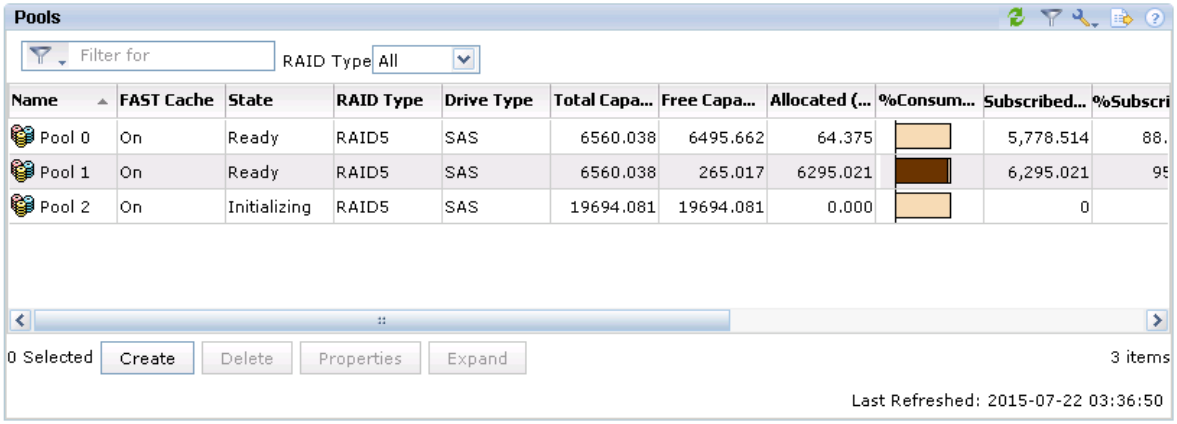

5. Click Create.
6. Keep Pool selected as the Storage Pool Type.
7. Enter <<var_vnx1_hana-pool1_name>> as the Storage Pool Name.
8. Choose RAID5 (8 + 1) as the RAID Configuration.
9. Choose 27 as the minimum Number of SAS Disks for a SAP HANA workload.
10. In the Disks Section keep Automatic selected, the Configuration wizard will select the SAS disks to create the storage pool.
11. Click OK.
12. Click Yes to Initiate the Pool creation.




13. Click Yes to accept the Auto-Tiering Warning.

14. Click OK.



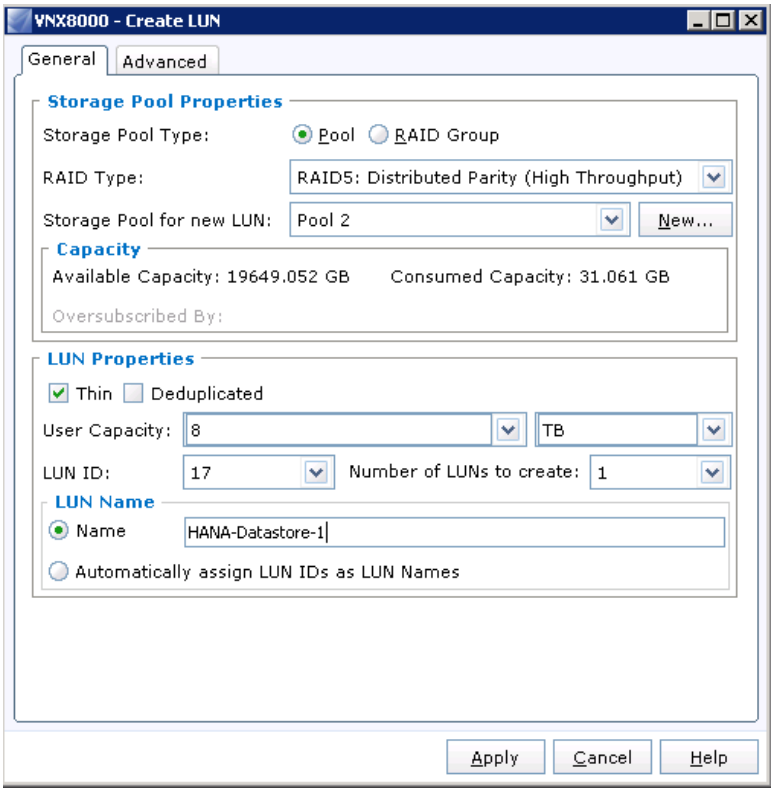




## Configure LUN for VMware Datastore for SAP HANA

To store the persistence of SAP HANA, using VMDKs is recommended. The VMDKs are stored on a datastore mapped to a LUN on the EMC VNX Storage. The following steps guide you through creating the LUN on the EMC VNX and mapping to the Storage-Pool so the VMware ESX hosts can access the LUN. To configure the LUN for the VMware Datastore, complete the following steps:

1. Right-click the created Storage Pool.
2. Click Create LUN.
3. As User Capacity enter 8 and select TB from the drop-down menu.
4. Select the Radio button for Name.
5. Enter HANA-Datastore-1 as the Name.
6. Click Apply.
7. Click Yes.
8. Click OK.

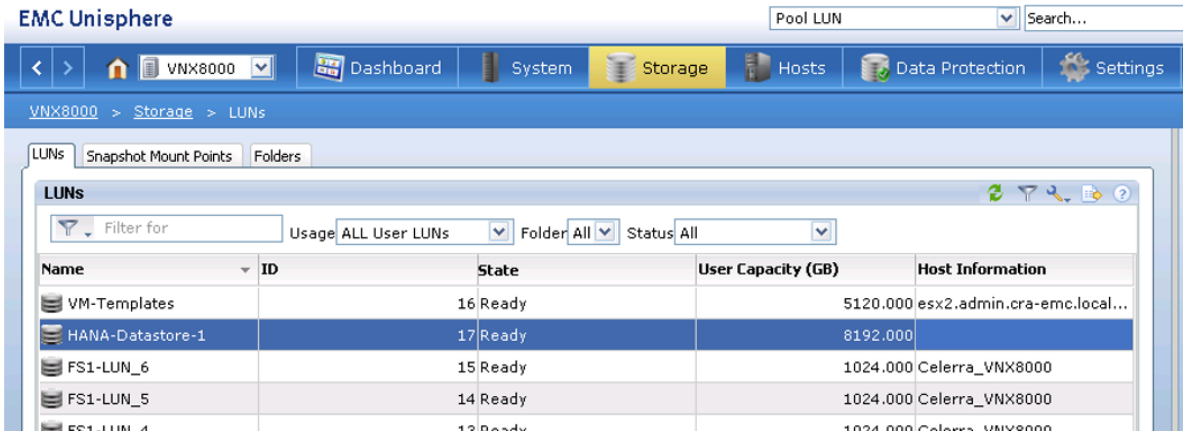
9. Click Cancel.




## Configure Storage Groups

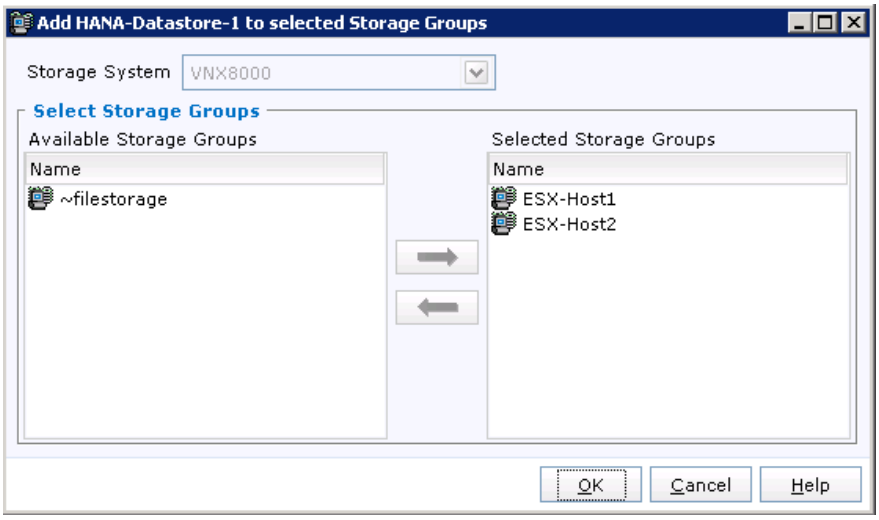
When the hosts as well as the LUNs are created on the VNX storage array, you will need to create storage groups to assign access to LUNs for various hosts. Boot LUN is dedicated to a specific server. To configure storage groups, complete the following steps:

1. Click Storage in EMC VNX Unisphere GUI.
2. Select LUNs > HANA-Datastore-1.
3. Click Add to Storage Group.

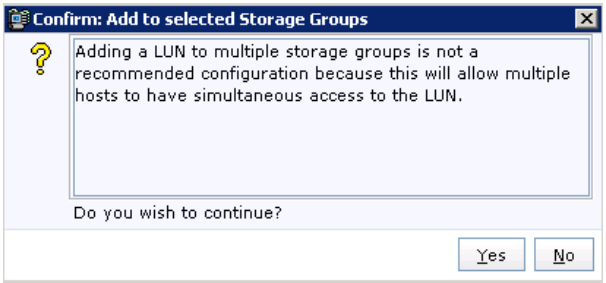



4. Select the Storage Groups ESX-HostX and click the → sign.

5. Click OK.



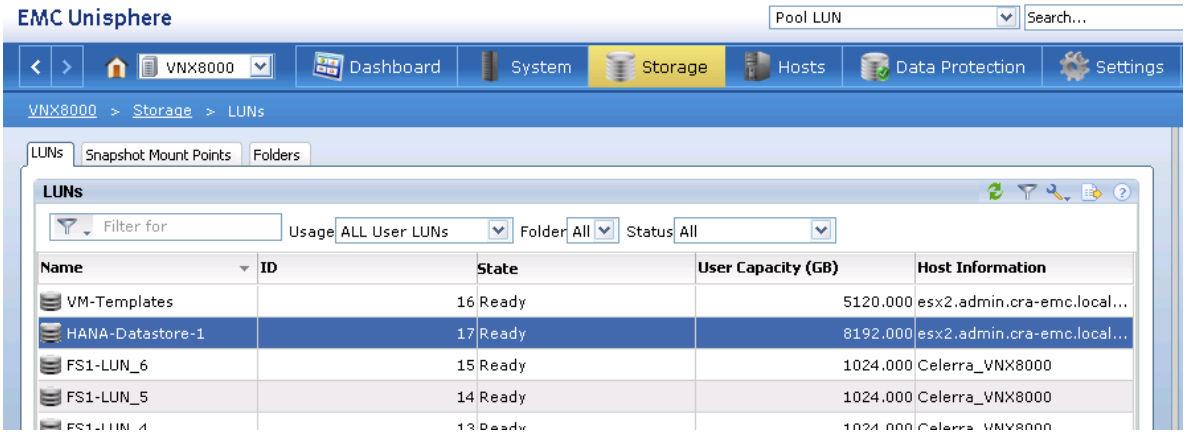

6. In a VMware ESX cluster, the default is having a LUN accessible from multiple hosts simultaneously. Click Yes.




7. Click Yes.

8. Click OK.

9. All Hosts with access are listed in the Host Information field.

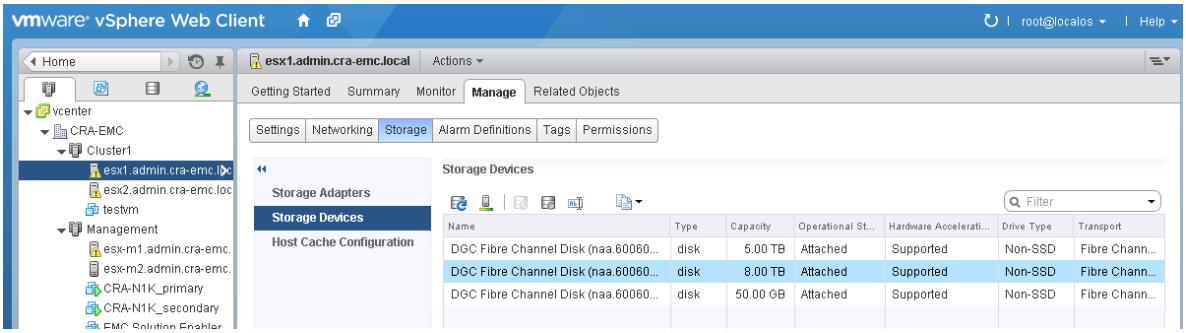



## Configure Datastore in VMware vSphere Web Client

To configure the datastore in VMware vSphere web client, complete the following steps:

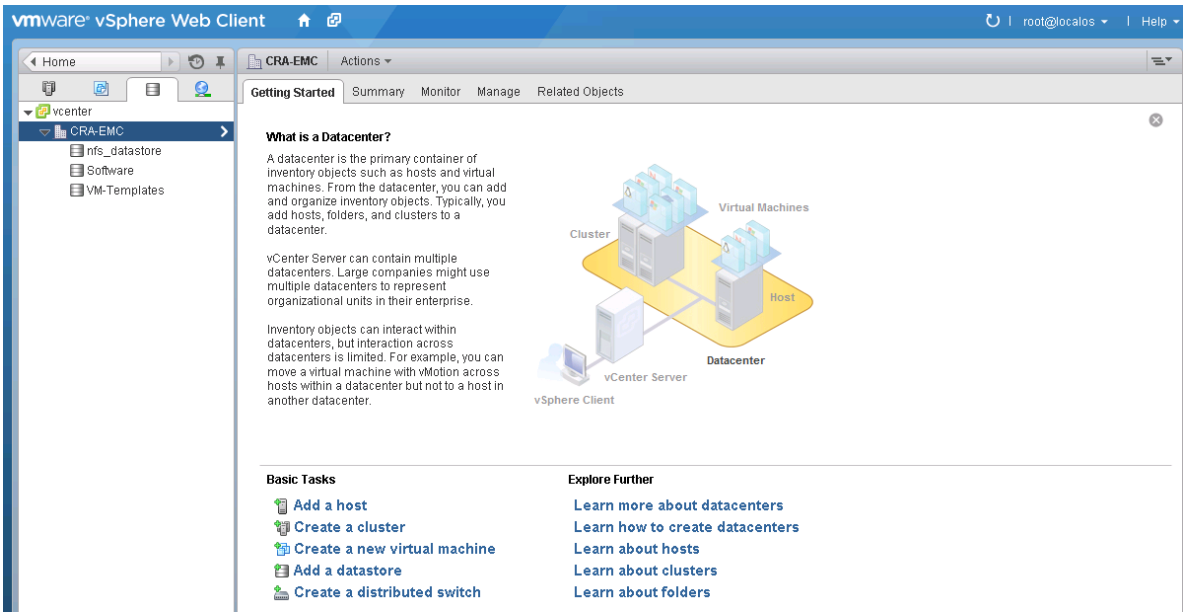
1. Log in to the VMware vSphere Web Client and click the Hosts and Clusters Icon in the Home screen.

2. Select one of the ESX-Hosts, in the right pane and select Manage Tab > Storage > Storage Devices. Check the available disk devices for this host. The recently created 18TB LUN are visible.

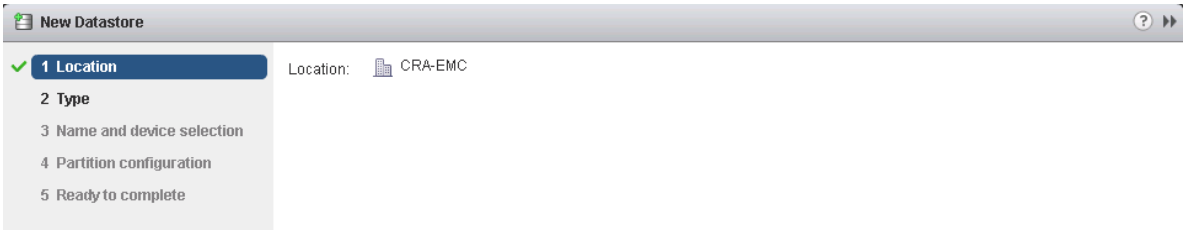



3. In the vSphere Web Client Home screen click Storage.

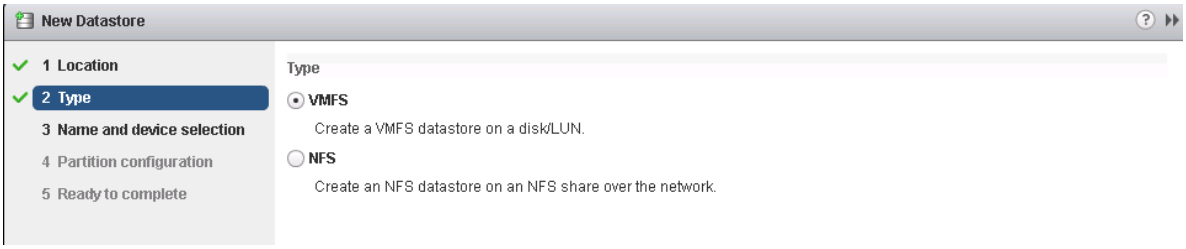
4. In the right pane click Getting Started > Add a Datastore.



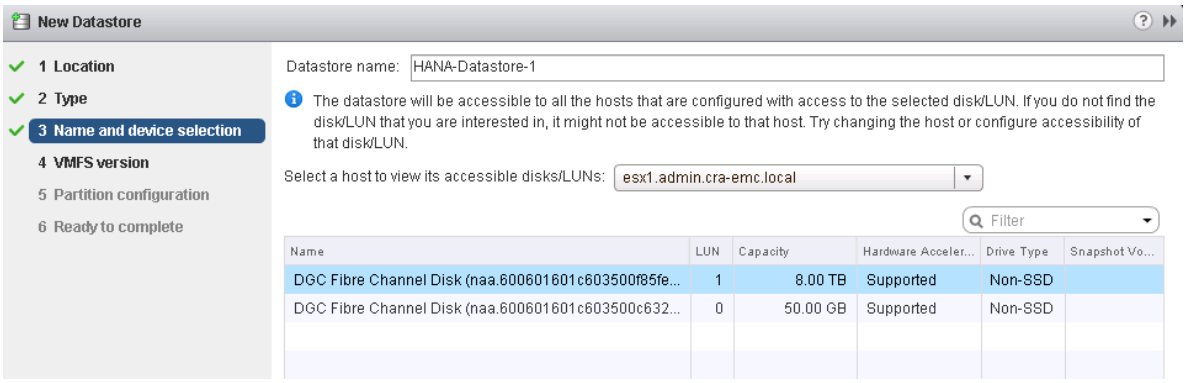

5. Click Next.



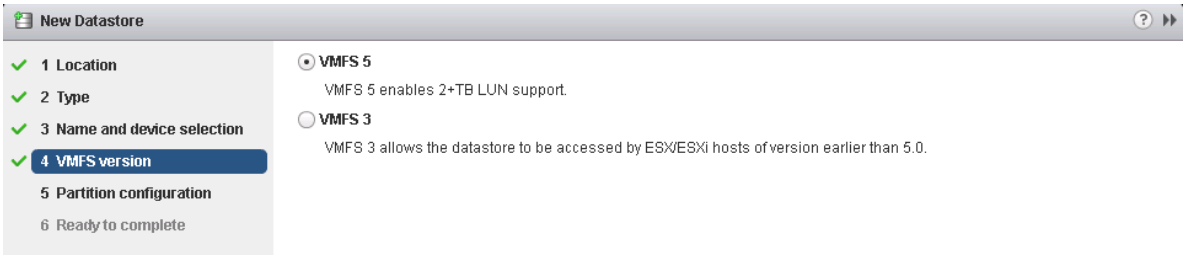

6. Select Type VMFS, click Next.




7. Enter <<var_vnx_hana_datastore1>> for the Name.
8. Select <<var_esx1_fqdn>>.
9. Select the created LUN, with the 8TB.
10. Click Next.

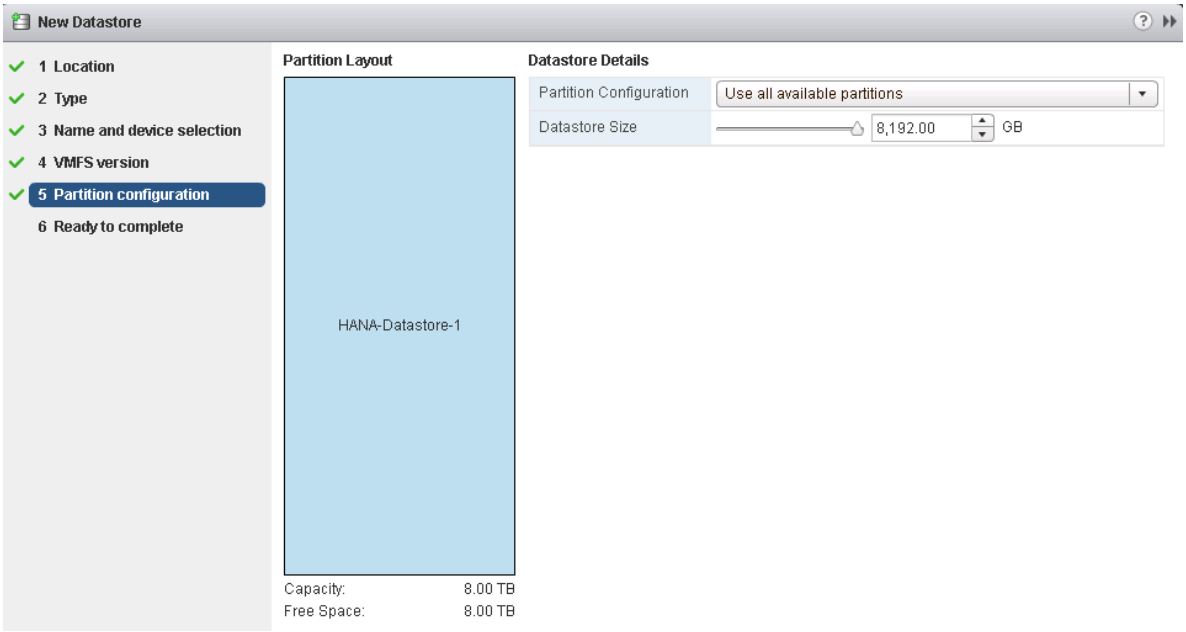



11. Select VMFS5, click Next.

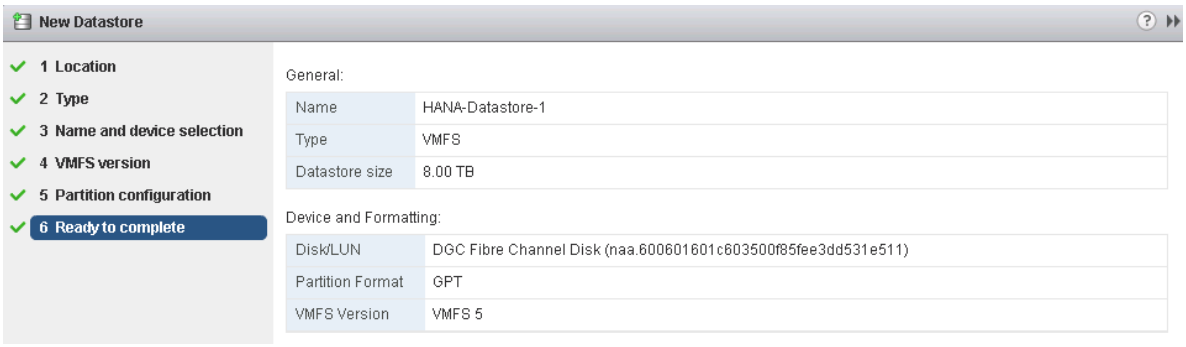



12. Select Use all available partitions and all capacity for the Datastore Size.

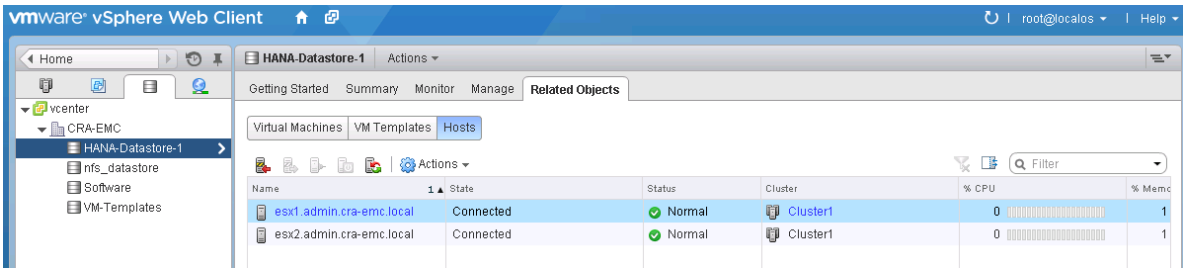
13. Click Next.




14. Review the Information, click Finish.




15. After the creation task finished, click the <<var_vnx_hana_datastore1>> > Related Objects > Hosts.

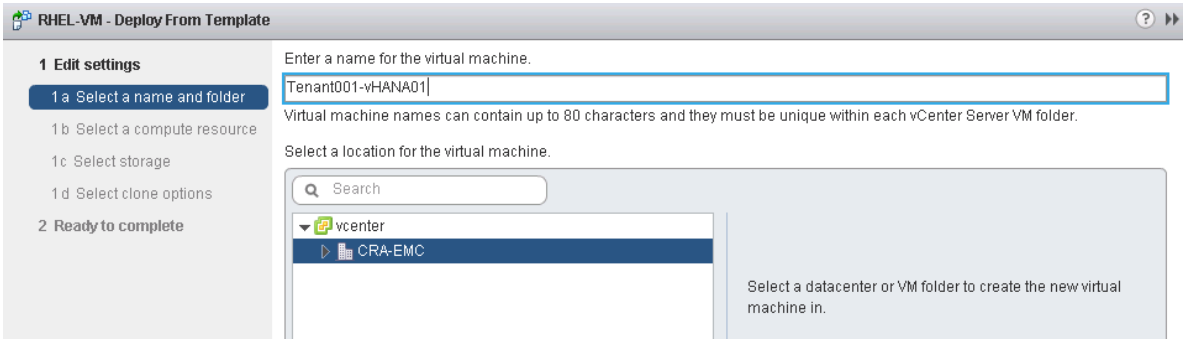



All hosts in the Cluster with access to the LUN are listed.

## Create Virtual Machine from VM-Template

To create a virtual machine from the VM-Template, complete the following steps:

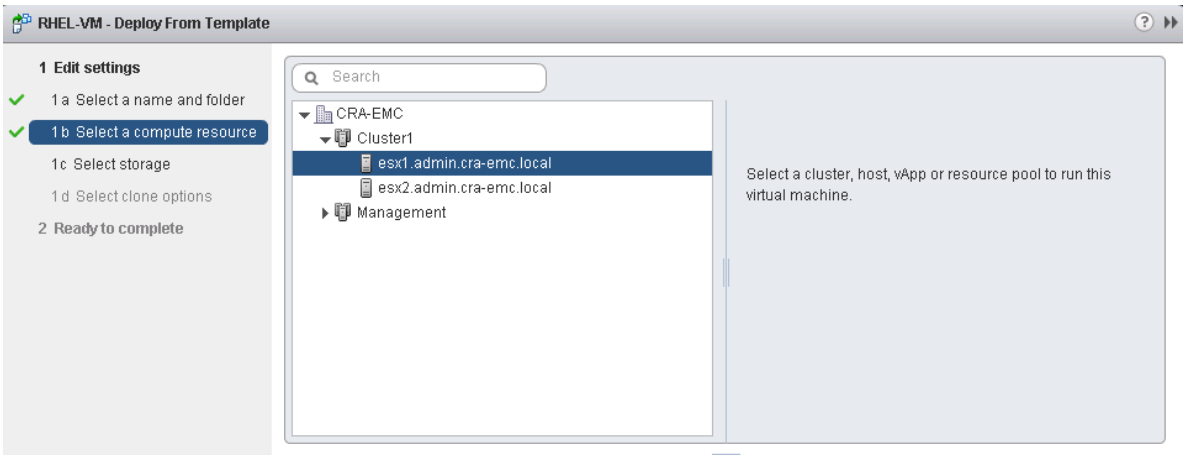
1. Open a web browser on the management workstation and navigate to the vCenter Server management IP address <<var_vc_ip_addr>>.
2. Logon as root and the password <<var_mgmt_passwd>>.
3. Click VMs and Templates in the Home Screen.
4. Select the <<var_vc_rhel_template>>.
5. From the Getting Started Screen, select Deploy to a new virtual machine.
6. Enter <<var_vc_t001_vm01_name>> as the Name of the virtual machine.
7. Click Next.




8. Select <<var_vc_cluster1_name>> or a ESXi host in this cluster.

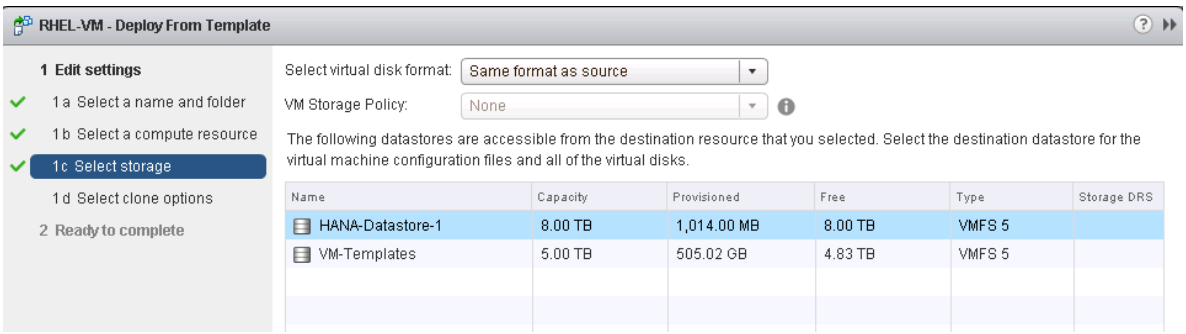
Make sure that at least one host of the Cluster or the specific host you have selected has the required free memory for this virtual machine. Since this is an example, memory size of 256GB for this virtual machine cannot run on the Cisco UCS B200 or Cisco UCS C220 in this setup since those servers only have 256GB main memory installed.

9. Click Next.

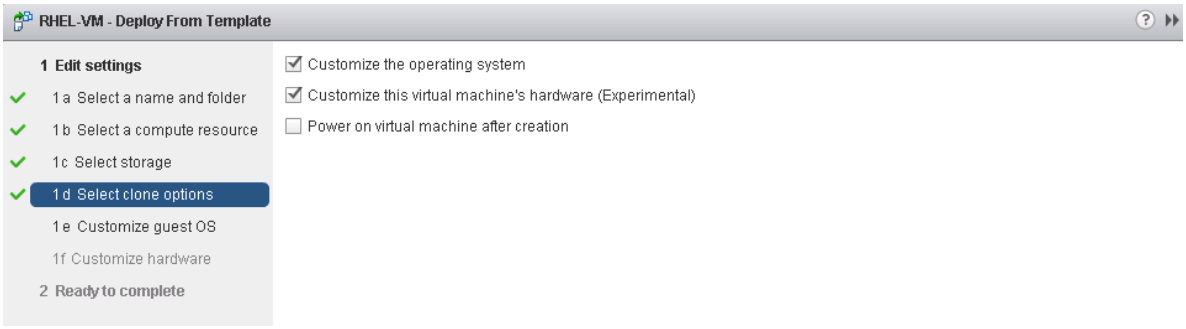



10. Select <<var_vnx_hana_datastore1>>.

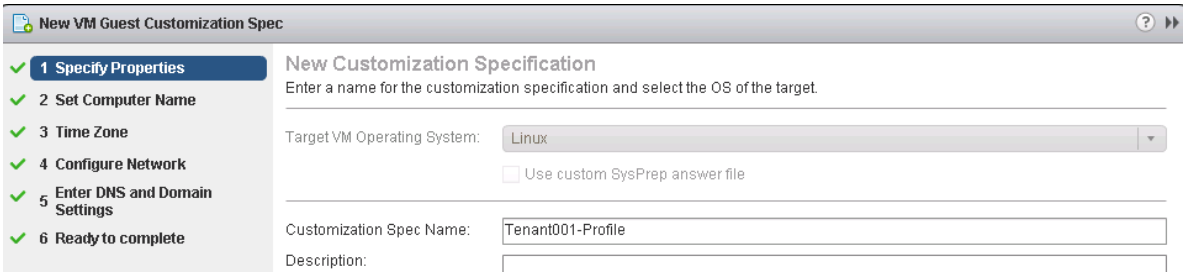
11. Click Next.



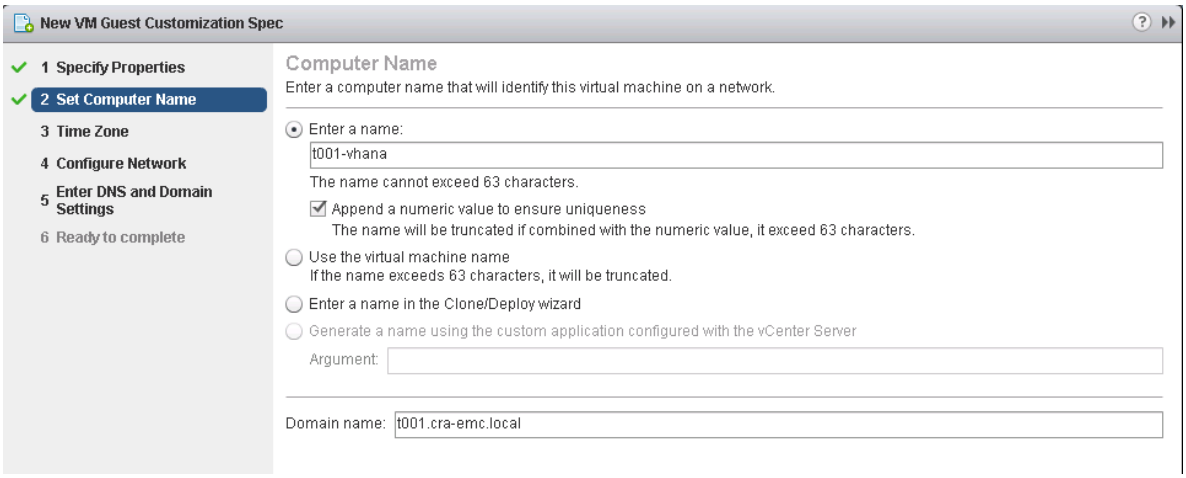
12. Select Customize the operating system.
13. Select Customize the virtual machine's hardware.
14. Click Next.




15. Click the sign.
16. Enter <<var_vc_t001_profile_name>> as the Customization Spec Name.
17. Click Next.

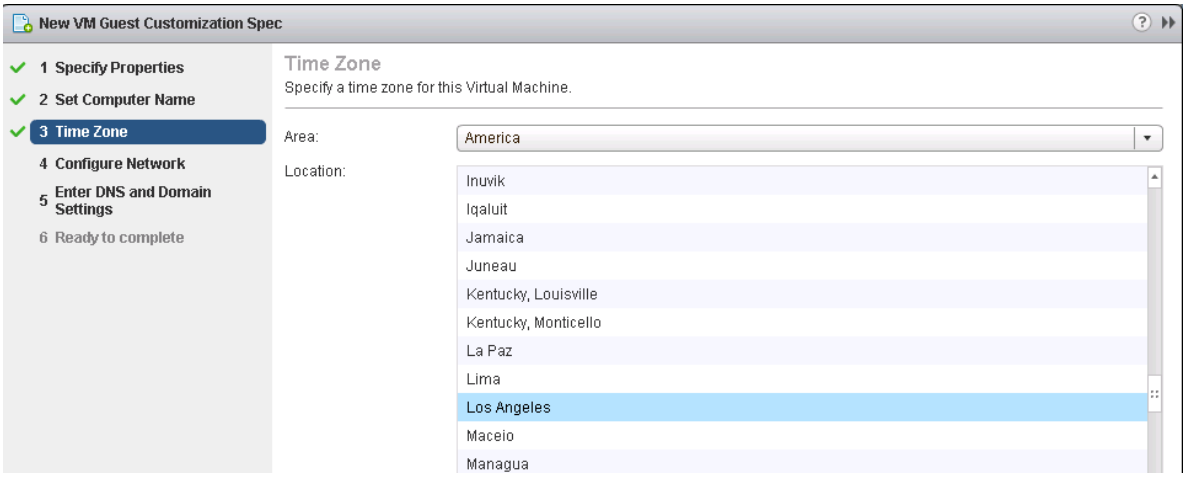



18. Enter <<var_vc_t001_hostname_prefix>> for the name.
19. Click the checkbox for Append a numeric value to ensure uniqueness.
20. Enter <<var_t001_domain>> for the Domain name for this virtual machine / tenant.
21. Click Next.



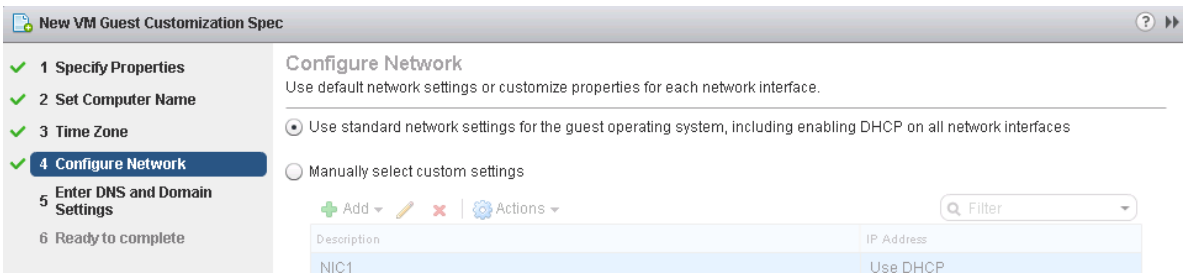

22. Select the time zone for this virtual machine / tenant.

23. Click Next.




24. Keep Use standard network settings for ... selected.

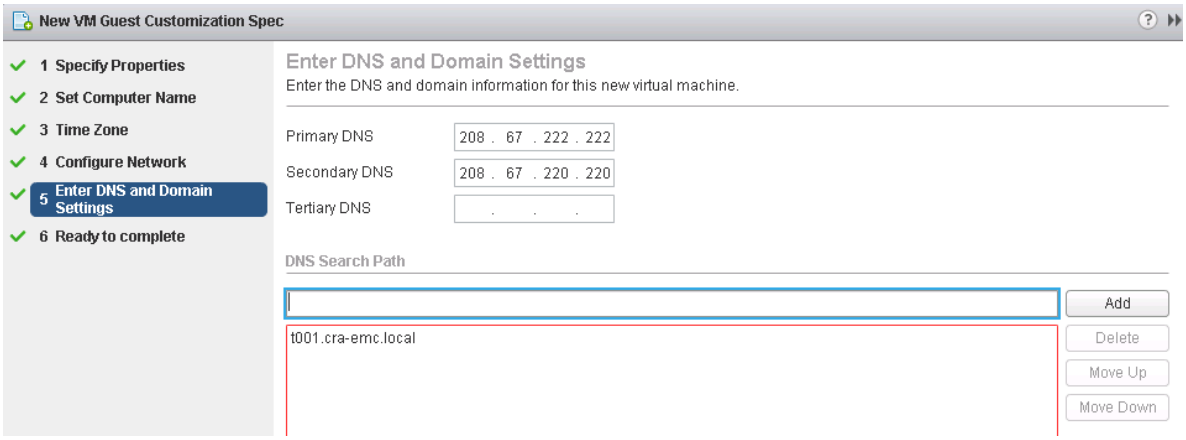
25. Click Next.




26. Enter the Tenant specific Primary DNS and Secondary DNS, <<var_t001_ns1>> and <<var_t001_ns2>>. This should be the same DNS as the client systems using accessing this SAP HANA system.

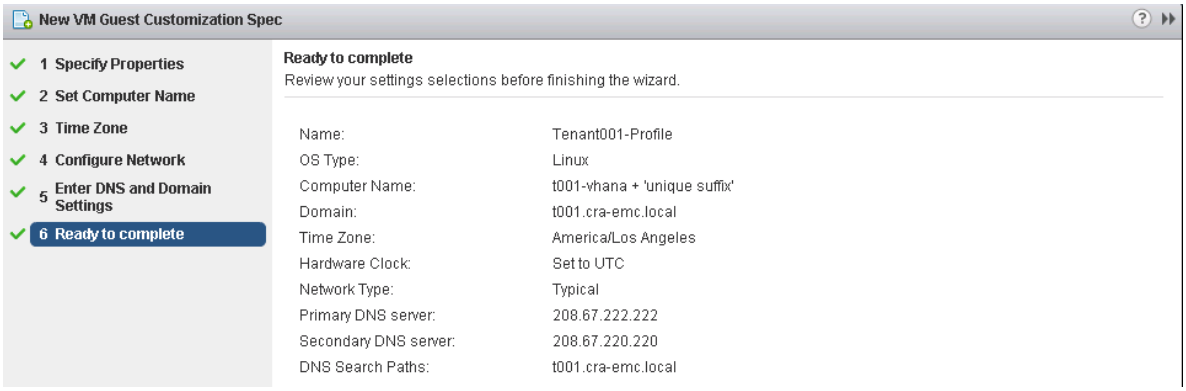
27. Enter a DNS Search Path that fits best for this SAP HANA system.

28. Click Next.



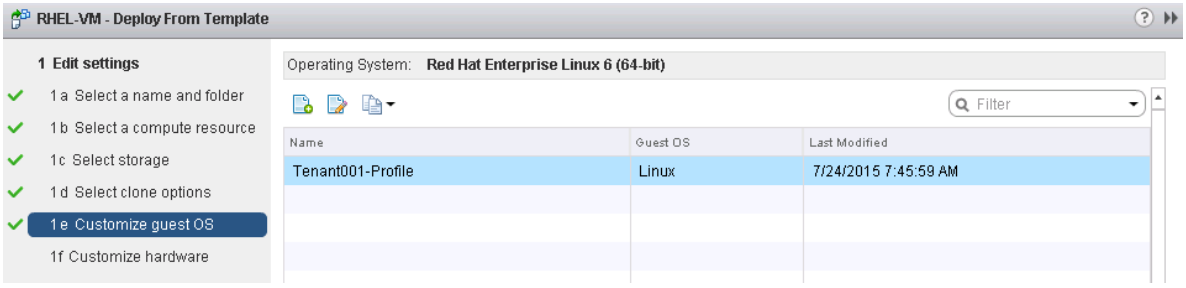

29. Review the settings.

30. Click Finish.




31. Select the Customization profile <<var_vc_t001_profile_name>>.

32. Click Next.



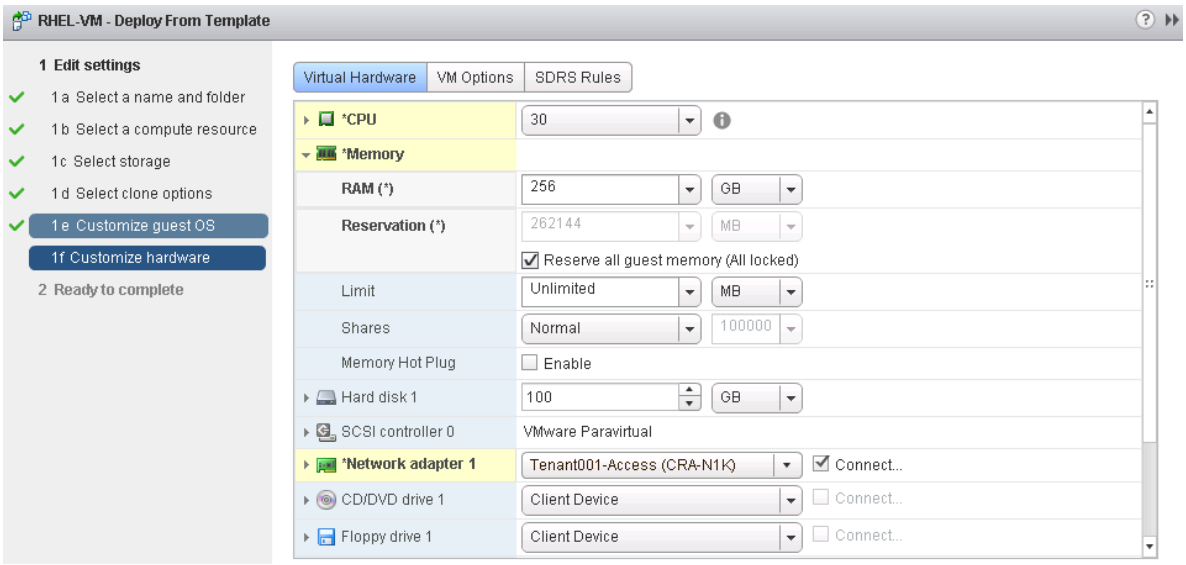

33. Select 30 for the number of CPUs.

34. Change the Memory to 256 and select GB as the unit.

35. Click the Icon left of Memory.

36. Click the checkbox for Reserve all guest memory (All locked).

37. Select <<var_ucs_t001_access_vlan_name>> for Network Adapter 1.




38. Select New Hard Disk from the New Device drop-down menu.

39. Click Add.

40. Enter 256 GB as the Size.

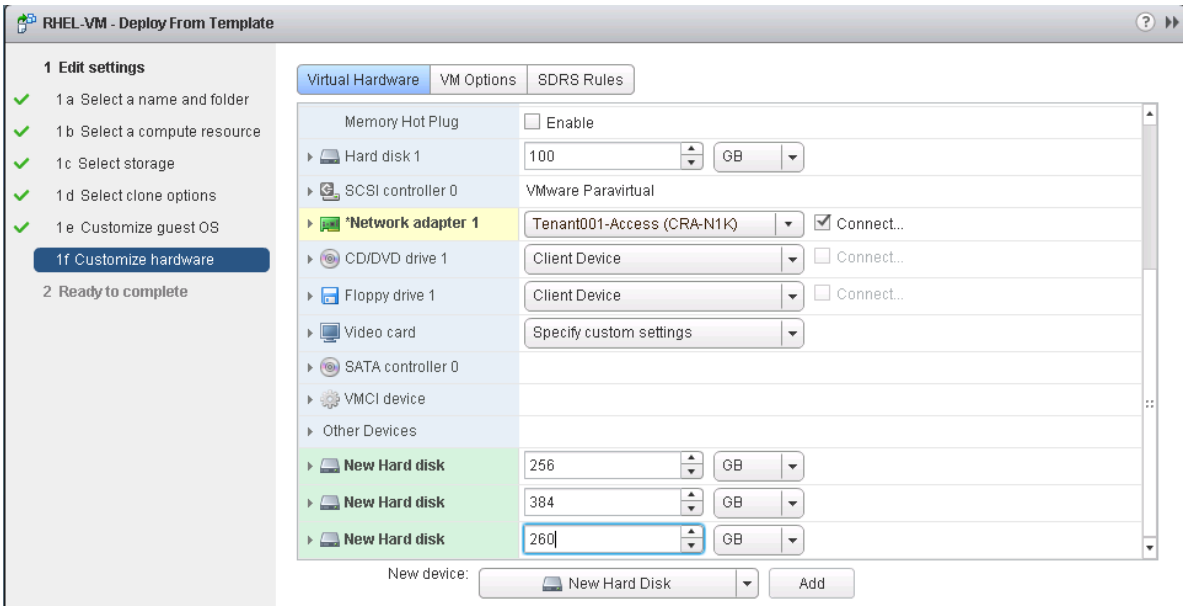
41. Click Add.

42. Enter 384 GB as the Size.

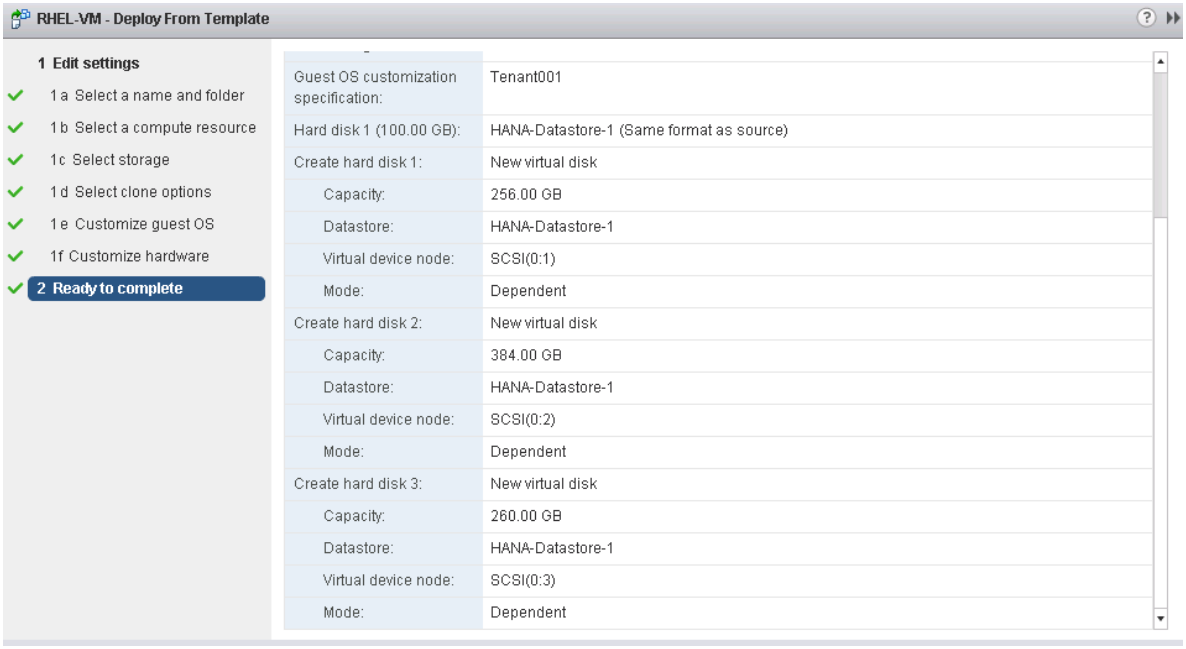
43. Click Add.

44. Enter 260 GB as the Size (this is to identify this as the /hana/shared disk).

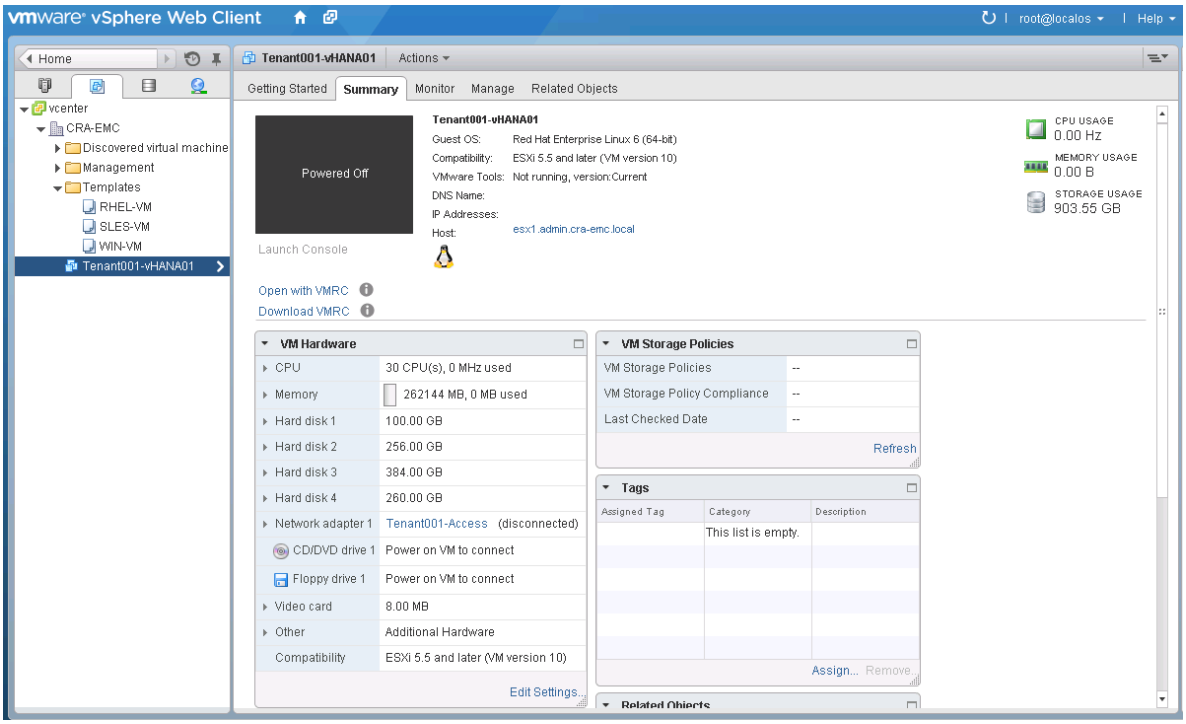
45. Click Next.




46. Review the Information and click Finish.




47. When the deployment is finished, the Virtual Machine summary will look like the screen shot below:

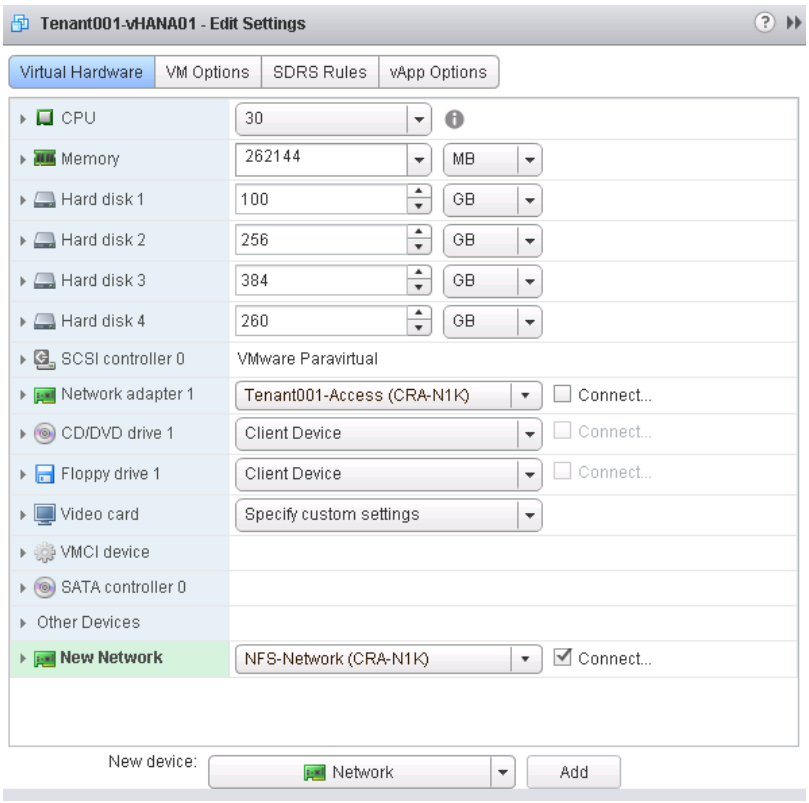



48. Click Edit Settings.

49. Select Network from the New Device drop-down menu and click Add.

50. Select NFS-Network for the destination network.

51. Click OK.




52. Power on the virtual machine.

53. Launch Console.

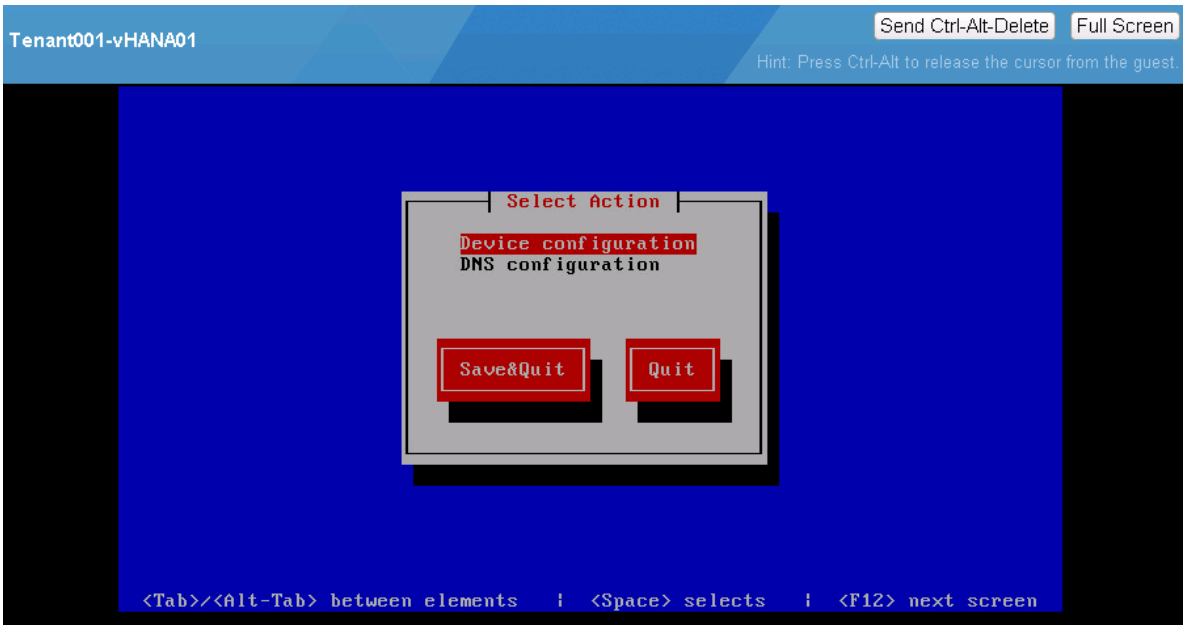
54. The operating system is defined as not configured.

55. Enter <<var_mgmt_passwd>> or the tenant specific password as new password.



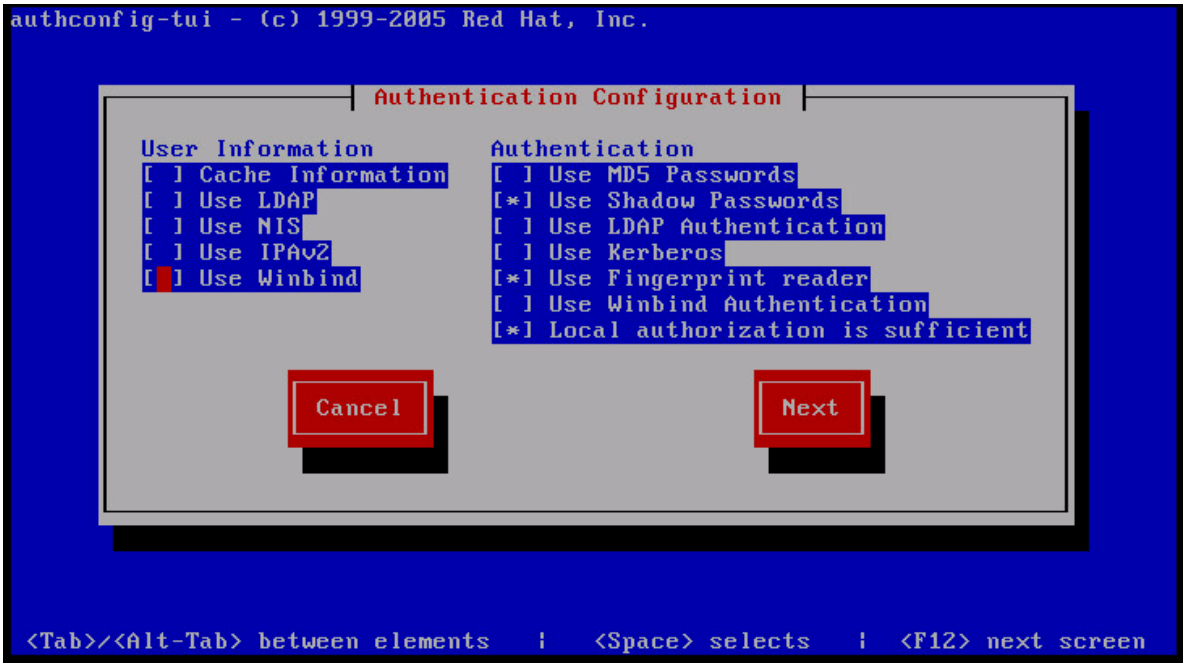

56. Skip the Network Device configuration since this is a part of the VMware customization wizard settings.

57. Select Quit and press Enter.



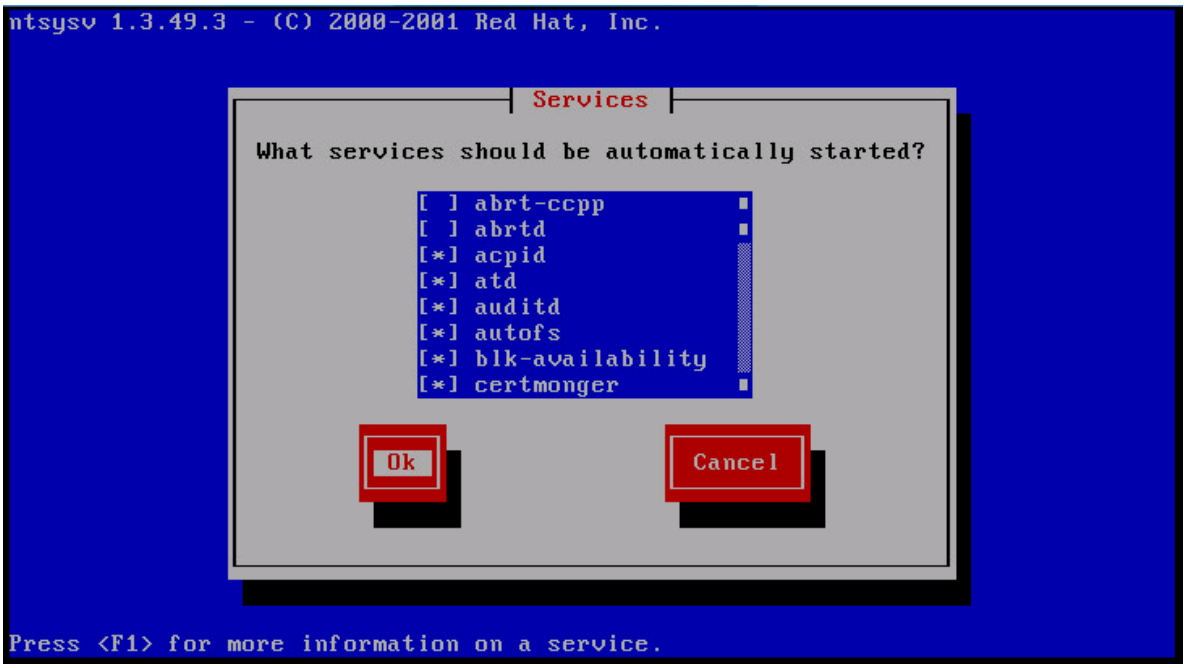

58. Select Tenant specific Authentication options.

59. Select Next and press Enter.

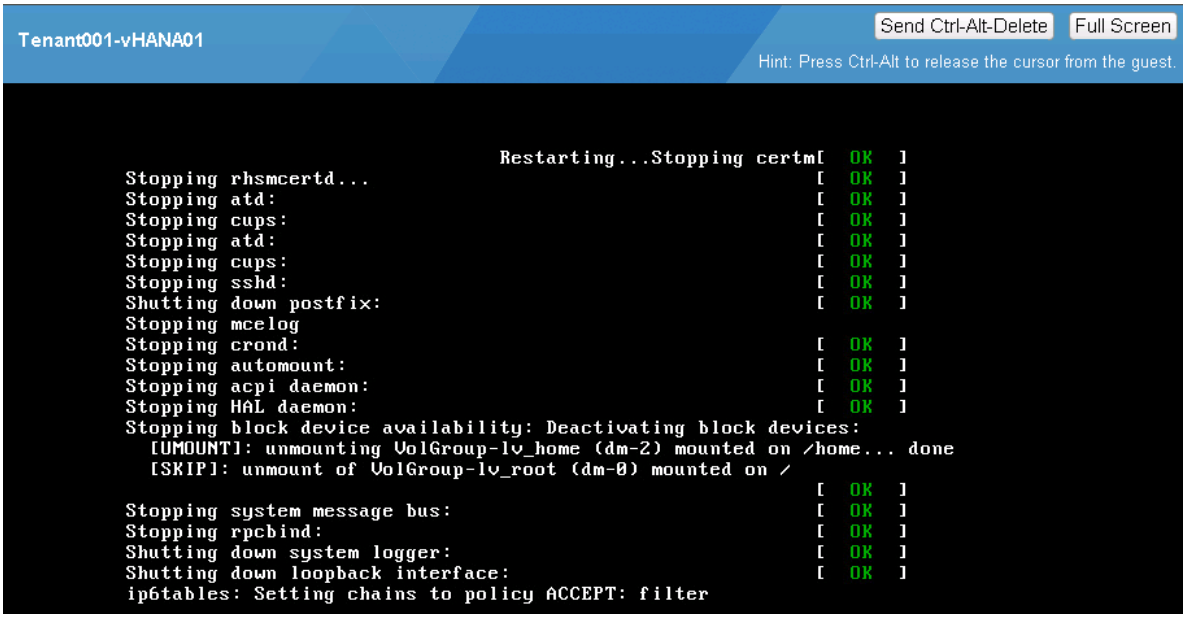



60. Define the services the system has to start automatically based on your data center best practices.

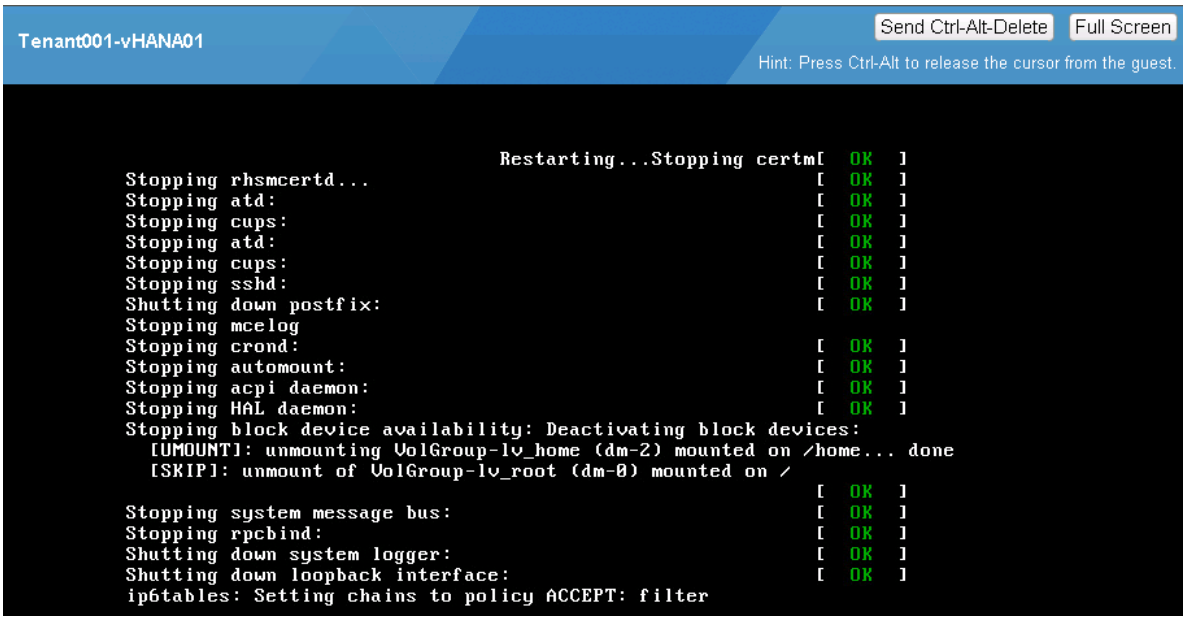
61. Select OK and press Enter.




62. The system will automatically reboot to apply the settings from the VMware customization wizard.




63. The system is ready for the next steps after the restart is done.




## Configure IP Addresses

If required to configure the IP addresses on the installed operating system manually, logon to the system and adopt the required settings in the /etc/sysconfig/network-scripts/ifcfg-ethX files.

```
DEVICE=eth0

BOOTPROTO=none

ONBOOT=yes

NETMASK=<<var_t001_access_mask>>

IPADDR=<<var_t001_vhana1_access_ip>>

USERCTL=no
```

## Configure Storage for SAP HANA

To configure the storage for SAP HANA, complete the following steps:

1. Log in to the operating system through the VMware Console or SSH over the network.
2. Create the Filesystems on the new disks:

```
mkfs -t xfs /dev/sdb

mkfs -t xfs /dev/sdc

/dev/sdd is entire device, not just one partition!

Proceed anyway

mkfs /dev/sdd
```

3. Create the directory structure for SAP HANA:

```
mkdir –p /hana/shared
mkdir /hana/log
mkdir /hana/data
```

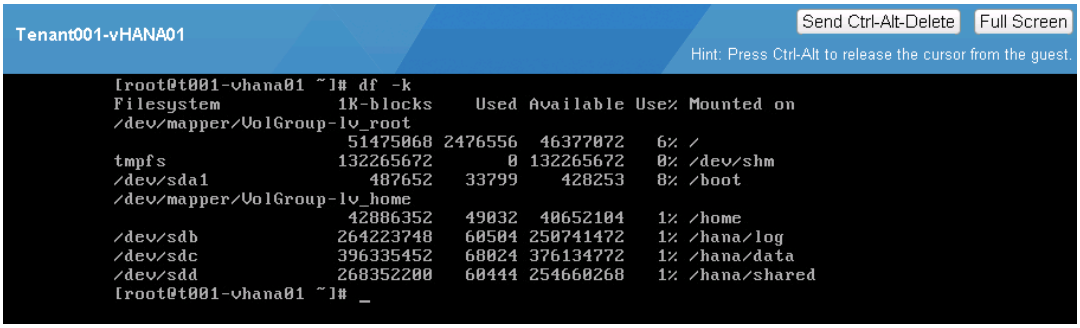
4. Add the new file systems into the /etc/fstab file:

```
echo "/dev/sdb    /hana/log   xfs   defaults    1 2" >> /etc/fstab
echo "/dev/sdc    /hana/data  xfs   defaults    1 2" >> /etc/fstab
echo "/dev/sdd    /hana/shares      ext4  defaults    1 2" >> /etc/fstab
```

5. Mount the File systems to the specific SAP HANA directories:

```
mount /hana/log
mount /hana/data
mount /hana/shared
```

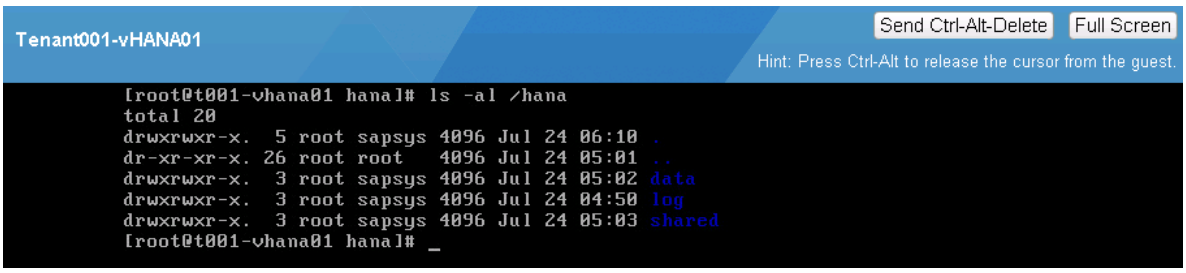
6. Make sure the filesystems are mounted and the sizes are available.




7. Change the permissions for the SAP HANA file systems:

```
chgrp –R sapsys /hana
chmod –R 775 /hana
```

8. Check the permissions.



## Install SAP HANA

To install SAP HANA, complete the following steps:

1. Mount the Software share to access the SAP HANA installation files

```
mkdir /software
mount 172.30.113.11:/FS_Software /software
```

Please use the SAP HANA Installation Guide provided by SAP for the software revision you plan to install. The program to install SAP HANA Revision 100 is hdblcm located in the directory <Installation source>/DATA_UNITS/HDB_LCM_LINUX_X86_64.

```
cd /software/SAP/SPS10/REV100/DATA_UNITS/HDB_LCM_LINUX_X86_64
./hdblcm
```

2. The text based installation menu is launching

```
Select 1 for Install new system

Select 2 for All Components

Enter Installation Path: /hana/shared : Press Enter
Enter local host name: t001-vhana-0: Press Enter
Do you want to add additional hosts to the system? N
Enter SAP HANA System ID: <<var_t001_hana_sid>>
Enter Instance Number:  <<var_t001_hana_nr>>
Select Database mode 1 for single_container
Select System Type: 2 for Test
Enter Location for Data Volumes /hana/data/T01: Press Enter
Enter Location for Log Volumes /hana/log/T01: Press Enter
Restrict maximum memory allocation n : Press Enter
Enter Certificate Host name t001-vhana-0 : Press Enter
Enter SAP Host Agent User (sapadm) password: <<var_mgmt_passwd>>
Confirm password
```

```
Enter System Administrator (t01adm) password: <<var_mgmt_passwd>>
Confirm password
Enter System Administrator Home Directory /usr/sap/T01/home : Press Enter
Enter System Administrator Login shell /bin/sh: Press Enter
Enter System Administrator User id 1000 : Press Enter
Enter Database User (SYSTEM) Password : <<var_t001_hana_sys_passwd>>
Confirm Passwd
Restart instance after machine reboot n : Press Enter
Do you want to continue : y
```

```
  Preparing package 'Studio Director'...
  Preparing package 'Client Installer'...
  Installing SAP HANA Studio to /hana/shared/T01/hdbstudio...
  Installing package 'Studio Director'...
  Installing package 'Client Installer'...
  Installing SAP HANA Studio Update repository...
    hdbupdrep: Importing delivery units...
    hdbupdrep: Importing delivery unit HANA_STUDIO_T01
Installing SAP HANA Smart Data Access...
  Removing old driver files from /hana/shared/T01/federation ...
Creating Component List...
  Registering SAP HANA Studio...
    Registering SAP HANA Database Client...
      Regenerating SSL certificates...
      Deploying SAP Host Agent configurations...
SAP HANA system installed

Note: Deployment of SAP Host Agent configurations finished with errors

You can send feedback to SAP with this form: https://t001-vhana-0:1129/lmsl/HDBL
CM/T01/feedback/feedback.html
Log file written to '/var/tmp/hdb_T01_hdblcm_install_2015-07-27_00.58.39/hdblcm.
log' on host 't001-vhana-0'.
You have new mail in /var/spool/mail/root
[root@t001-vhana-0 HDB_LCM_LINUX_X86_64]# _
```

After the installation is finished please check the status of the SAP HANA database.

3. Change the user to <SID>adm (here t01adm) with the command su

```
su - t01 adm
t001-vhana-0:t01adm>
```

4. Use the commands HDB info and HDB version to check the installation

```
t001-vhana-0:t01adm> HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
```

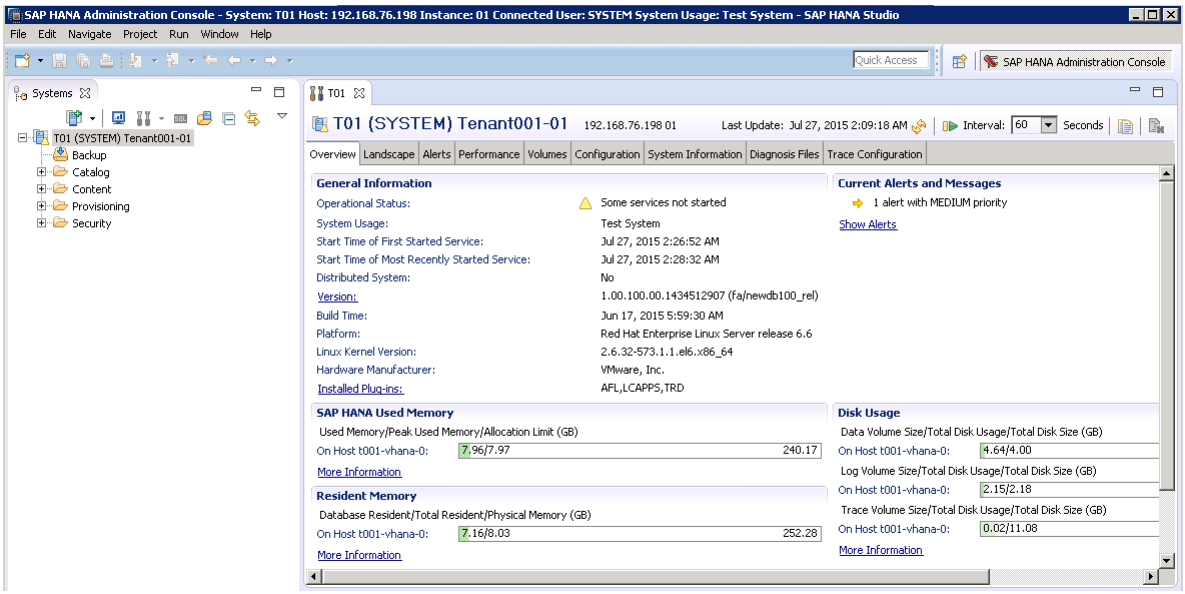
```
t01adm    9841  9840  0.2 108432  1956 -sh
t01adm    9898  9841  0.0 114064  1972  \_ /bin/sh /usr/sap/T01/HDB01/HDB info
t01adm    9925  9898  0.0 118036  1564      \_ ps fx -U t01adm -o user,pid,ppid,
t01adm    9404  9403  0.0 108468  1976 -sh
t01adm    7548     1  0.0  22196  1544 sapstart pf=/hana/shared/T01/profile/T01_
t01adm    7556  7548  0.0 549900 286996  \_ /usr/sap/T01/HDB01/t001-vhana-0/trac
t01adm    7574  7556  0.8 11261988 1242232      \_ hdbnameserver
t01adm    7682  7556  3.6 3301968 744264      \_ hdbcompileserver
t01adm    7685  7556 71.0 10535368 8059748      \_ hdbpreprocessor
t01adm    7708  7556 23.2 12699580 8826808      \_ hdbindexserver
t01adm    7711  7556  2.1 4196404 1118644      \_ hdbxsengine
t01adm    8150  7556  0.6 3088496 414320      \_ hdbwebdispatcher
t01adm    4276     1  0.1 868164 61956 /usr/sap/T01/HDB01/exe/sapstartsrv pf=/ha
t001-vhana-0:t01adm>
t001-vhana-0:t01adm> HDB version
HDB version info:
  version:             1.00.100.00.1434512907
  branch:              fa/newdb100_rel
  git hash:            e88f645daf7c574022a4f10eff99ca4016009d14
  git merge time:      2015-06-17 05:48:27
  weekstone:           0000.00.0
  compile date:        2015-06-17 05:59:30
  compile host:        ld7272
  compile type:        rel
t001-vhana-0:t01adm>
```

## Test the connection to SAP HANA

Use the SAP HANA Studio on a system with network access to the installed SAP HANA system and add the SAP HANA Database. The information you need to do so are:

- Hostname or IP address <<var_tenant001_access_ip>>
- SAP HANA System Number <<var_t001_hana_nr>>

- SAP HANA database user (default: SYSTEM)
- SAP HANA database user password <<var_t001_hana_sys_passwd>>




## SAP HANA Scale-Up System on a Bare Metal Server (Single SID)

This is a common deployment methodology of SAP HANA on premise. In a Cloud model this option is only used if the size of the SAP HANA system does not fit into a virtual machine. Reference SAP and VMware about the actual limitations for virtualized SAP HANA on VMware ESX.

The high-level steps for this use case are as follows:

1. Create the access VLAN on Cisco Nexus 9000, and Cisco UCS.
2. Create Service Profile on Cisco UCS.
3. Define LUNs on the EMC VNX, register the server and configure the Storage-Group.
4. Install and Configure the Operating System.
5. Install SAP HANA.
6. Test the connection to the SAP HANA database.

### Workload Definition

This SAP HANA system is defined as requiring a system size of 1TB main memory, it is for Production and has to run on SUSE Linux Enterprise.

## Requirements

For a SAP HANA database in a Scale-Up configuration, the required networks are the access network and the storage network (in this case through Fibre Channel). To access the installation, sources for SAP HANA and other applications, the access to the NFS share on the EMC VNX storage is also configured; this can be temporary only until all applications are installed. All other networks are optional. For this use case no optional network is used. This is the first system for a tenant, so no existing network definition can be used. Since this is for non-production the relaxed storage requirements apply. The following configuration is required:

Network: 1x Access Network with >=100Mbit/sec

1x NFS-Access Network (to access the installation sources)

Storage: 512GB for /hana/log, 3TB for /hana/data, 1TB for /hana/shared

An average of 300 MB/sec throughput can be used as the baseline. Dependent on the use case it can be less (default analytics) or much more (heavy Suite on HANA)

Memory: 1 TB

CPU: 4x Intel Xeon E7 v2 CPUs (Ivy Bridge)

## Switch Configuration

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

1. On each Nexus 9000, enter configuration mode:

```
config terminal
```

2. From the configuration mode, run the following commands:

```
vlan <<var_t002_access_vlan_id>>
name T002-Access
```

3. Add the VLAN to the VPC Peer-Link:

```
interface po1
switchport trunk allowed vlan <<var_t002_access_vlan_id>>
```

4. Add the VLAN to the Port Channels connected to the Cisco UCS:

```
interface po13,po14
switchport trunk allowed vlan <<var_t002_access_vlan_id>>
```

5. Add the VLAN to the data center uplink

```
interface po99
```

```
switchport trunk allowed vlan add <<var_t002_access_vlan_id>>
```

6. Save the running configuration to start-up:

```
copy run start
```

7. Validate the configuration:

```
#show vpc
…
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,2031,2034,3001

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
11   Po11   up     success     success                    76,177,199,
                                                          2031,2034
12   Po12   up     success     success                    76,177,199,
                                                          2031,2034
13   Po13   up     success     success                    76,177,199,
                                                          2031,2034,3
                                                          001,3002
14   Po14   up     success     success                    76,177,199,
                                                          2031,2034,3
                                                          001,3002
…

show vlan id 3002
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3002 Tenant002-Access                 active    Po1, Po13, Po14, Po99, Eth1/1
                                                Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                Eth1/9, Eth1/10, Eth1/15
                                                Eth1/16, Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3002 enet         CE

Remote SPAN VLAN
----------------
Disabled

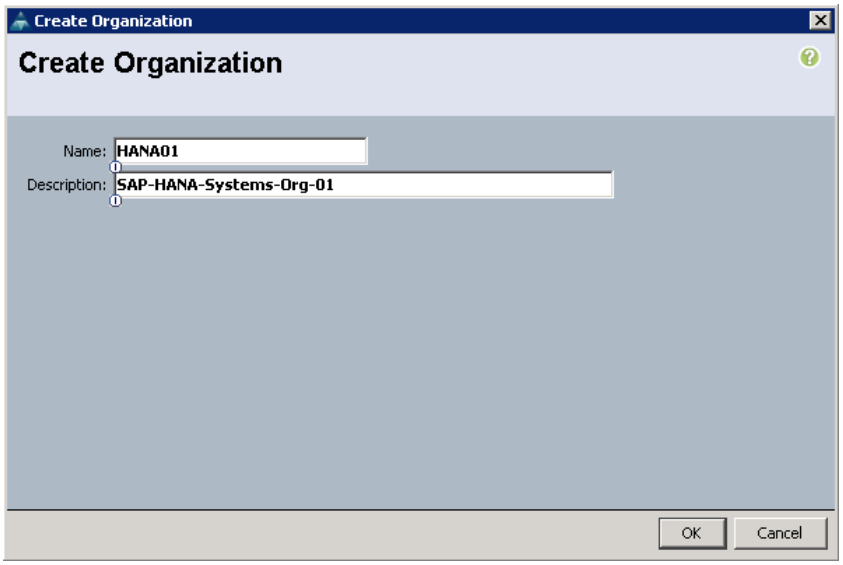
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

## Cisco UCS Configuration

### Create Sub-Org HANA01

To create the Sub-Org HANA01, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service-Profiles > root.
3. Right-click Sub-Organizations.
4. Enter T002 in the Name field.
5. Enter a Description.
6. Click OK.

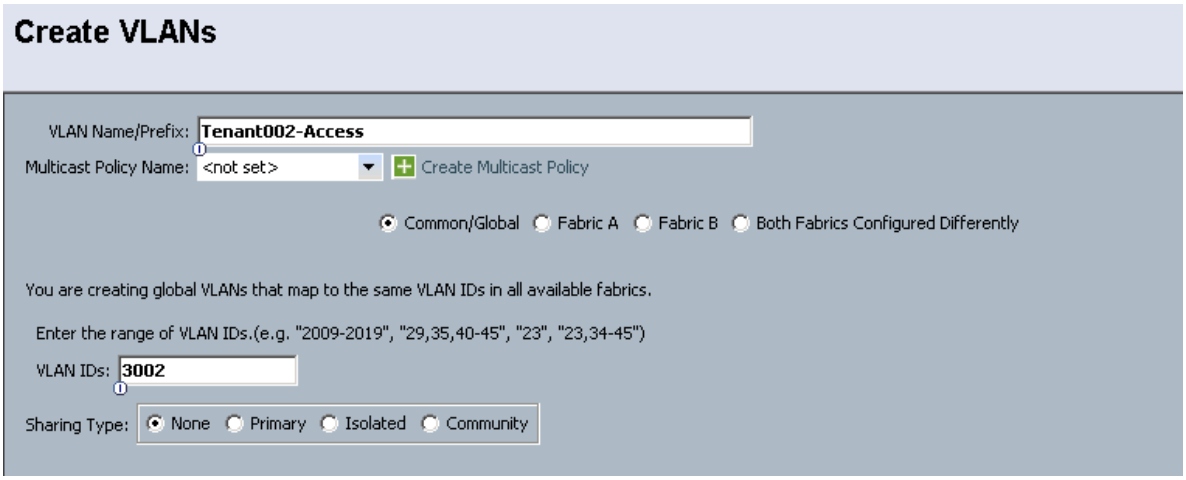



### Configure VLANs and VLAN-Group Membership

To create a VLAN, complete the following steps:

1. Log in to Cisco UCS Manager.
2. Go to LAN Tab > LAN Cloud > VLANs.
3. Right-click > Create VLANs.
4. Enter <<var_ucs_t002_access_vlan_name>> as the VLAN Name.
5. Enter <<var_t002_access_vlan_id>> as the VLAN ID.
6. Click OK.

7. Click OK.



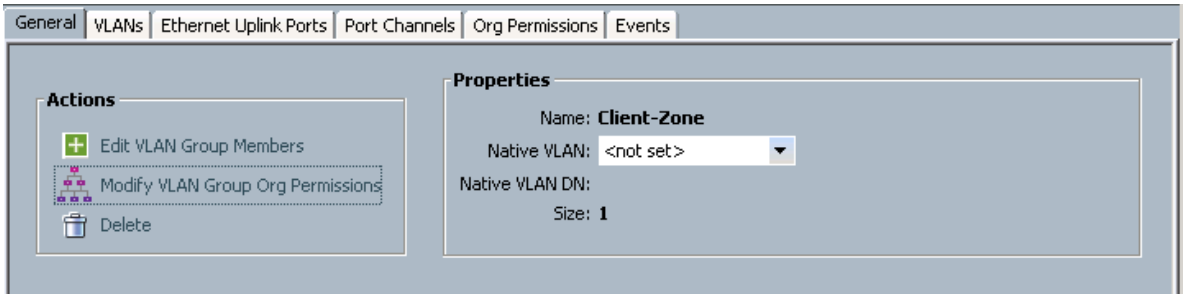

8. Go to LAN Tab > LAN Cloud > VLAN Groups.

9. Select VLAN group Client-Zone.

10. Click the Info Icon 

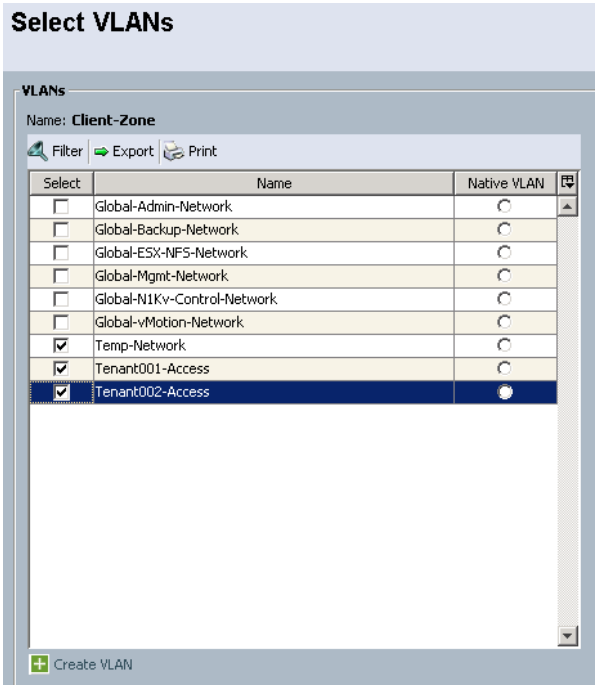
on the right side of the list.

11. Click Edit VLAN Group Members.




12. Select <<var_ucs_t002_access_vlan_name>>.

13. Click Finish.

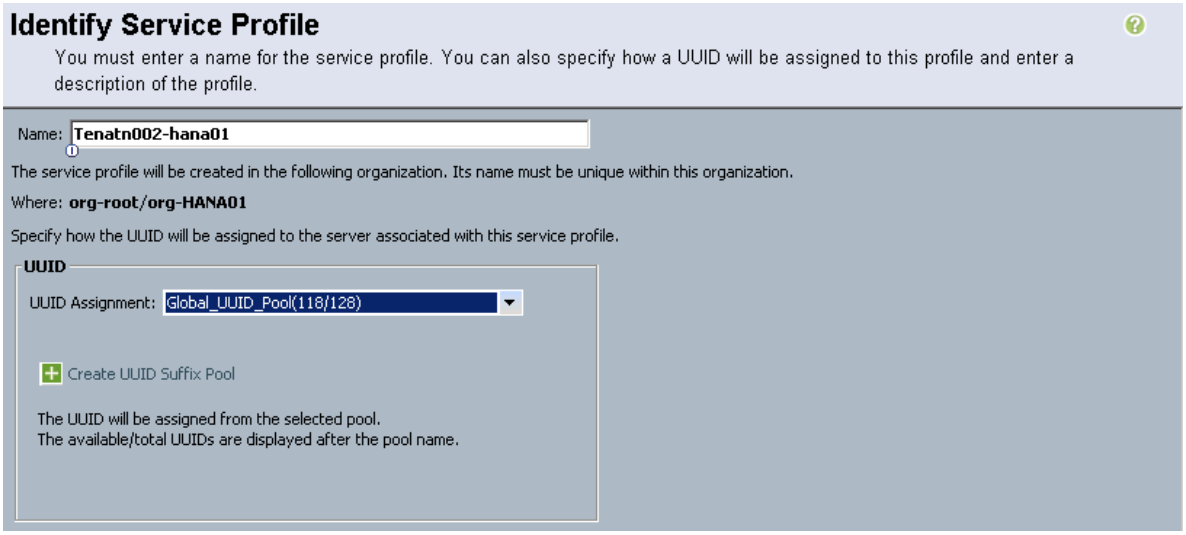



14. Click OK.

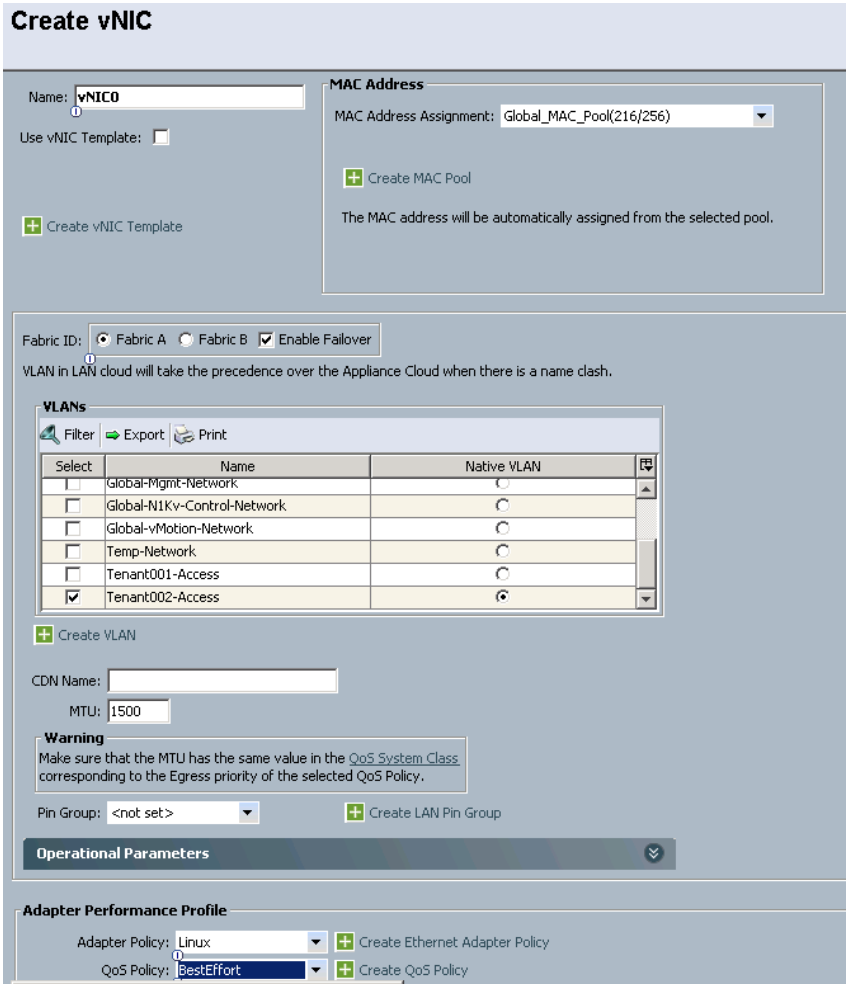
## Create Service Profile for a Cisco UCS B460 M4 or C460 M4 Server

To create a service profile, complete the following steps:

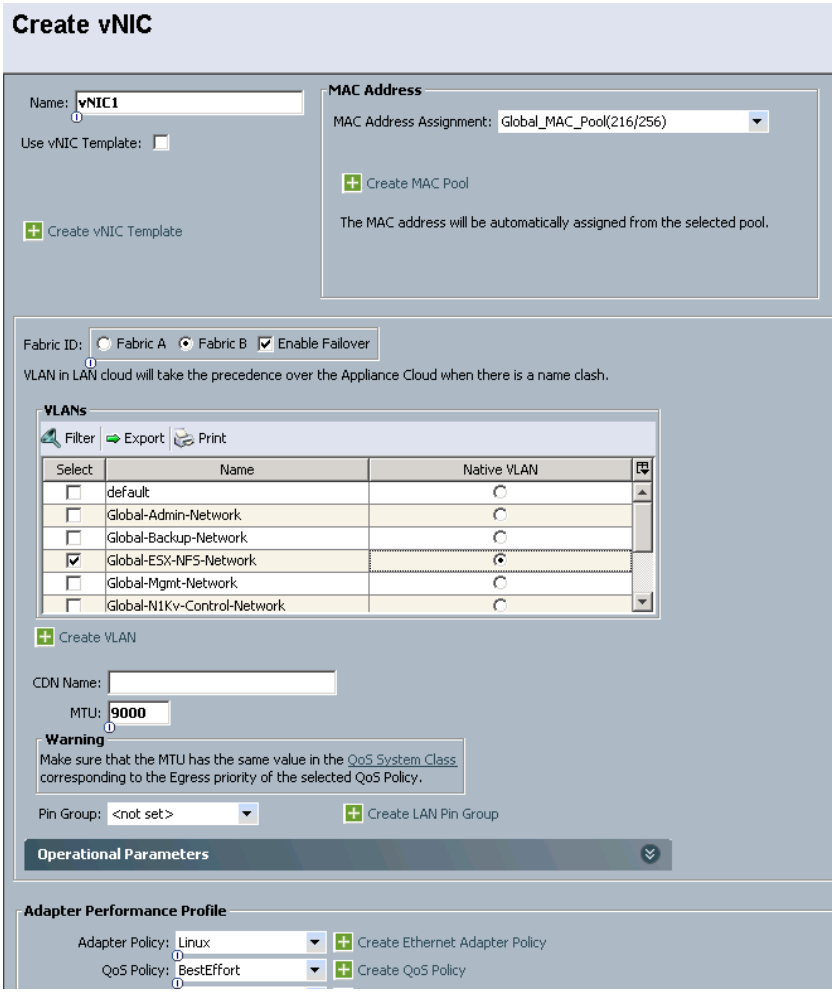
1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. In the Actions section on the right pane click Create Service Profile (expert)
3. Enter <<var_ucs_t002_hana1_sp_name>>  as the Name
4. Select Global_UUID_Pool from the drop-down menu UUID-Assignment
5. Click Next



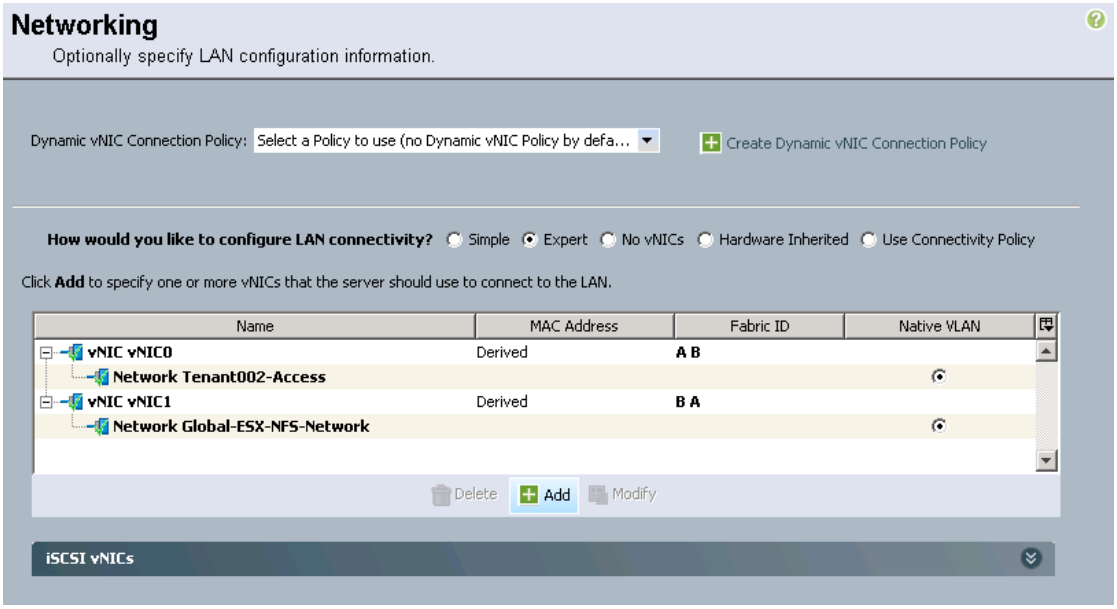

6. Click Next on the Storage Provisioning View
7. On the Networking View select Expert and click Add
8. Enter vNIC0 as the Name
9. Select <<var_global_mac_pool>> for the MAC Address Assignment
10. Select Fabric A and click the Check-Box for Enable Failover
11. Select <<var_ucs_t002_access_vlan_name>> and click the Radio-Button for Native VLAN
12. Enter 1500 as the MTU
13. Select Linux as the Adapter Policy
14. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy
15. Click OK



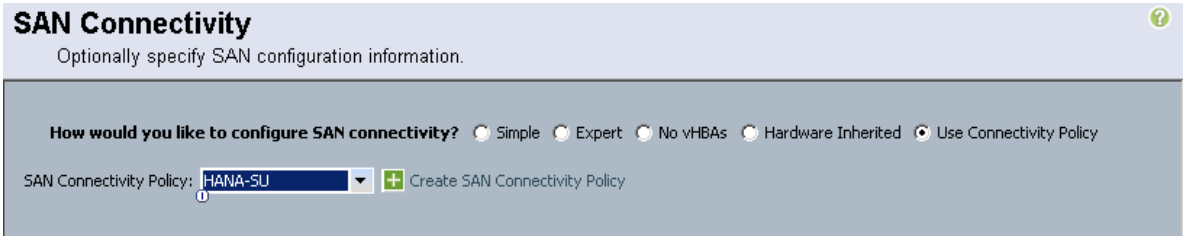

16. Click Add
17. Enter vNIC1 as the Name
18. Select <<var_global_mac_pool>> for the MAC Address Assignment
19. Select Fabric B and click the Check-Box for Enable Failover
20. Select <<var_ucs_esx_nfs_vlan_name>> and click the Radio-Button for Native VLAN
21. Enter 9000 as the MTU
22. Select Linux as the Adapter Policy
23. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy
24. Click OK



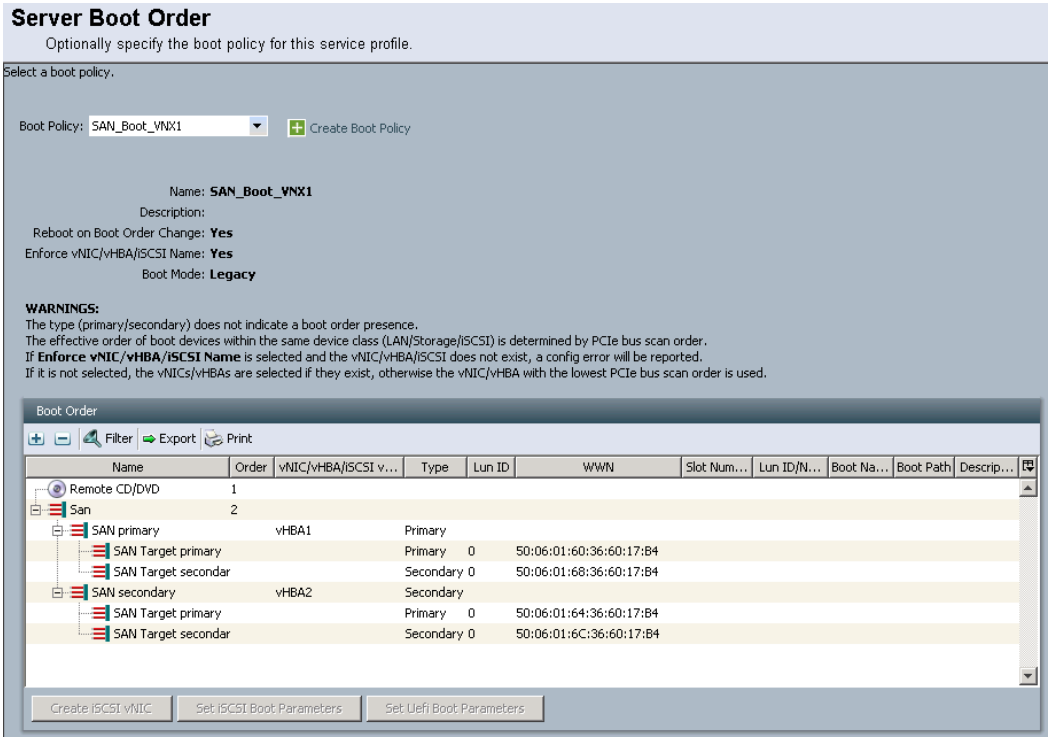

25. Click Next




26. On the SAN Connectivity View select Use Connectivity Policy
27. Select <<var_ucs_hana_su_connect_policy_name>> as the SAN Connectivity Policy
28. Click Next

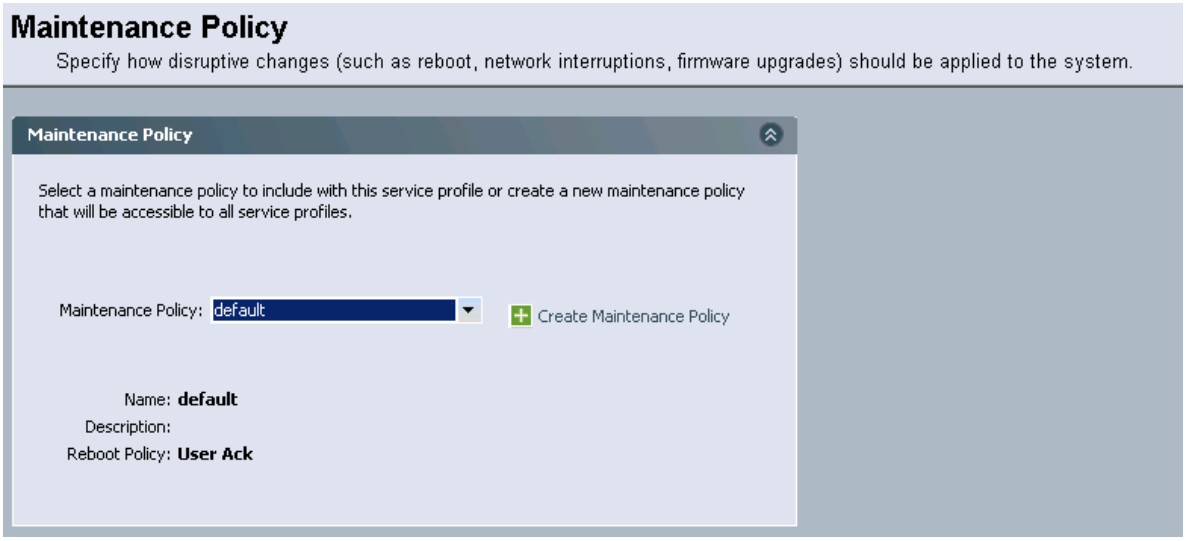



29. On the Zoning View, click Next
30. On the vNIC/vHBA Placement view, click Next
31. On the vMedia Policy view, click Next
32. On the Server Boot Order view, select <<var_ucs_san_boot_policy>> as the boot policy
33. Click Next




34. On the Maintenance Policy view, select default as the Policy

35. Click Next

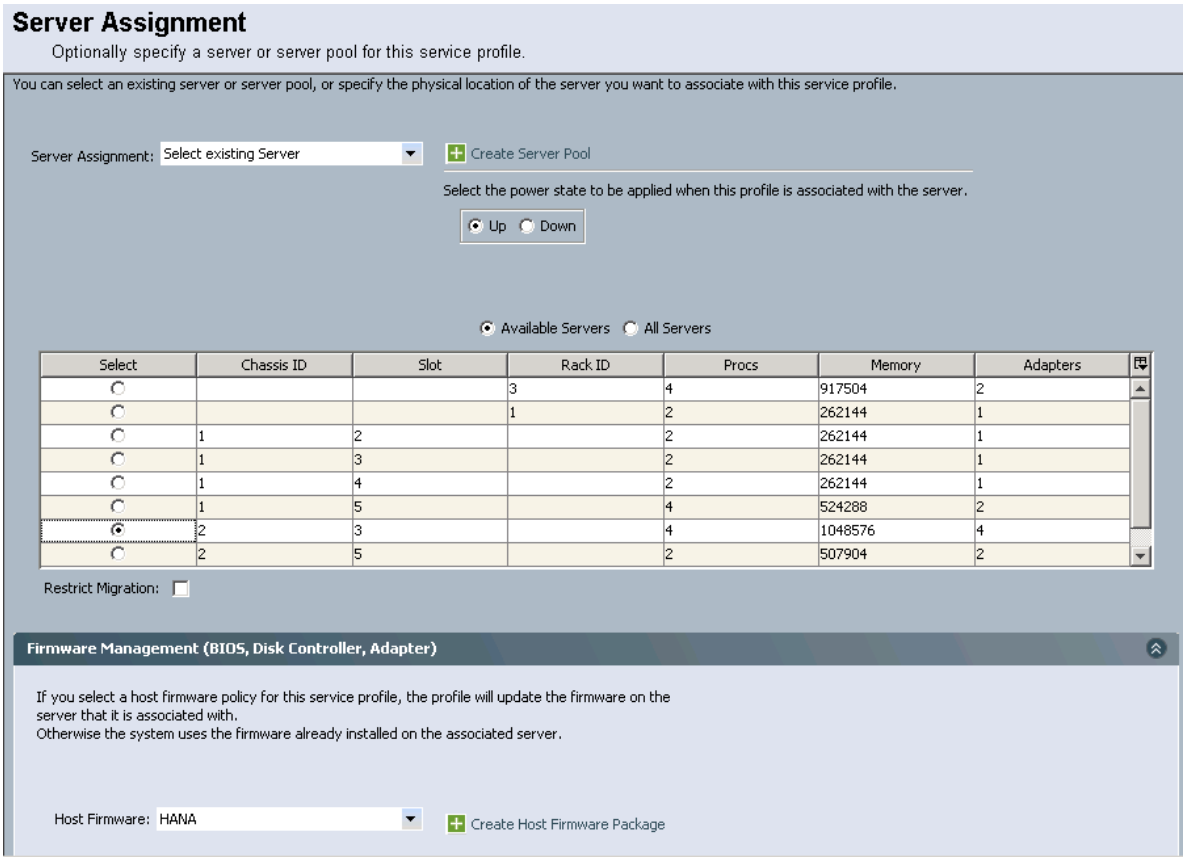



36. On the Server Assignment view, select a Server or Server Pool with the required configuration (1TB memory)

37. Open the Firmware Management section

38. Select <<var_ucs_hana_fw_package_name>> as the Host Firmware package

39. Click Next



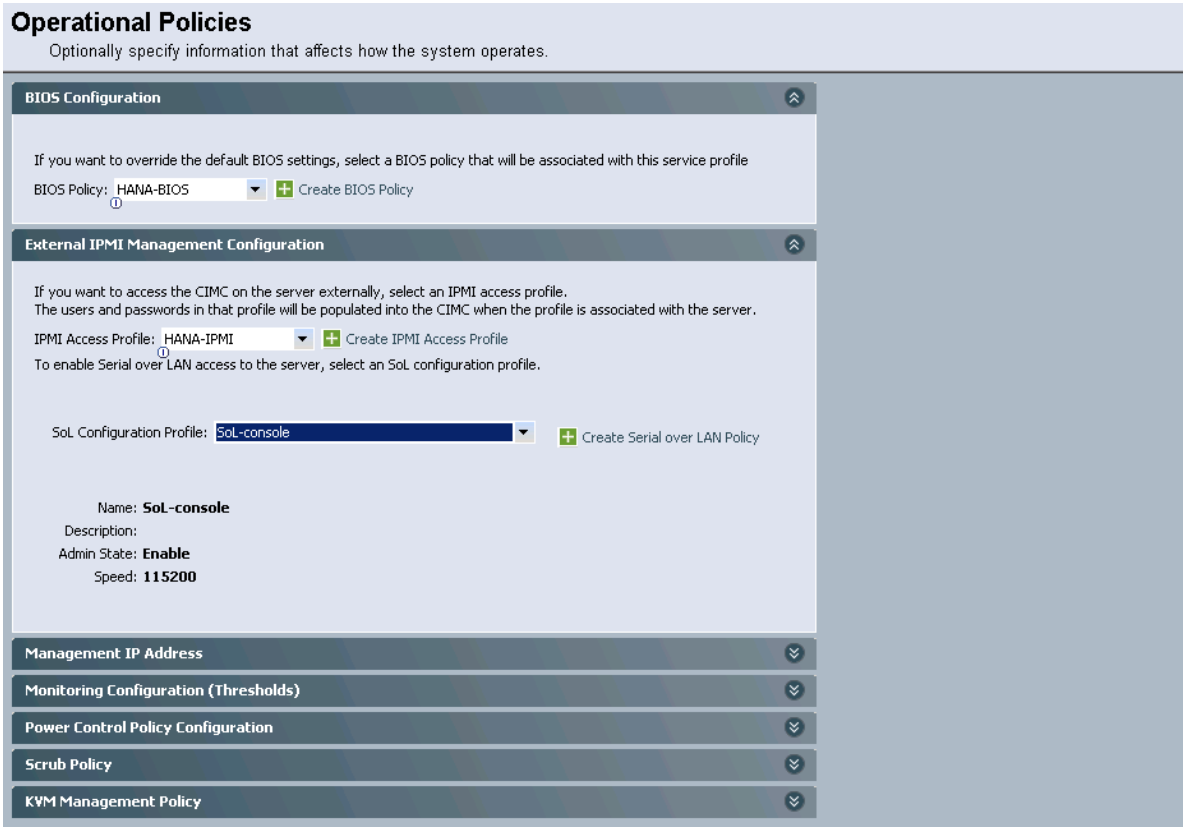

40. On the Operational Policies view, select HANA-BIOS as the BIOS-Policy

41. Open the External IPMI Management Configuration

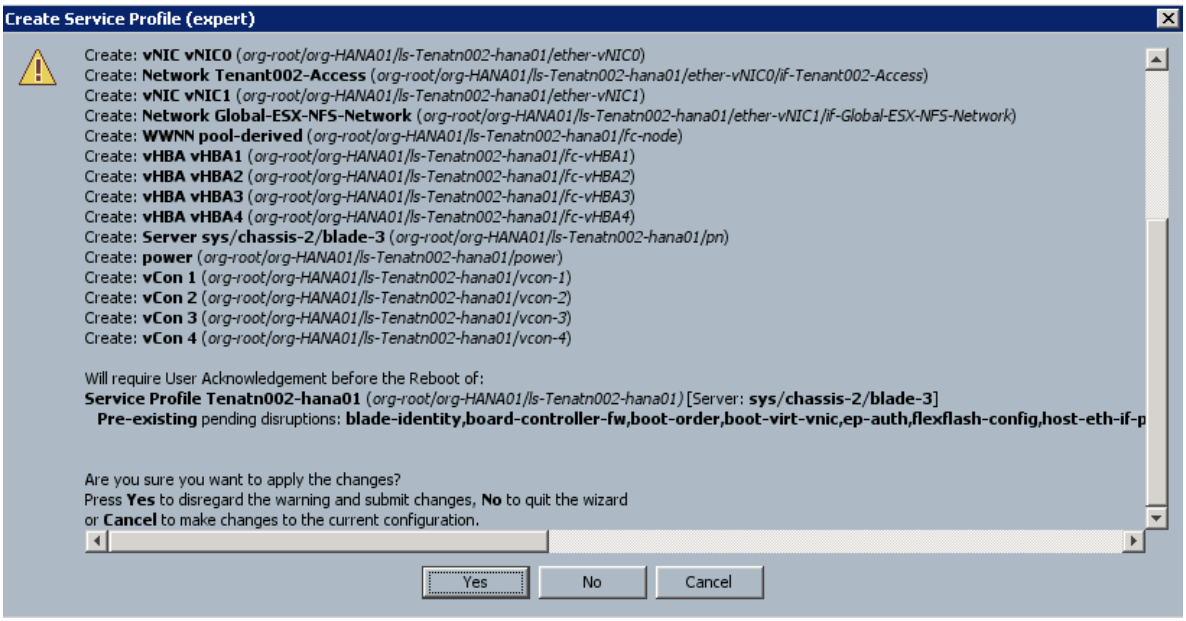
42. Select <<var_ucs_ipmi_policy>> as the IPMI Access Policy

43. Select <<var_ucs_sol_profile>> as the SoL Configuration Profile

44. Click Finish

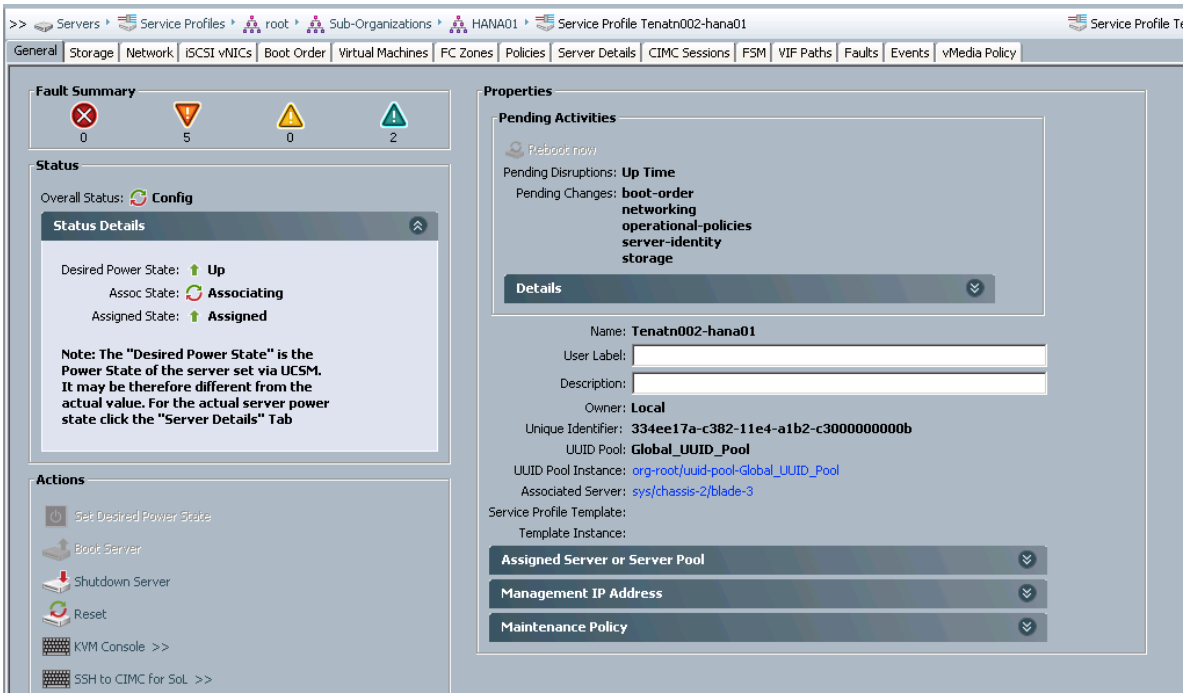



45. Click Yes

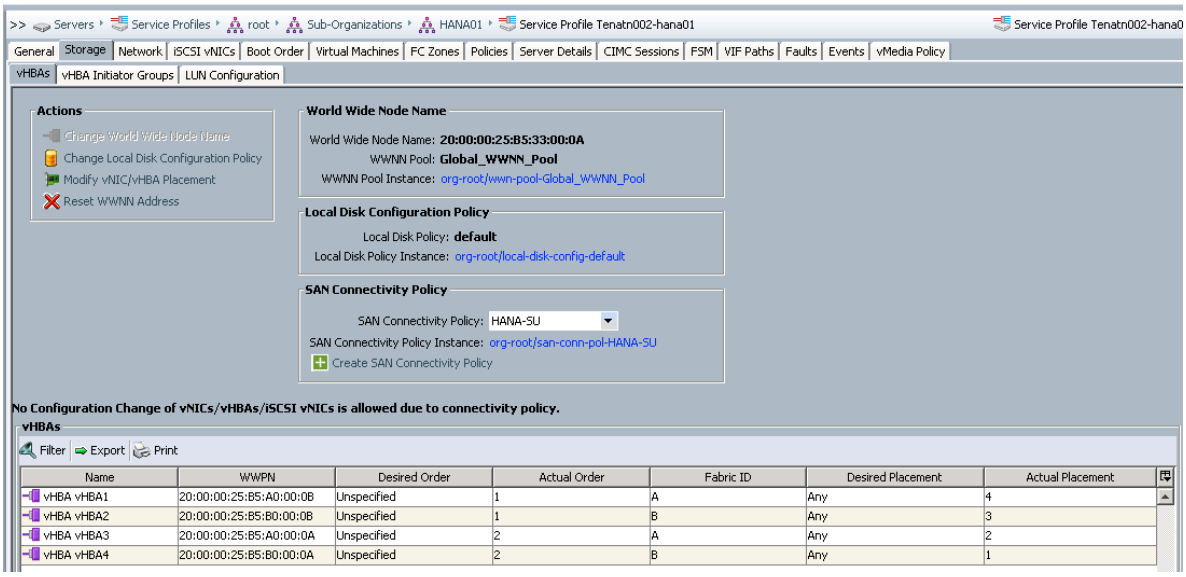



46. Click OK

47. The Cisco UCS Service Profile is deployed, the server is selected and the Service Profile is in Config status




48. Click the Storage Tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX




## Configure Cisco MDS Switches

For every Service Profile in Cisco UCS, one or more SAN Zones are required per Cisco MDS switch.

## Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t002-hana1>> vsan 10
zone name <<var_zone_t002-hana1>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:0b
   exit

zoneset name CRA-EMC-A vsan 10
member pwwn <<var_zone_t002-hana1>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

…
```

```
zone name zone_t002-hana1 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0b

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-hana1
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t002-hana1>> vsan 20

zone name <<var_zone_t002-hana1>> vsan 20
```

```
   member pwwn 20:00:00:25:b5:b0:00:0b
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_t002-hana1>>
exit

zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_t002-hana1 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0b

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
```

```
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-hana1
CRA-EMC-B#
```

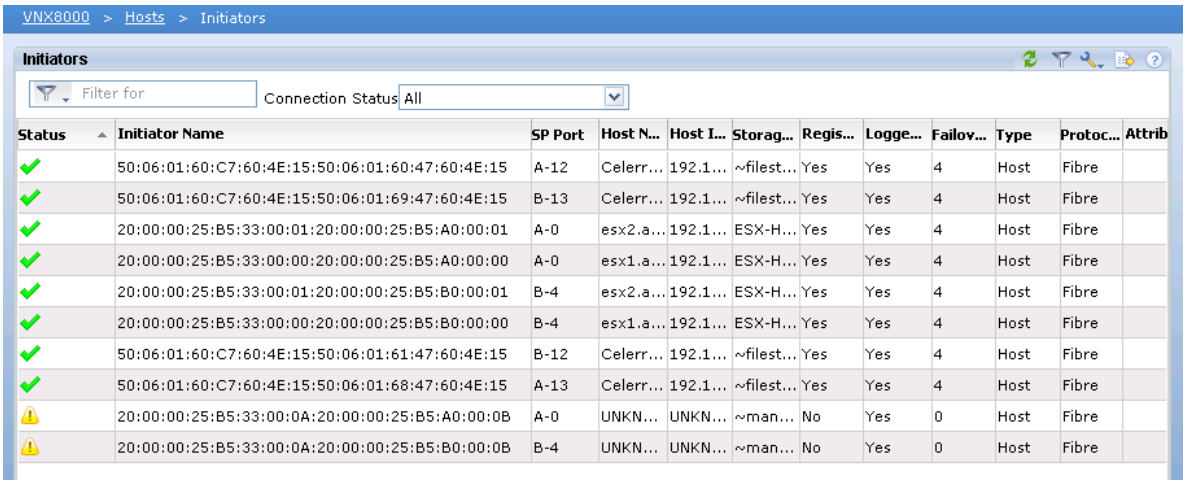
4. Save the running configuration as startup configuration

```
Copy run start
```

## Configure EMC VNX

### Register Host

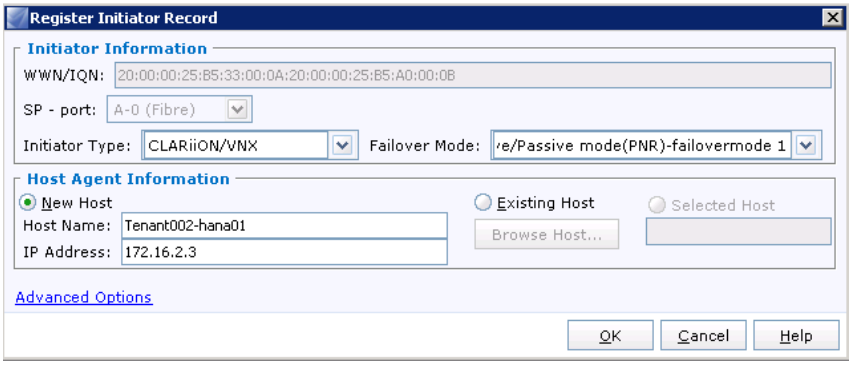
1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators



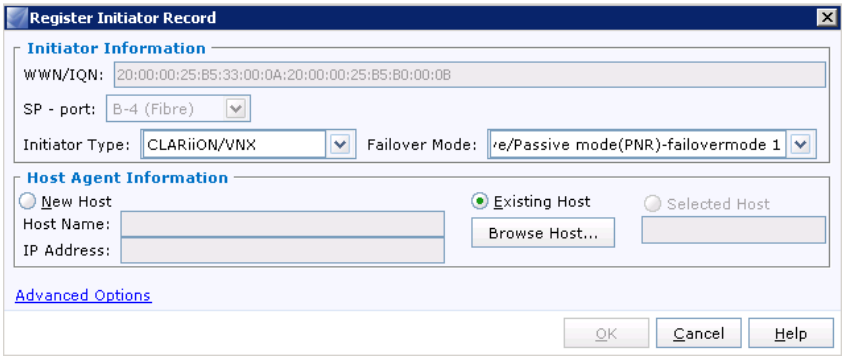

| Status | Initiator Name | SP Port | Host N... | Host I... | Storag... | Regis... | Logge... | Failov... | Type | Protoc... | Attrib |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:60:47:60:4E:15 | A-12 | Celerr... | 192.1... | ~filest... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:69:47:60:4E:15 | B-13 | Celerr... | 192.1... | ~filest... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:01:20:00:00:25:B5:A0:00:01 | A-0 | esx2.a... | 192.1... | ESX-H... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:00:20:00:00:25:B5:A0:00:00 | A-0 | esx1.a... | 192.1... | ESX-H... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:01:20:00:00:25:B5:B0:00:01 | B-4 | esx2.a... | 192.1... | ESX-H... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 20:00:00:25:B5:33:00:00:20:00:00:25:B5:B0:00:00 | B-4 | esx1.a... | 192.1... | ESX-H... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:61:47:60:4E:15 | B-12 | Celerr... | 192.1... | ~filest... | Yes | Yes | 4 | Host | Fibre | |
| ✔ | 50:06:01:60:C7:60:4E:15:50:06:01:68:47:60:4E:15 | A-13 | Celerr... | 192.1... | ~filest... | Yes | Yes | 4 | Host | Fibre | |
| ⚠ | 20:00:00:25:B5:33:00:0A:20:00:00:25:B5:A0:00:0B | A-0 | UNKN... | UNKN... | ~man... | No | Yes | 0 | Host | Fibre | |
| ⚠ | 20:00:00:25:B5:33:00:0A:20:00:00:25:B5:B0:00:0B | B-4 | UNKN... | UNKN... | ~man... | No | Yes | 0 | Host | Fibre | |

2. Select one of the unregistered entries for the host Tenant002-hana01, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
5. Enter <<var_ucs_t002_hana1_sp_name>> as the Host Name (indicates the relationship to the Service Profile)
6. Enter <<var_t002_hana1_access_ip>> as the IP Address

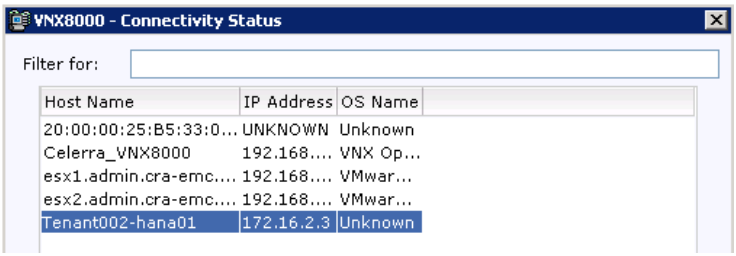
7. Click OK
8. Click Yes
9. Click OK
10. Click OK




11. Select the second Entry for this host <<var_ucs_t002_hana1_sp_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and Click Browse Host



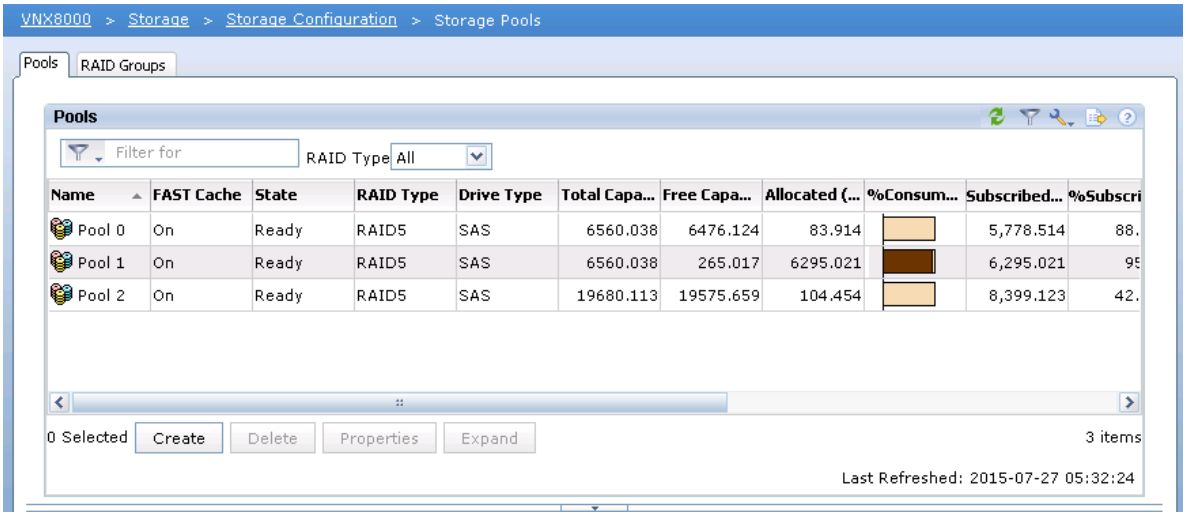

15. Select <<var_ucs_t002_hana1_sp_name>> and click OK



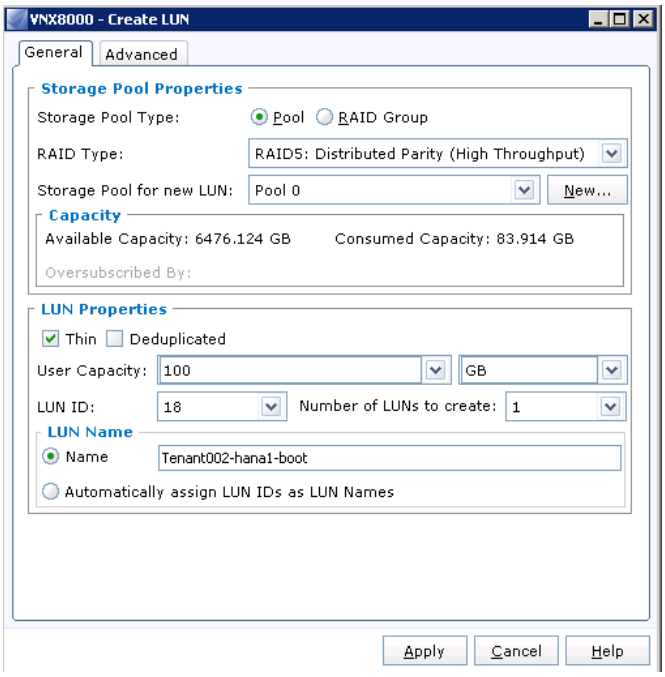
16. Click OK
17. Click Yes
18. Click OK
19. Click OK

## Create LUNs

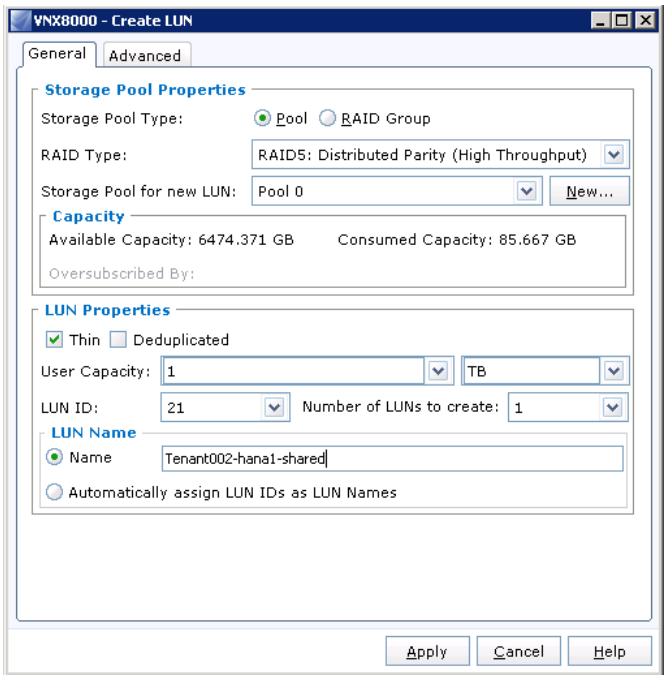
1. Navigate to Storage > Storage Pool



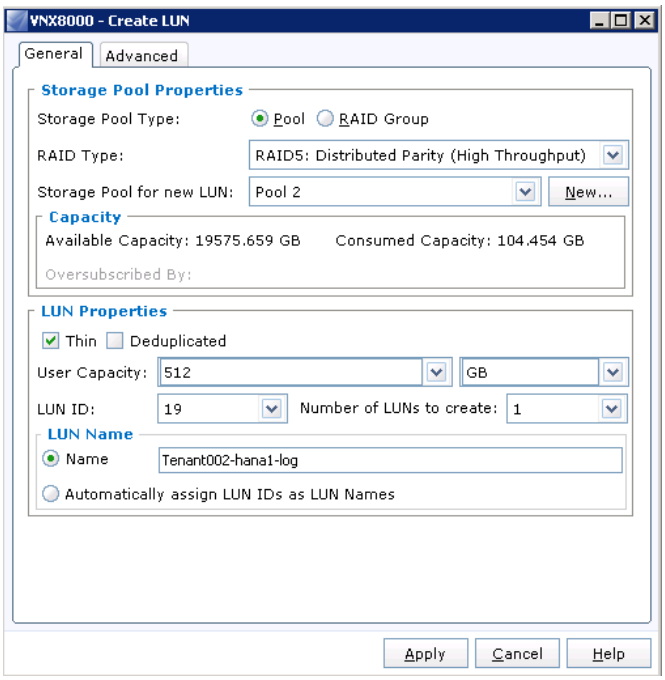

2. Right-click Pool 0
3. Select Create LUN
4. Enter 100 GB as the User Capacity
5. Click Name and enter <<var_ucs_t002_hana1_sp_name>>-boot
6. Click Apply
7. Click Yes
8. Click OK



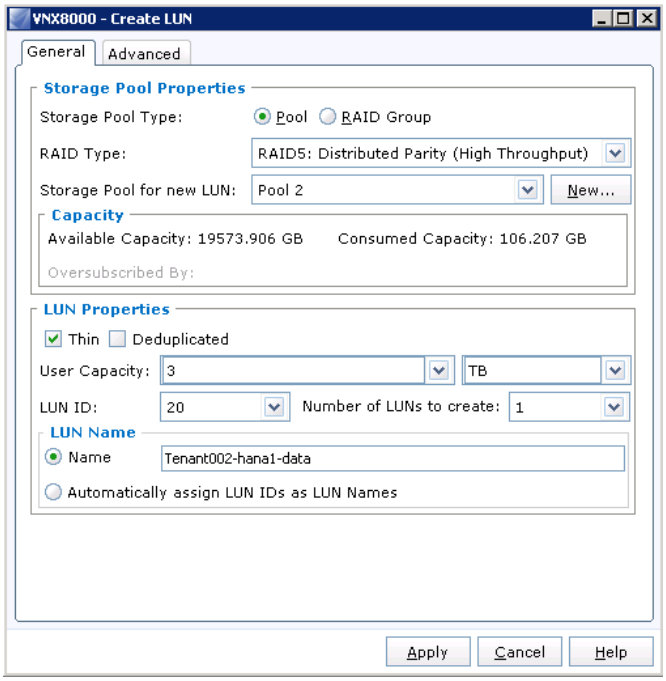

9. Enter 1 TB as the User Capacity
10. Click Name and enter <<var_ucs_t002_hana1_sp_name>>-shared
11. Click Apply
12. Click Yes
13. Click OK




14. Click Cancel
15. Right-click Pool 2
16. Select Create LUN
17. Enter 512 GB as the User Capacity
18. Click Name and enter <<var_ucs_t002_hana1_sp_name>>-log
19. Click Apply
20. Click Yes
21. Click OK



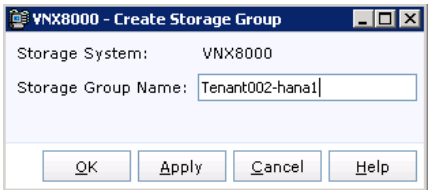

22. Enter 3 TB as the User Capacity
23. Click Name and enter <<var_ucs_t002_hana1_sp_name>>-data
24. Click Apply
25. Click Yes
26. Click OK




27. Click Cancel

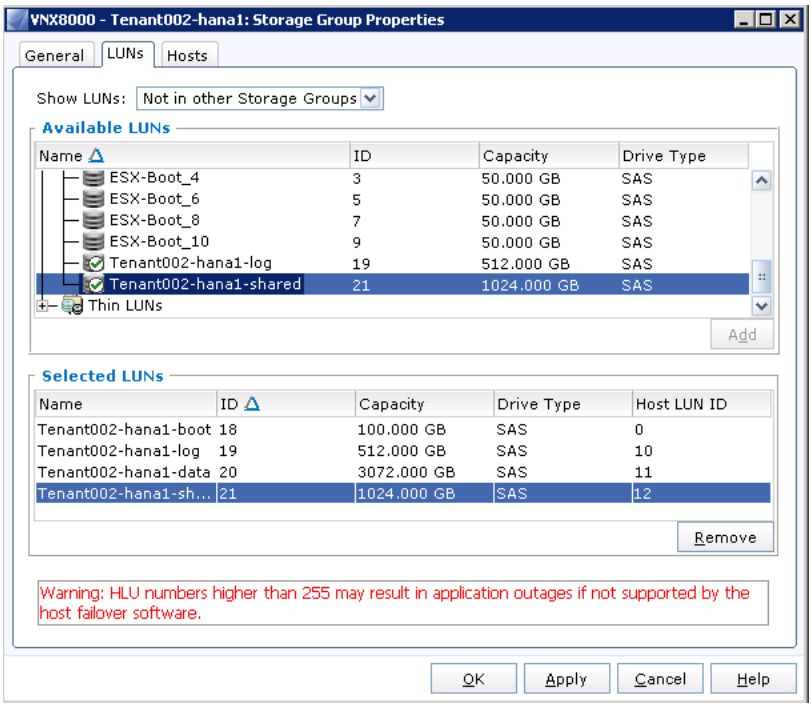
## Create Storage-Group

1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t002_hana1_sp_name>> as the Name
4. Click OK
5. Click Yes

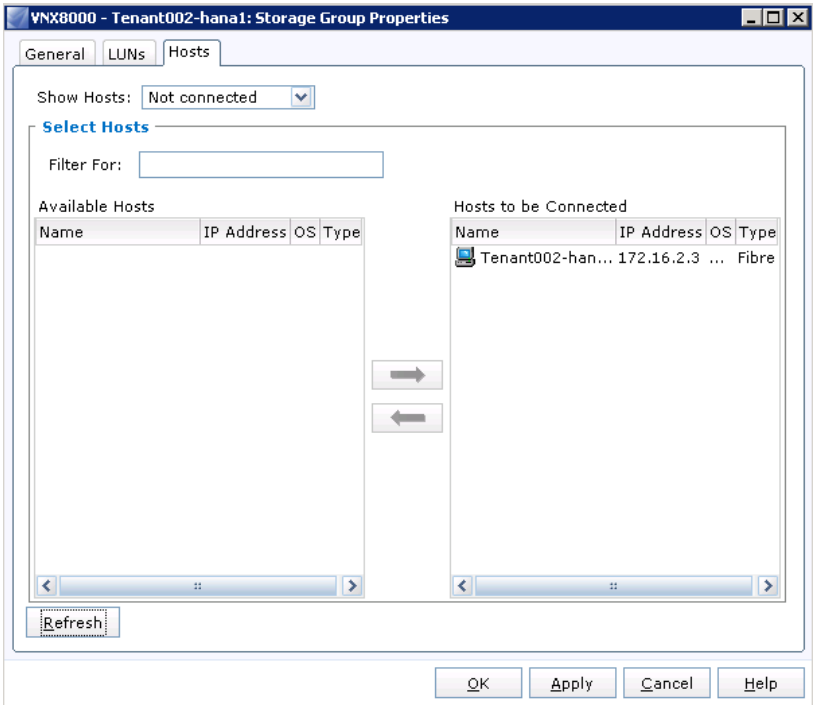



6. Click Yes
7. Select one of the four created LUNs and click Add
8. Repeat this for the other LUNs excepting the data LUN
9. Select 0 as the Host LUN ID for <<var_ucs_t002_hana1_sp_name>>-boot

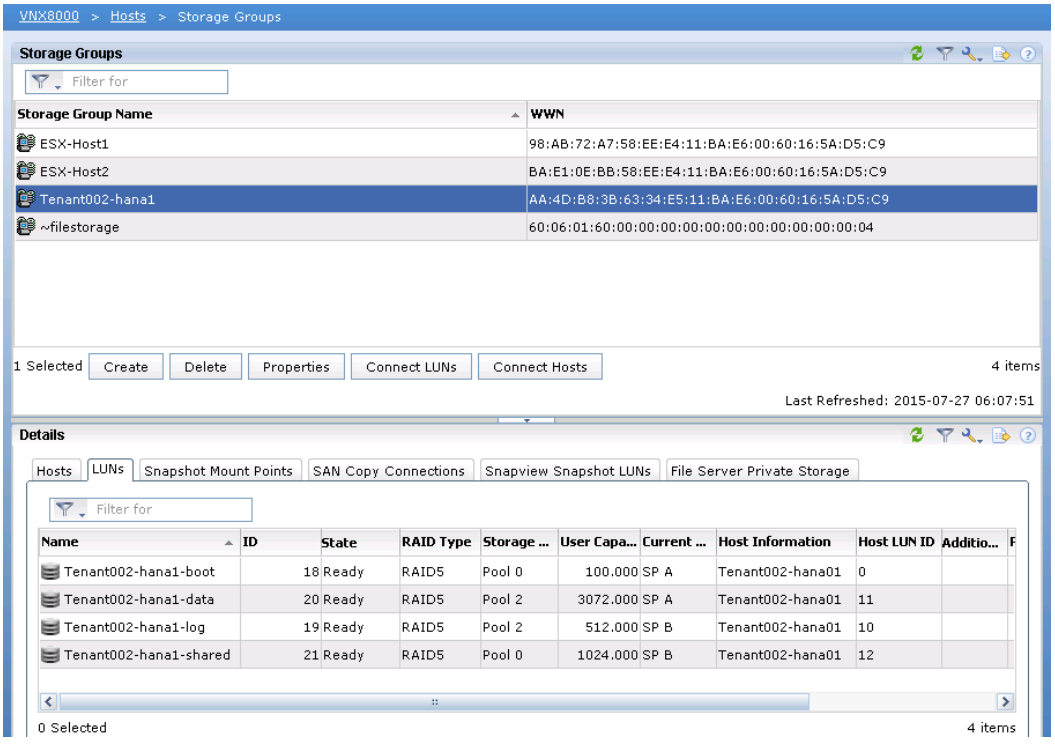
10. Select 10 as the Host LUN ID for <<var_ucs_t002_hana1_sp_name>>-log
11. Select 11 as the Host LUN ID for <<var_ucs_t002_hana1_sp_name>>-data
12. Select 12 as the Host LUN ID for <<var_ucs_t002_hana1_sp_name>>-shared
13. Click Apply
14. Click Yes
15. Click OK




16. Click the Hosts tab
17. Select <<var_ucs_t002_hana1_sp_name>>
18. Click OK
19. Click Yes
20. Click OK



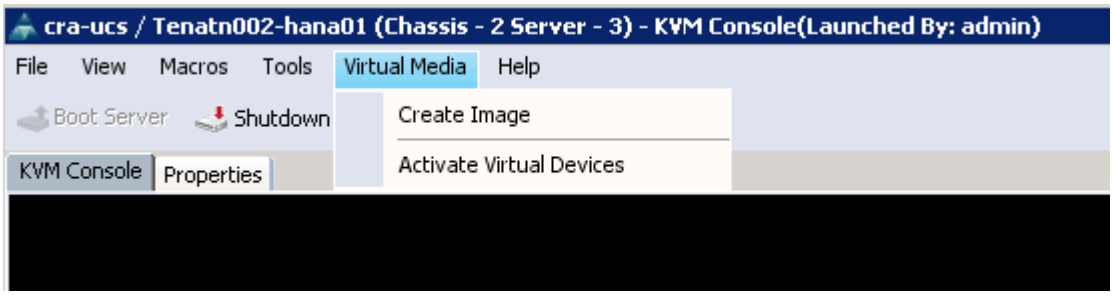

21. The Result will look as shown below:



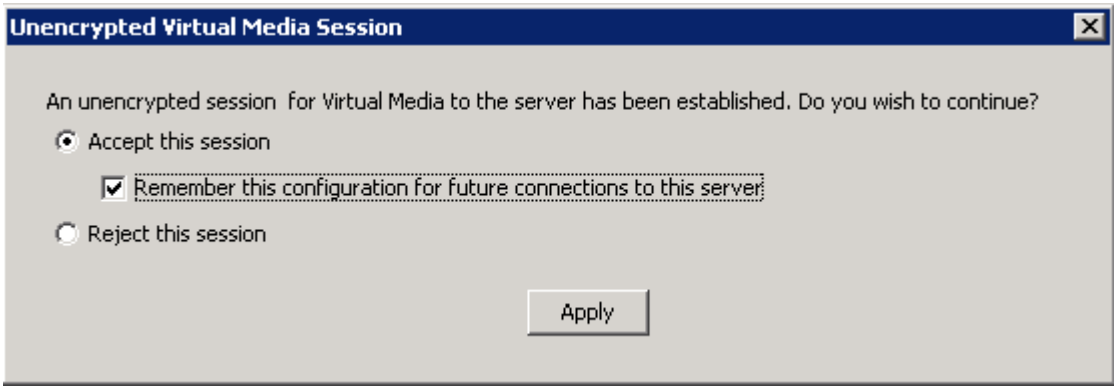

## Install the Operating System

To install the operating system, complete the following steps:

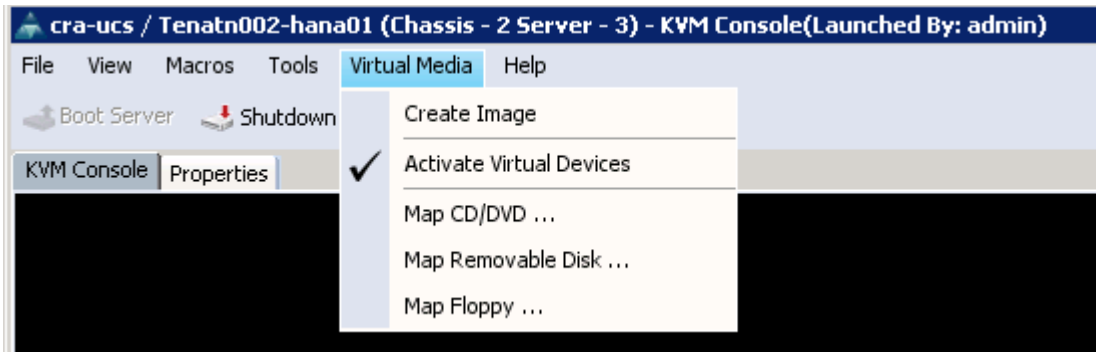
1. Return to the Cisco UCS Manager and select the Service Profile <<var_ucs_t002_hana1_sp_name>>
2. Click KVM Console
3. Click the Menu Virtual Media
4. Select Activate Virtual Devices




5. In the new Window, Select Accept this Session. If you like you can also select the Check-Box to Remember this setting
6. Click Apply

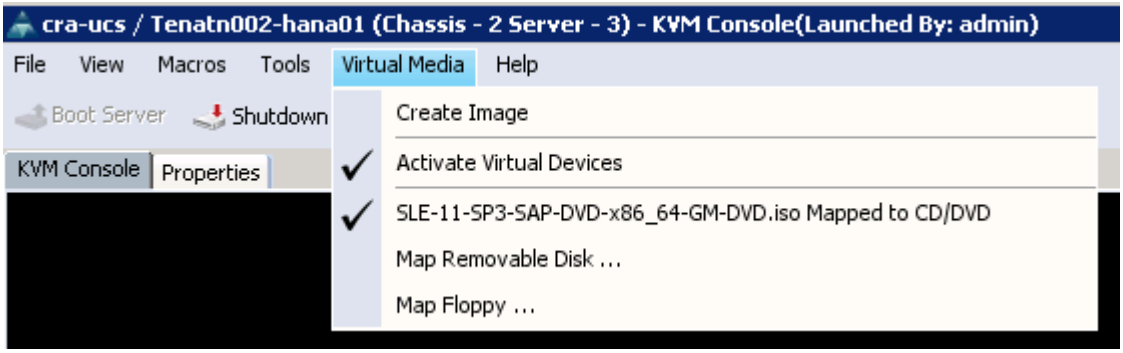



7. Click again on the Menu Virtual Media
8. Select Map CD/DVD...

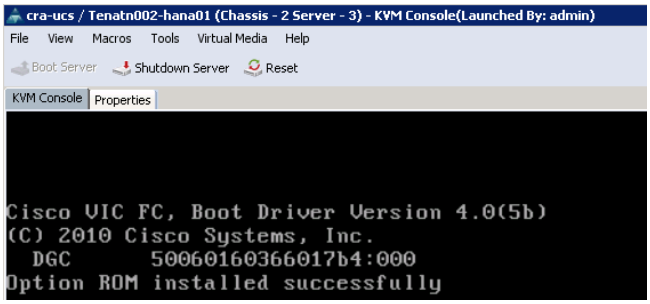


9. Click Browse, and select the SUSE Linux Enterprise for SAP Installation ISO

10. Click Map Device

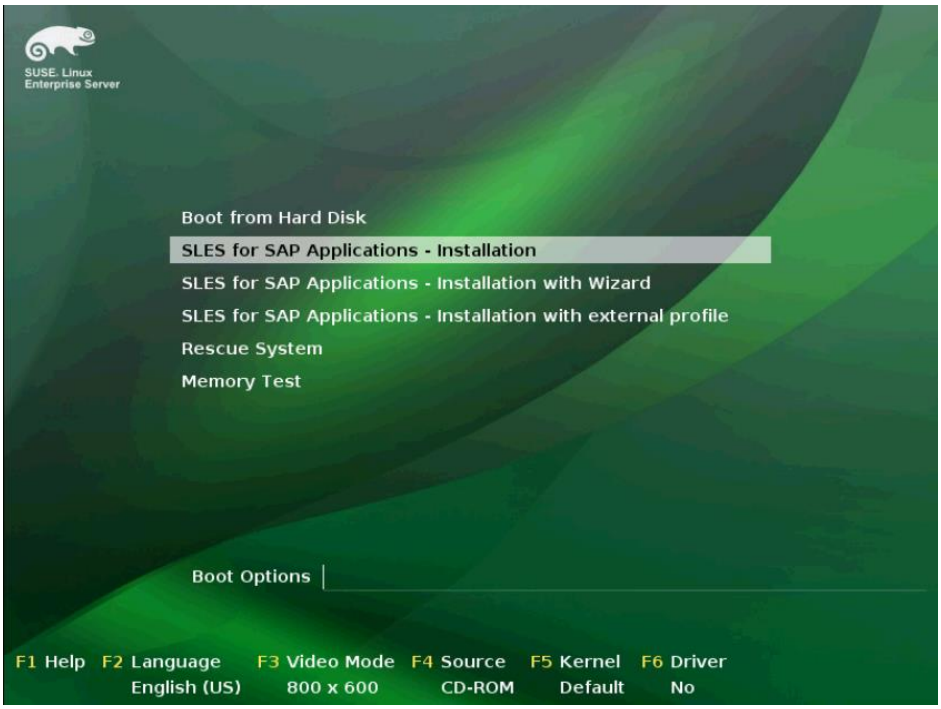



11. Click Reset to reset the server. This will force the system to scan the SAN and get access to the LUNs on the EMC VNX.

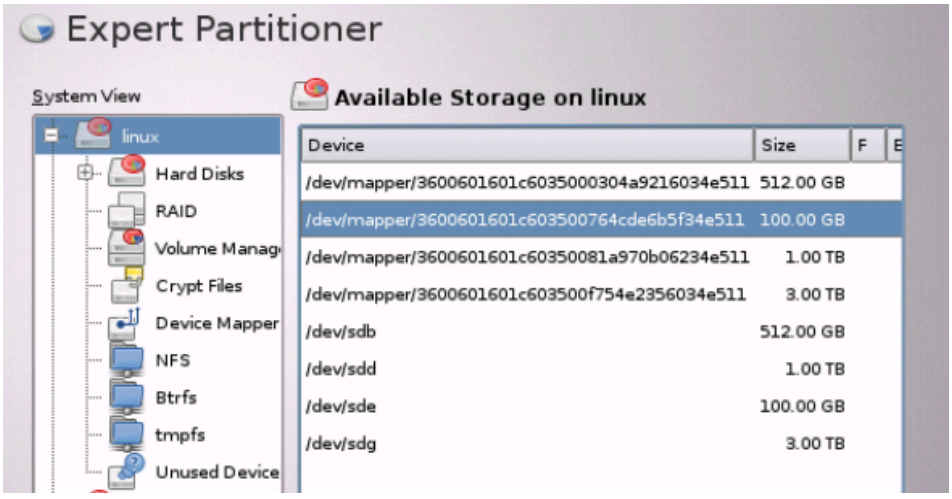



12. The System will automatically boot from the ISO image

13. Select SLES for SAP Applications – Installation and press Enter




14. Follow the instructions on screen and select Yes to activate multipath
15. Please change the Partitioning as following:
    a. Select Custom Partitioning (for Experts), click Next
    b. Select the /dev/mapper device with the size of 100GB




16. Right-click the device, select Add Partition.
17. Select Primary Partition, click Next
18. Use 98GB as the Size, click Next

19. Use Ext3 as the File System
20. Use / as the Mount Point
21. Click Finish

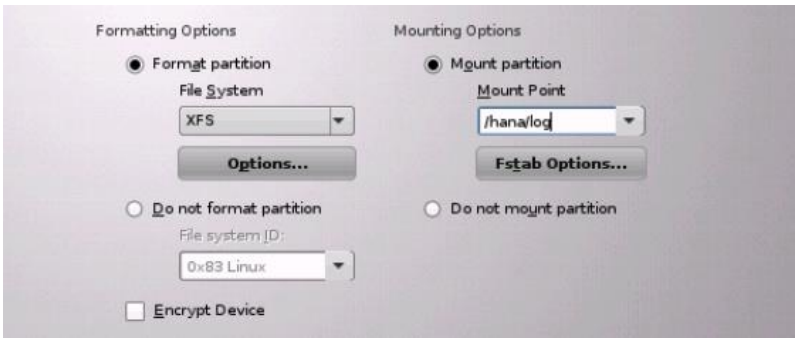



22. Right-click the same device
23. Select Add Partition
24. Select Primary Partition, click Next
25. Use 2GB as the Size, click Next
26. Use Swap as the File System
27. Use swap as the Mount Point
28. Click Finish




29. Click the Device with the size of 512GB
30. Right-click the Device and Select Add Partition
31. Select Primary Partition, click Next
32. Select Maximum Size, click Next

33. Use XFS as the File System
34. Use /hana/log as the Mount point
35. Click Finish




36. Click the Device with the size of 3TB
37. Right-click the Device and Select Add Partition
38. Select Primary Partition, click Next
39. Select Maximum Size, click Next
40. Use XFS as the File System
41. Use /hana/data as the Mount point
42. Click Finish

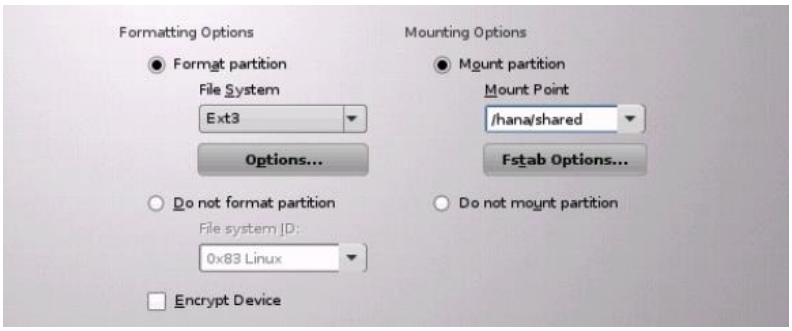



43. Click the Device with the size of 1TB
44. Right-click the Device and Select Add Partition
45. Select Primary Partition, click Next
46. Select Maximum Size, click Next

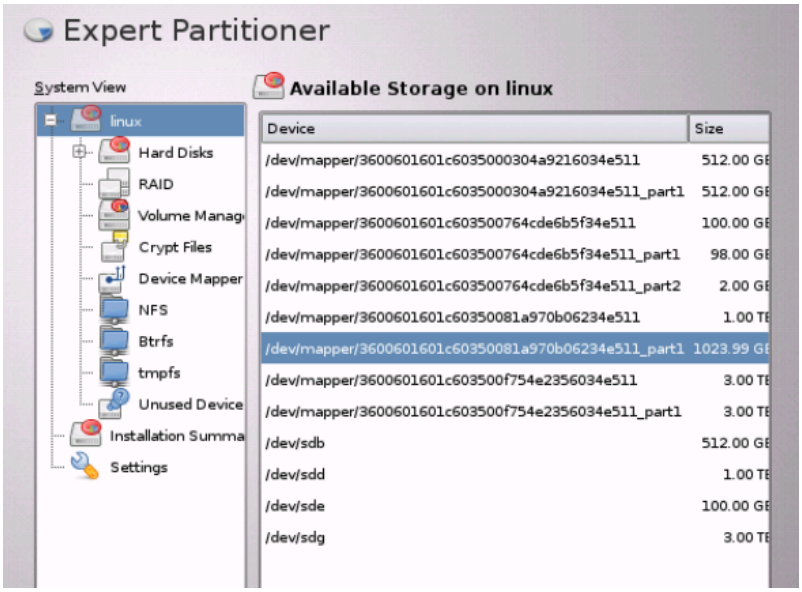
47. Use EXT3 as the File System

48. Use /hana/shared as the Mount point

49. Click Finish




The Partition Table should look like this:




50. Click Accept

51. Click Change, select Booting

52. Select Boot Loader Installation Tab

53. Click Boot Loader Installation Details

54. Take care that the boot device is the first in the list

55. Click OK



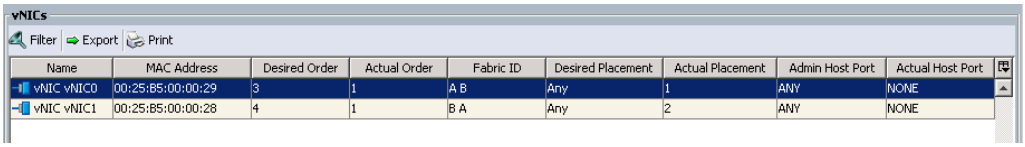

56. Click OK
57. Click Change, select Software
58. Unselect GNOME Desktop Environment
59. Select SAP HANA Server Base
60. Click OK
61. Click Accept
62. Click Change, select Default Runlevel
63. Select 3: Full multiuser with network
64. Click OK
65. Click Install
66. Click Install

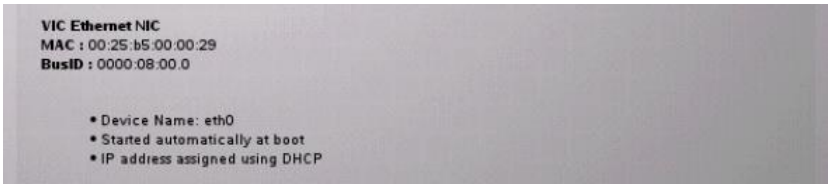


The Operating System will be installed as defined and the server reboots automatically.

67. After the reboot, please proceed with the system configuration
68. Use <<var_mgmt_passwd>> as the password for root
69. Use <<var_t002_hana01_hostname>> as the hostname
70. Use <<var_t002_domain>> as the domain. It is possible to use the end customer domain.
71. Disable the firewall for now.
72. Change the Network Settings as following:

73. Select the interface connected to <<var_ucs_t002_access_vlan_name>>, best way is to check the MAC address in UCS Manager and on the operating system




74. Select Edit

75. Select Static assigned IP Address

76. Use <<var_t002_hana1_access_ip>> as the IP Address

77. Use <<var_t002_access_mask>> as the Subnet Mask

78. Click Next

79. Select the second NIC, click Edit

80. Select Static assigned IP Address

81. Use <<var_t002-hana01_nfs_ip>> as the IP Address

82. Use <<var_nfs_mask>> as the Subnet Mask

83. Click the Routing Tab

84. Enter <<var_t002_access_gw>> as the Default Gateway

85. Click OK

86. Proceed with the configuration using the defaults or your datacenter best practices.

## Enabling data traffic on vHBA3 and vHBA4

Now that the Cisco FNIC driver is loaded in the operating system, vHBA3 and vHBA4 are also logged into the MDS switches. For best performance of a SAP HANA Scale-Up system it is recommended to move the paths for the data volume from the single storage path zoning into the multi paths zoning.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_t002-hana1-data>> vsan 10
zone name <<var_zone_t002-hana1-data>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:0a
   exit

zoneset name CRA-EMC-A vsan 10
member <<var_zone_t002-hana1-data>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_t002-hana1 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0b
…
```

```
zone name zone_t002-hana1-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0a

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-hana1
  zone zone_t002-hana1-data
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
Copy run start
```

## Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_t002-hana1-data>> vsan 20
zone name <<var_zone_t002-hana1-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:0a
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_t002-hana1-data>>
exit
zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_t002-hana1 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0b

zone name zone_t002-hana1-data vsan 20
```

```
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0a

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-hana1
  zone zone_t002-hana1-data
CRA-EMC-B#
```

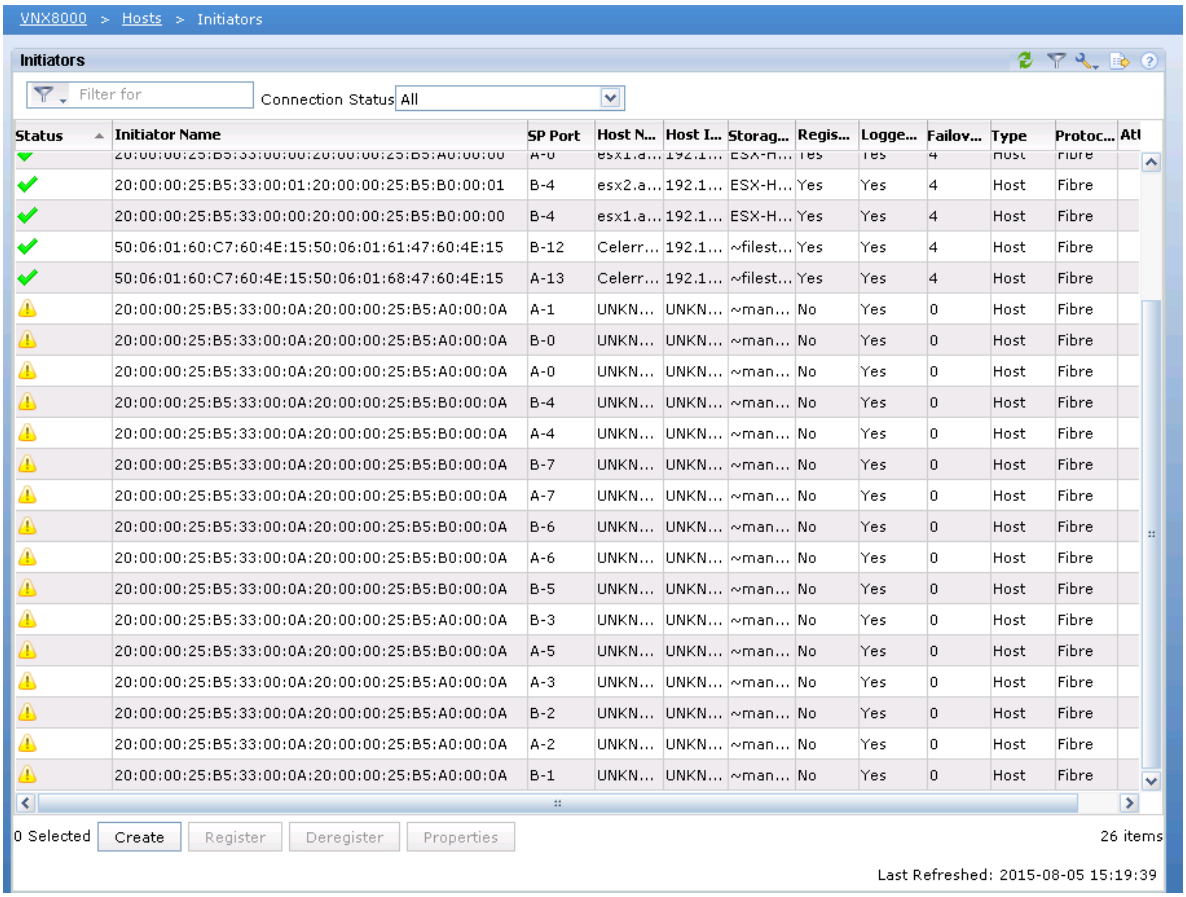
4. Save the running configuration as startup configuration:

```
copy run start
```

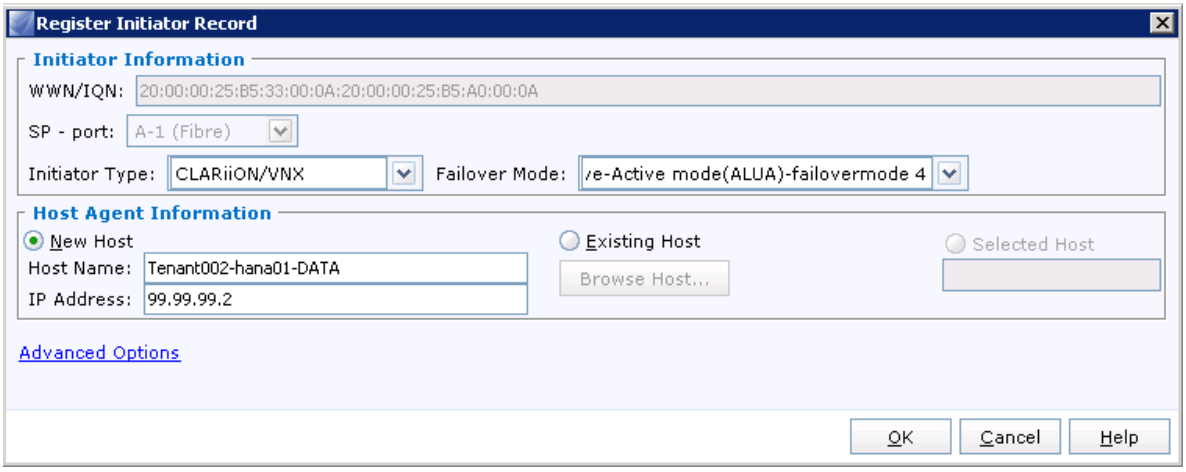
## Configure EMC VNX

### Register Host

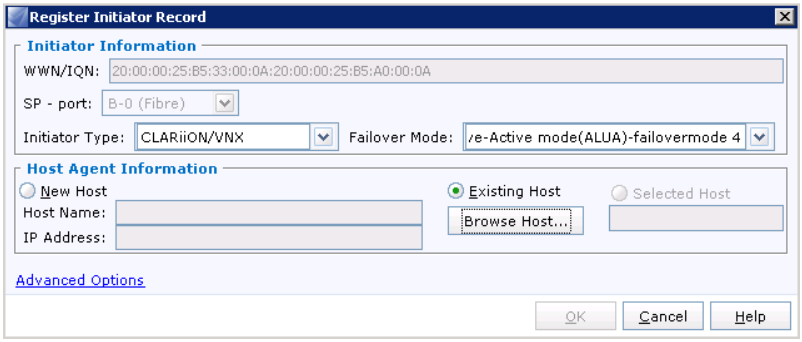
1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators



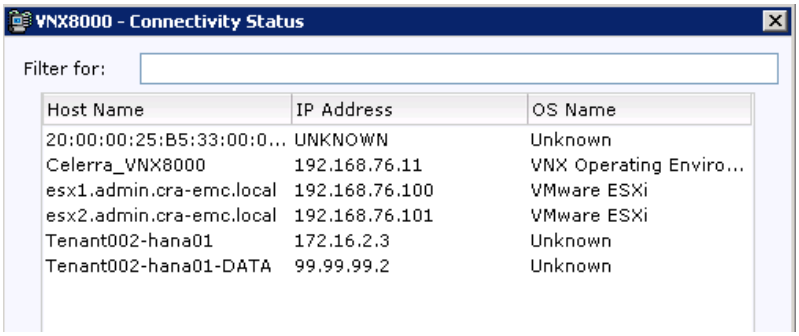

2. Select one of the unregistered entries for the host Tenant002-hana01, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Active mode(ALUA)-failovermode 4 as the Failover Mode
5. Enter <<var_ucs_t002_hana1_sp_name>>-data as the Host Name (indicates the relationship to the Service Profile)
6. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
7. Click OK
8. Click Yes
9. Click OK
10. Click OK




11. Select the second Entry for this host <<var_ucs_t002_hana1_sp_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and click Browse Host




15. Select <<var_ucs_t002_hana1_sp_name>>-data and click OK



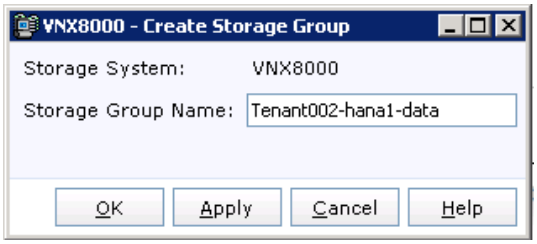

16. Click OK
17. Click Yes

18. Click OK
19. Click OK

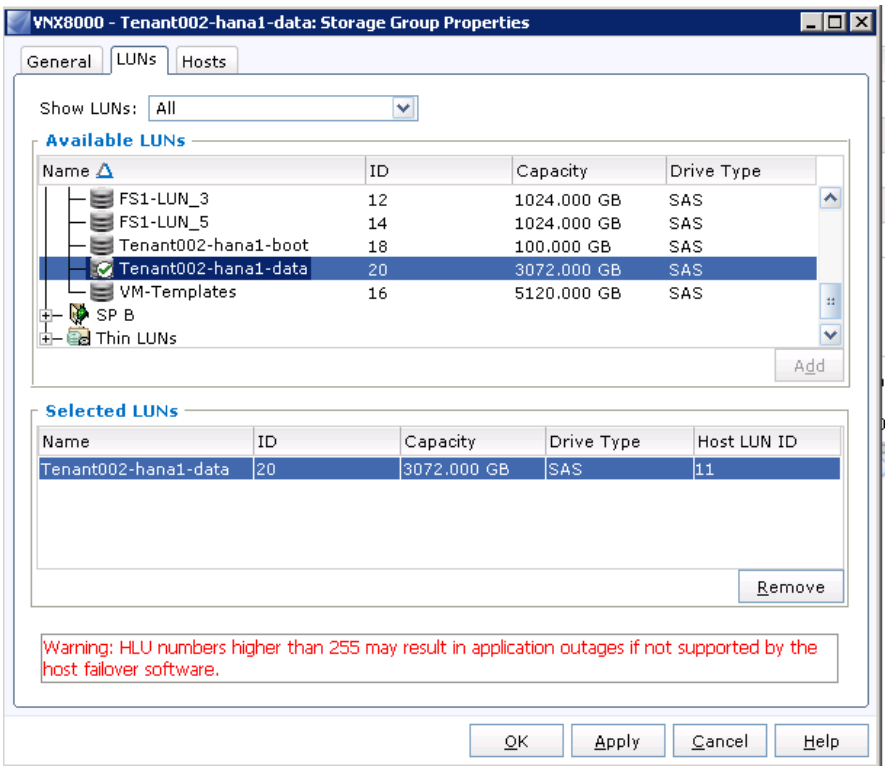
Repeat Step 10 to 18 for all remaining paths of this server in the list.

### Create Storage-Group

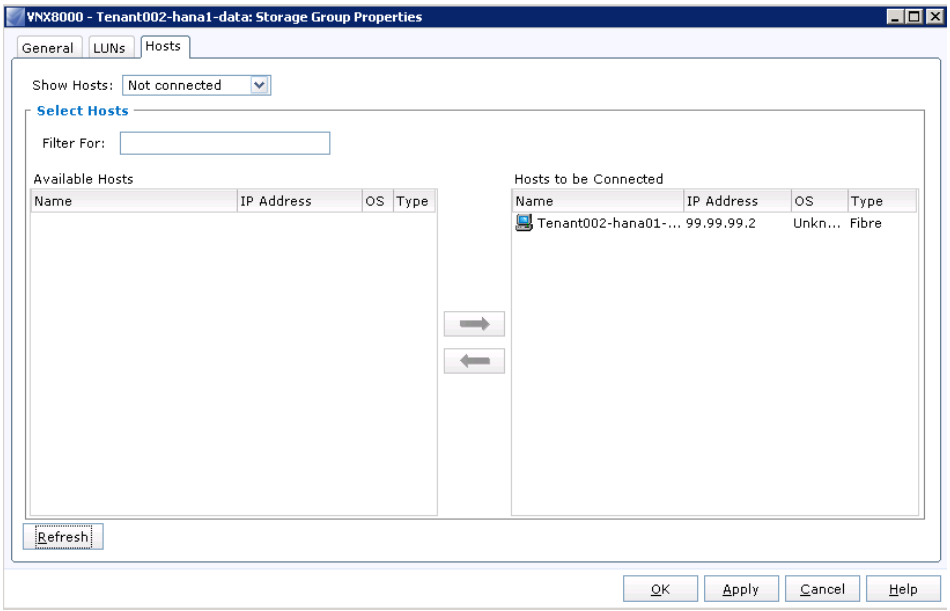
1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t002_hana1_sp_name>>-data as the Name
4. Click OK
5. Click Yes



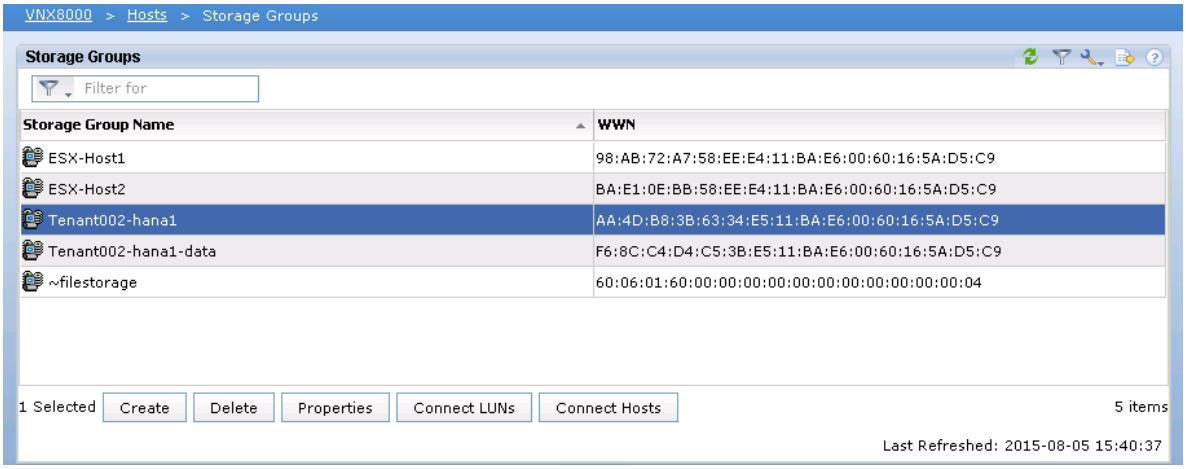

6. Click Yes
7. Select All from the Show LUNs Drop-Down menu, click OK
8. Select the Data-LUN from the list of LUNs and click Add
9. Select 11 as the Host LUN ID for <<var_ucs_t002_hana1_sp_name>>-data (the same ID as before)




10. Click the Hosts tab
11. Select <<var_ucs_t002_hana1_sp_name>>-data and click the  Icon
12. Click OK
13. Click Yes
14. Click OK



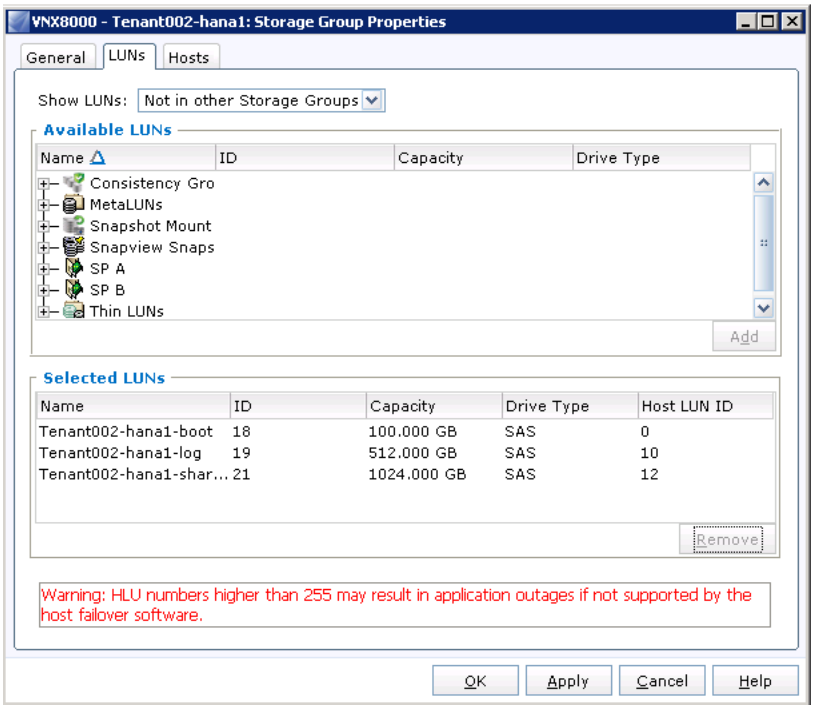

15. Back on the list of Storage Groups, select <<var_ucs_t002_hana1_sp_name>>, click Properties




16. Click the LUNs Tab

17. Select the data LUN from the below list “Selected LUNs”

18. Click Remove




19. Click OK
20. Click Remove LUNs from storage group
21. Click OK
22. Go back to the server and boot/reboot the system

## Configure SUSE Linux for SAP HANA

1. Use a SSH client to logon to the installed system with the user root and the password <<var_mgmt_passwd>>.
2. Register the System at SUSE to get latest Patches.



The system must have access to the internet to proceed with this step.

```
suse_register -i -r -n -a email= <<email_address>> -a regcode-
sles=<<registration_code>>
```

3. Update the system with the following command



The system must have access to the internet to proceed with this step.

```
zypper update
```

Please follow the on-screen instructions to complete the update process. It is required to reboot the server and login to the system again.

4. Configure the Network Time Protocol with the following step

```
vi /etc/ntp.conf


server <<var_global_ntp_server_ip>>
fudge <<var_global_ntp_server_ip>> stratum 10
keys /etc/ntp.keys
trustedkey 1
```

5. Create User-Group sapsys

```
groupadd –g 401 sapsys
```

6. Change the permissions for the SAP HANA file systems

```
chgrp –R sapsys /hana
chmod –R 775 /hana
```

7. We recommend to disable Transparent Huge Pages and the swappiness on the system

```
vi /etc/init.d/after.local


 #!/bin/bash
# (c) Cisco Systems Inc. 2014
echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status
# set sappiness to 30 to aviod swapping
echo "Set swappiness to 30 to avoid swapping"
echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status
```

8. Based on different SAP Notes multiple entries in /etc/sysctl.conf are required

```
vi /etc/sysctl.conf


#SAP Note 1275776
vm.max_map_count = 2000000
```

```
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
net.ipv4.tcp_slow_start_after_idle = 0
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_slot_table_entries = 128
# Memory Page Cache Linit Feature SAP Note 1557506
vm.pagecache_limit_mb = 4096
vm.pagecache_limit_ignore_dirty = 1
```

9. Edit boot loader configuration file /etc/sysconfig/bootloader. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

```
intel_idle.max_cstate=0
```

10. Append the “intel_idle.max_cstate=0 processor.max_cstate=0” value to the kernel's parameter line in /boot/grub/menu.lst – 3.0.xxx-x.xx is the placeholder for your Kernel patch version

```
vi /boot/grub/menu.lst


title SLES for SAP Applications - 3.0.XXX-X.XX
root (hd0,0)
```

```
kernel /boot/vmlinuz-3.0.XXX-X.XX-default root=/dev/sda2 resume=/dev/sda1
splash=silent showopts intel_idle.max_cstate=0 processor.max_cstate=0

initrd /boot/initrd-3.0.XXX-X.XX-default
```

11. Reboot the server before continue with the next steps

```
reboot
```

## Install SAP HANA

1. Mount the Software share to access the SAP HANA installation files

```
mkdir /software

mount 172.30.113.11:/FS_Software /software
```

Please use the SAP HANA Installation guide provided by SAP for the software revision you plan to install. The program to install SAP HANA Revision 100 is hdblcm located in the directory <Installation source>/DATA_UNITS/HDB_LCM_LINUX_X86_64.

```
cd /software/SAP/SPS10/REV100/DATA_UNITS/HDB_LCM_LINUX_X86_64

./hdblcm
```

2. The text-based installation menu launches

```
Select 1 for Install new system


Select 2 for All Components


Enter Installation Path: /hana/shared : Press Enter

Enter local host name: t001-vhana-0: Press Enter

Do you want to add additional hosts to the system? N

Enter SAP HANA System ID: <<var_t002_hana_sid>>

Enter Instance Number:  <<var_t002_hana_nr>>

Select Database mode 1 for single_container

Select System Type: 1 for Production

Enter Location for Data Volumes /hana/data/T02: Press Enter
```

Enter Location for Log Volumes /hana/log/T02: Press Enter

Restrict maximum memory allocation n : Press Enter

Enter Certificate Host name t002hana01: Press Enter

Enter SAP Host Agent User (sapadm) password: <<var_mgmt_passwd>>

Confirm password

Enter System Administrator (t02adm) password: <<var_mgmt_passwd>>

Confirm password

Enter System Administrator Home Directory /usr/sap/T02/home : Press Enter

Enter System Administrator Login shell /bin/sh: Press Enter

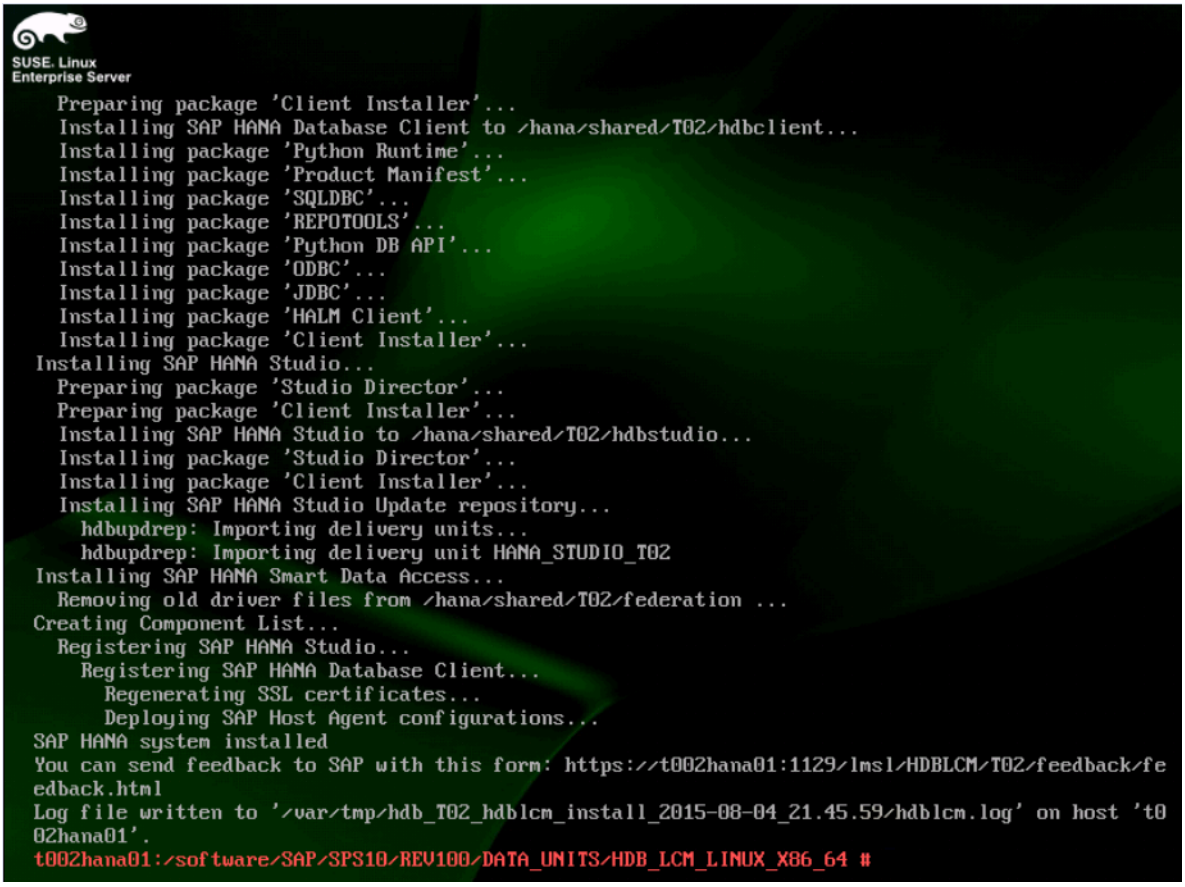
Enter System Administrator User id 1000 : Press Enter

Enter Database User (SYSTEM) Password : <<var_t002_hana_sys_passwd>>

Confirm Passwd

Restart instance after machine reboot n : Press Enter

Do you want to continue : y



After the installation is finished please check the status of the SAP HANA database

3. Change the user to <SID>adm (here t02adm) with the command su

```
su – t02 adm
t002hana01:t02adm>
```

4. Use the commands HDB info and HDB version to check the installation

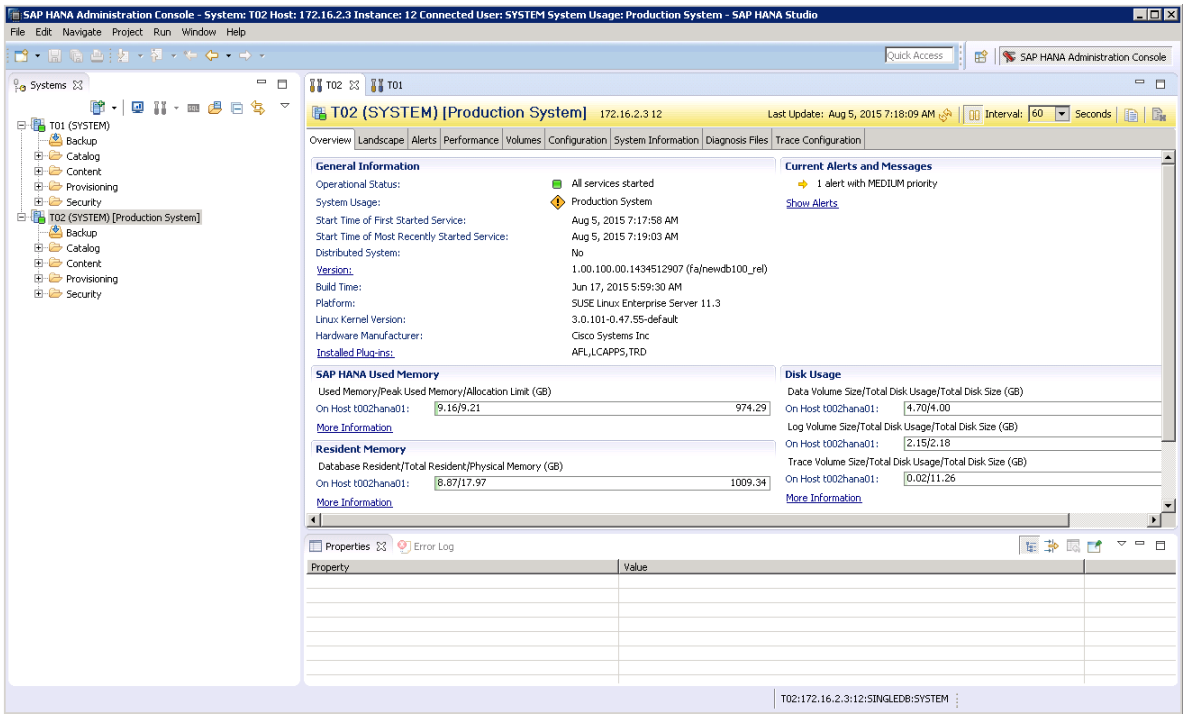
```
t002hana01:t02adm> HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
t01adm    9841  9840  0.2 108432  1956 -sh
t01adm    9898  9841  0.0 114064  1972  \_ /bin/sh /usr/sap/T02/HDB01/HDB info
t01adm    9925  9898  0.0 118036  1564      \_ ps fx -U t02adm -o user,pid,ppid,
t01adm    9404  9403  0.0 108468  1976 -sh
t01adm    7548     1  0.0  22196  1544 sapstart pf=/hana/shared/T02/profile/T02_
t01adm    7556  7548  0.0 549900 286996  \_ /usr/sap/T02/HDB01/t002hana01/trac
t01adm    7574  7556  0.8 11261988 1242232      \_ hdbnameserver
t01adm    7682  7556  3.6 3301968 744264      \_ hdbcompileserver
t01adm    7685  7556 71.0 10535368 8059748      \_ hdbpreprocessor
t01adm    7708  7556 23.2 12699580 8826808      \_ hdbindexserver
t01adm    7711  7556  2.1 4196404 1118644      \_ hdbxsengine
t01adm    8150  7556  0.6 3088496 414320      \_ hdbwebdispatcher
t01adm    4276     1  0.1 868164 61956 /usr/sap/T02/HDB12/exe/sapstartsrv pf=/ha
t002hana01:t02adm>
t002hana01:t02adm> HDB version
HDB version info:
  version:             1.00.100.00.1434512907
  branch:              fa/newdb100_rel
  git hash:            e88f645daf7c574022a4f10eff99ca4016009d14
  git merge time:      2015-06-17 05:48:27
  weekstone:           0000.00.0
  compile date:        2015-06-17 05:59:30
```

```
    compile host:         ld7272
    compile type:         rel
t002hana01:t02adm>
```

## Test the Connection to SAP HANA

Use the SAP HANA Studio on a system with network access to the installed SAP HANA system and add the SAP HANA Database. The information you is as follows:

- Hostname or IP address <<var_t002_access_ip>>
- SAP HANA System Number <<var_t002_hana_nr>>
- SAP HANA database user (default: SYSTEM)
- SAP HANA database user password <<var_t002_hana_sys_passwd>>




# SAP HANA Scale-Up System with Multi Database Container

This is a new deployment methodology of SAP HANA introduced with Service Pack 9 to create a very flexible way to configure and use the resources for multiple databases. The database Container sharing the binaries and the file systems. Every container can be operated independent from the other containers (start, stop, backup, restore). The use of a single operating system and SAP HANA binaries keeps the operational costs lower compared to a virtualized SAP HANA option where every SAP HANA system requires a own Operating System and SAP HANA installation.

Please read the documentation from SAP about the SAP HANA Multi Database Container installation and configuration before you start the installation. It is required to understand the configuration requirements around network and security to deploy a SAP HANA MDC system on a shared infrastructure.

The high-level step for this use case are as follows:

1. Create the access VLAN on Cisco Nexus 9000, and Cisco UCS.
2. Create Service Profile on Cisco UCS.
3. Define LUNs on the EMC VNX, register the server and configure the Storage-Group.
4. Install and Configure the Operating System.
5. Install SAP HANA.
6. Test the connection to the SAP HANA database.

## Workload Definition

This SAP HANA system requires 1TB main memory, that it is for Production, and has to run on SUSE Linux Enterprise.

This SAP HANA system is defined for multiple small databases as containers in a single SAP HANA system – Multi Database Container option. The minimum size of the main memory is 1TB. The containers are only for Sand-Box and Test systems.

## Requirements

For a SAP HANA system with Multi Database Containers on a regular Scale-Up configuration, the networks required are the access network and the storage network (in this case via Fibre Channel). To access the installation, sources for SAP HANA and other applications the access to the NFS share on the EMC VNX storage is also configured; this can be temporary only until all applications are installed. All other networks are optional. For this use case no optional network is used. This is the first system for SAP HANA MDC, so no existing network definition can be used. As this is for Non-Production the relaxed storage requirements apply. The following configuration is required:

Network: 1x Access Network with >=1 Gbit/sec; This is a shared network for all Clients accessing the SAP HANA MDC system

1x NFS-Access Network (to access the installation sources)

Storage: 512GB for /hana/log, 1.5TB for /hana/data, 1TB for /hana/shared

An average of 300 MB/sec throughput can be used as the baseline. Dependent on the use case it can be less (default analytics) or much more (heavy Suite on HANA)

Memory: 1 TB

CPU: 4x Intel Xeon E7 v2 CPUs (Ivy Bridge)

## Switch Configuration

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

1. On each Nexus 9000, enter configuration mode:

```
config terminal
```

2. From the configuration mode, run the following commands:

```
vlan <<var_mdc_access_vlan_id>>
name MDC-Access
```

3. Add the VLAN to the VPC Peer-Link:

```
interface po1
switchport trunk allowed vlan <<var_mdc_access_vlan_id>>
```

4. Add the VLAN to the Port Channels connected to the Cisco UCS:

```
interface po13,po14
switchport trunk allowed vlan <<var_mdc_access_vlan_id>>
```

5. Add the VLAN to the data center uplink

```
interface po99
switchport trunk allowed vlan add <<var_mdc_access_vlan_id>>
```

6. Save the running configuration to start-up:

```
copy run start
```

7. Validate the configuration:

```
#show vpc
…
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,2031,2034,3001,3002,3003
```

```
vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
11   Po11   up     success     success                    76,177,199,
                                                          2031,2034
12   Po12   up     success     success                    76,177,199,
                                                          2031,2034
13   Po13   up     success     success                    3001-3003
14   Po14   up     success     success                    3001-3003
…

show vlan id 3003
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3003 MDC-Access                       active    Po1, Po13, Po14, Po99, Eth1/1
                                                Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                Eth1/9, Eth1/10, Eth1/15
                                                Eth1/16, Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3003 enet         CE

Remote SPAN VLAN
----------------
Disabled

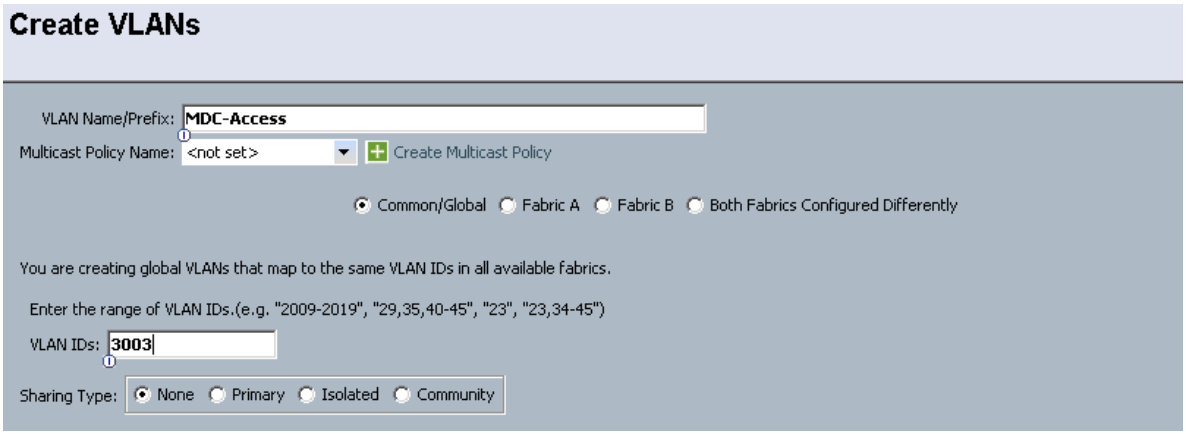
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

## Cisco UCS Configuration

### Configure VLANs and VLAN-Group Membership

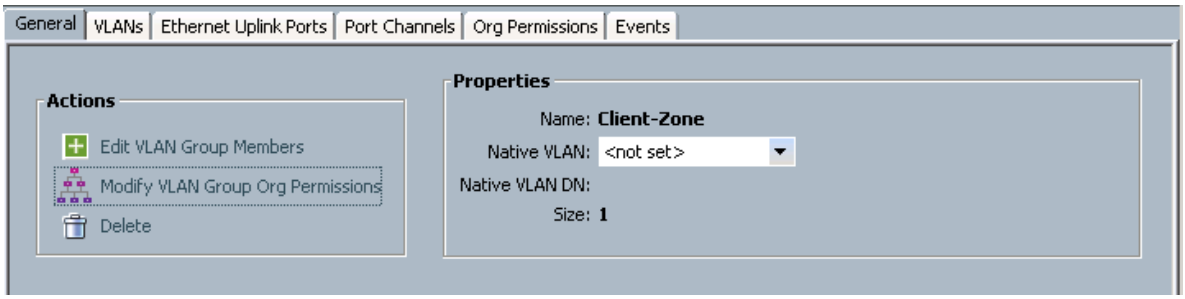
To create a VLAN, complete the following steps:

1. Log in to Cisco UCS Manager.
2. Go to LAN Tab > LAN Cloud > VLANs.
3. Right-click > Create VLANs.
4. Enter <<var_ucs_mdc_access_vlan_name>> as the VLAN Name.
5. Enter <<var_mdc_access_vlan_id>> as the VLAN ID.
6. Click OK.
7. Click OK.

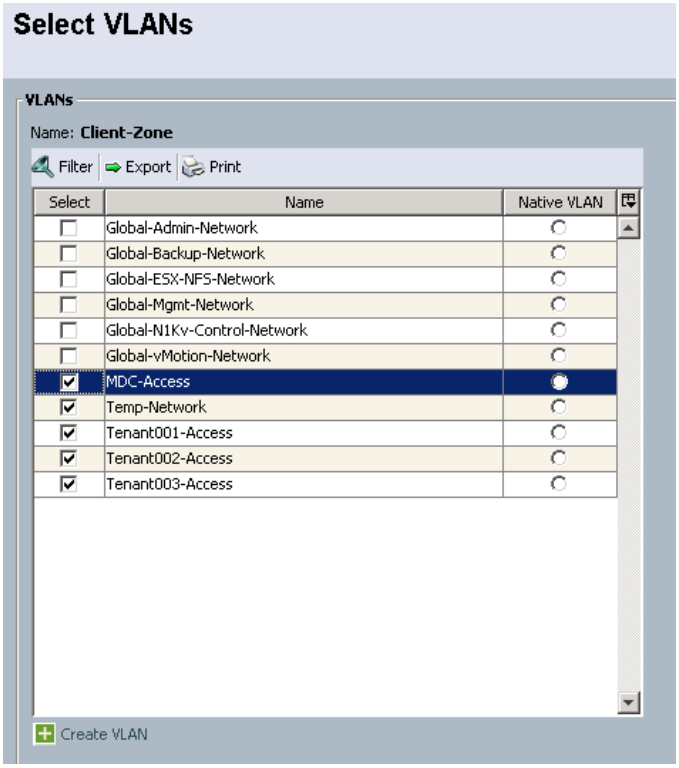



8. Go to LAN Tab > LAN Cloud > VLAN Groups.
9. Select VLAN group Client-Zone.
10. Click the Info Icon 

on the right side of the list.
11. Click Edit VLAN Group Members.




12. Select <<var_ucs_mdc_access_vlan_name>>.
13. Click Finish.

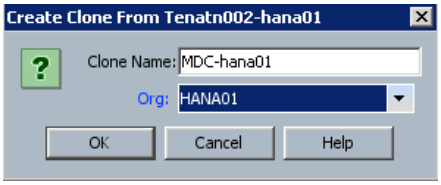



14. Click OK.

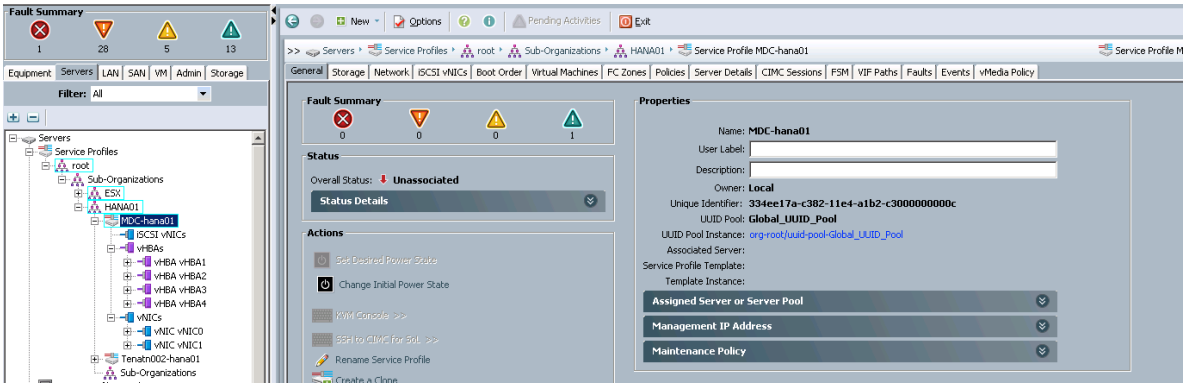
## Create Service Profile for a Cisco UCS B460 M4 or C460 M4 Server

1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. Select an existing Service Profile in the Sub-Organization
3. Click Create a Clone
4. Enter <<var_ucs_mdc1_sp_name>> as the Name
5. Select <<var_ucs_hana01_org>> as the Org

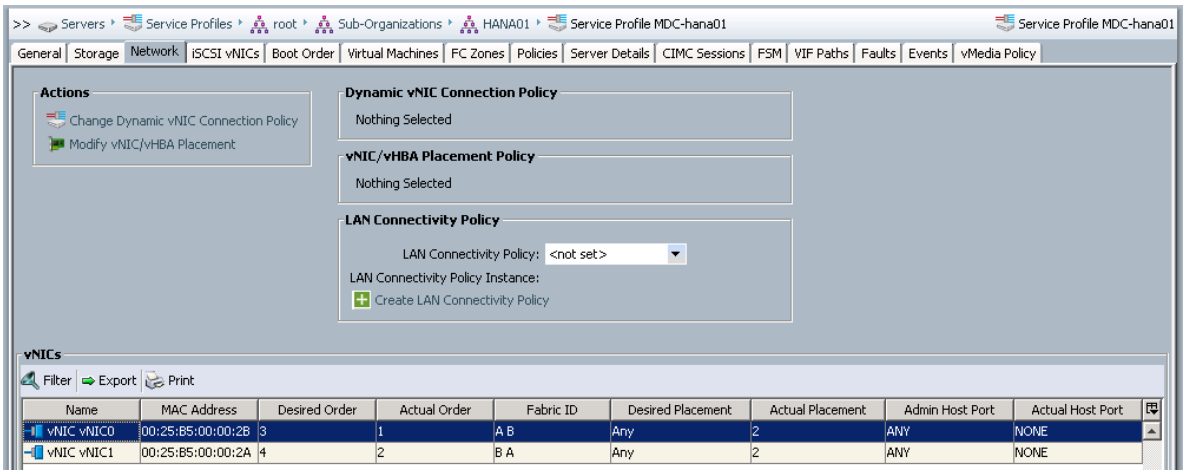
6. Click OK




7. The Service Profile is available immediately

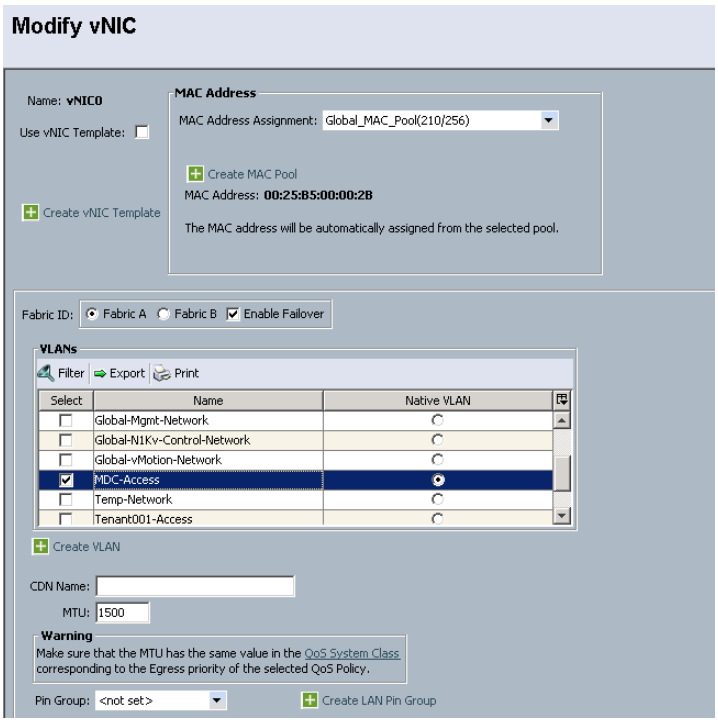



8. Select the Service Profile, click Change Service Profile Association
9. Select “Select existing Server” from the Server Assignment drop-down menu
10. Select a server that meets the requirements, click OK
11. Click Yes
12. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.
13. Click the Network Tab and select vNIC0
14. Click the Modify Icon



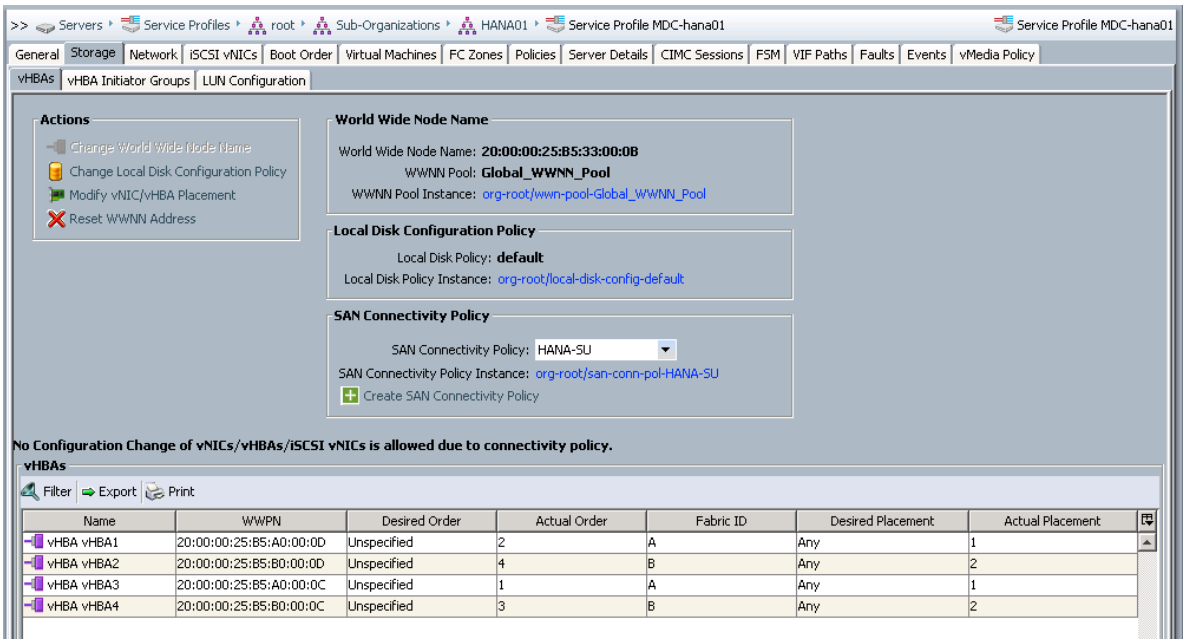

15. Select <<var_ucs_mdc_access_vlan_name>> and make it the Native VLAN

16. Click OK




17. Click Save Changes. In some cases the system requires a reboot to activate this change. This is indicated through the Pending Activities.

18. Click the Storage Tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX




## Configure Cisco MDS Switches

For every Service Profile in the Cisco UCS one or more SAN Zones are required per Cisco MDS switch.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_MDC-hana01>> vsan 10


zone name <<var_zone_MDC-hana01>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:0d
   exit


zoneset name CRA-EMC-A vsan 10
member <<var_zone_MDC-hana01>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

…
zone name zone_MDC-hana01 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0d

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
```

```
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_MDC-hana01
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_MDC-hana01>> vsan 20

zone name <<var_zone_MDC-hana01>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:0d
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_MDC-hana01>>
exit

zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
```

```
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_MDC-hana01 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0d

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_MDC-hana01
CRA-EMC-B#
```

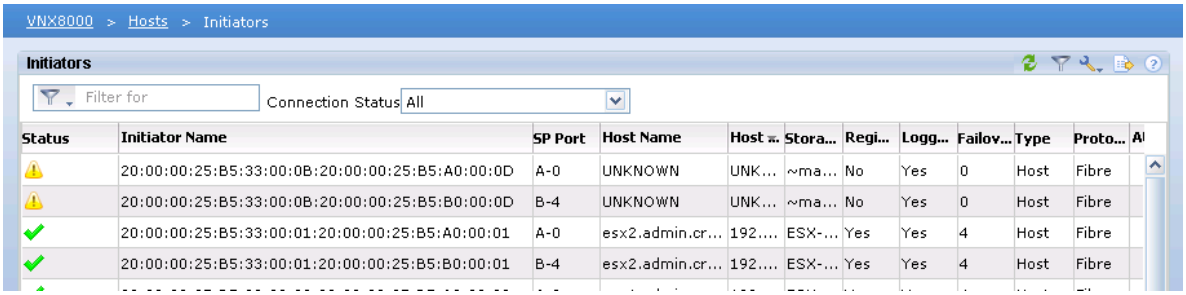
4. Save the running configuration as startup configuration

```
Copy run start
```

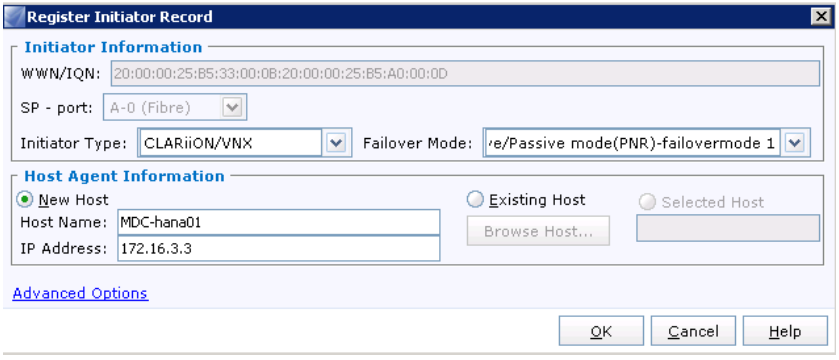
## Configure EMC VNX

### Register Host

1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators



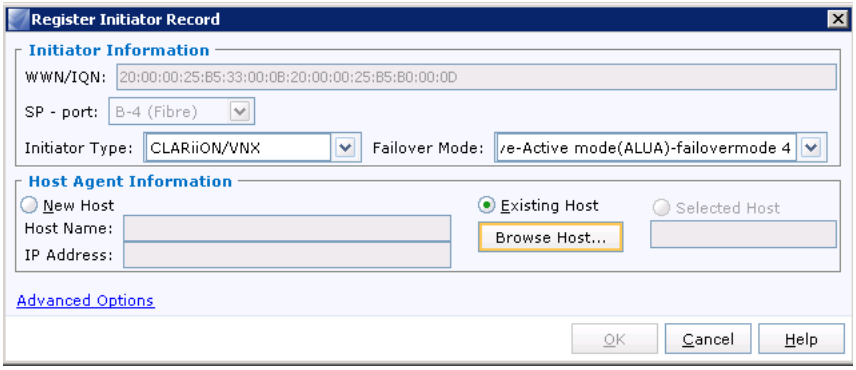

2. Select one of the unregistered entries for the host MDC-hana01, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
5. Enter <<var_ucs_mdc_hana1_name>> as the Host Name (indicates the relationship to the Service Profile)
6. Enter <<var_mdc_hana1_access_ip>> as the IP Address
7. Click OK
8. Click Yes
9. Click OK
10. Click OK



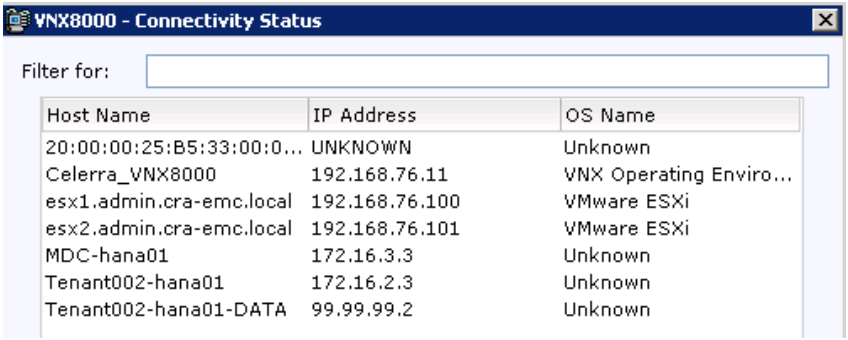

11. Select the second Entry for this host <<var_ucs_mdc_hana1_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type

13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

14. Select Existing Host and Click Browse Host




15. Select <<var_ucs_mdc_hana1_name>> and click OK




16. Click OK

17. Click Yes

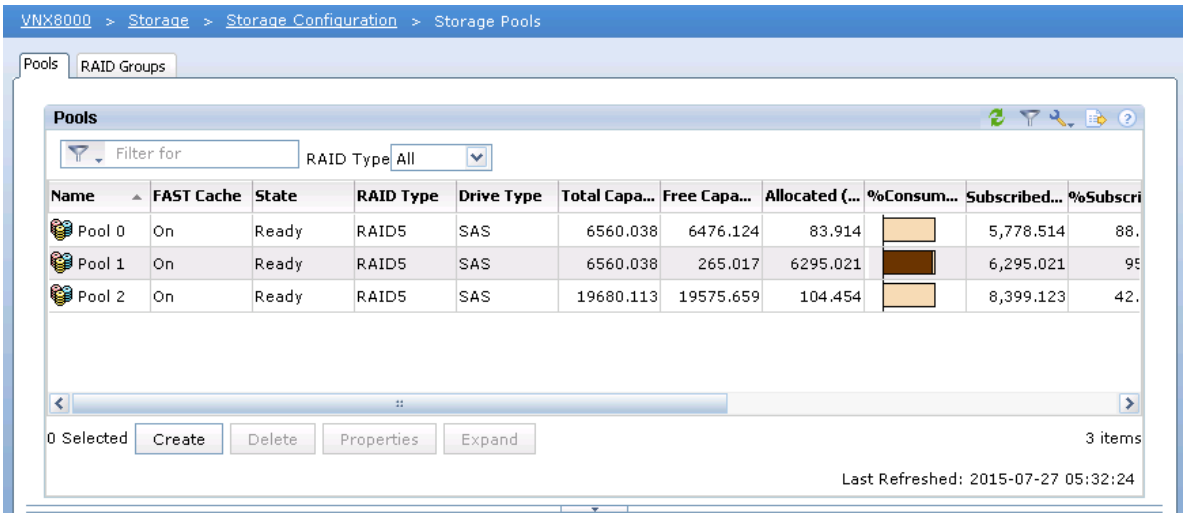
18. Click OK

19. Click OK

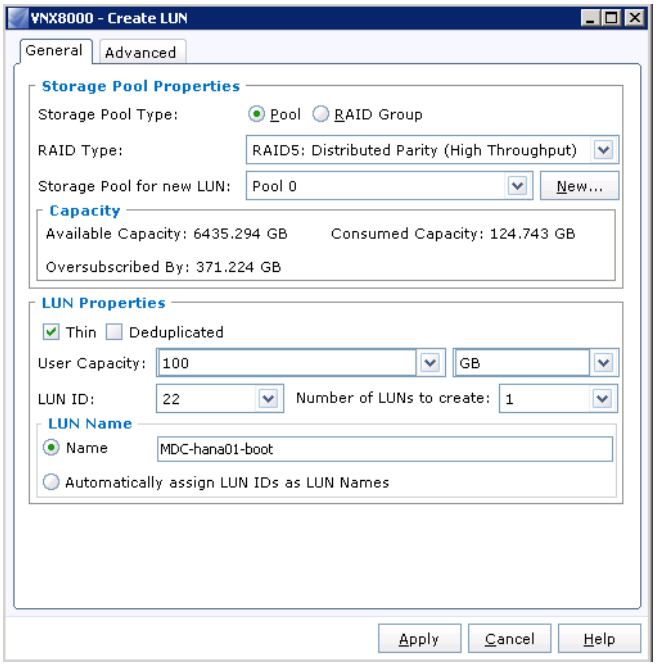
## Create LUNs

To create LUNs, complete the following steps:

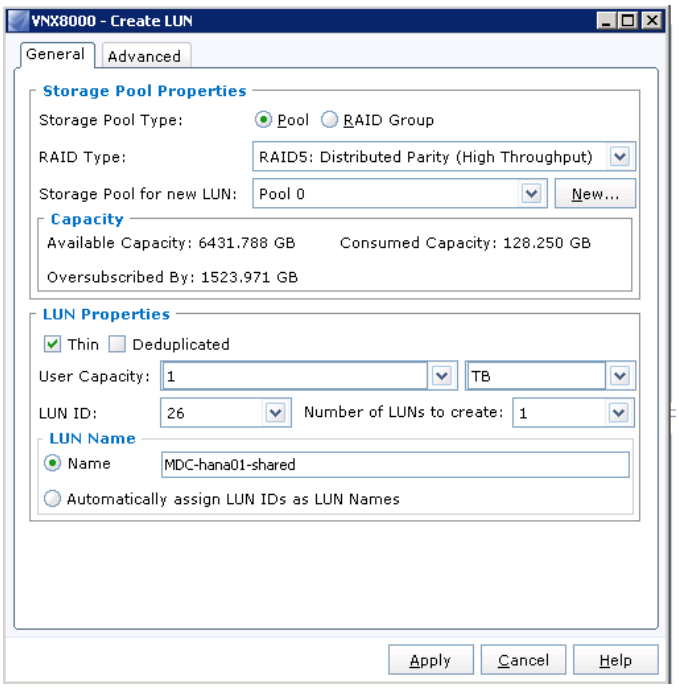
1. Navigate to Storage > Storage Pool



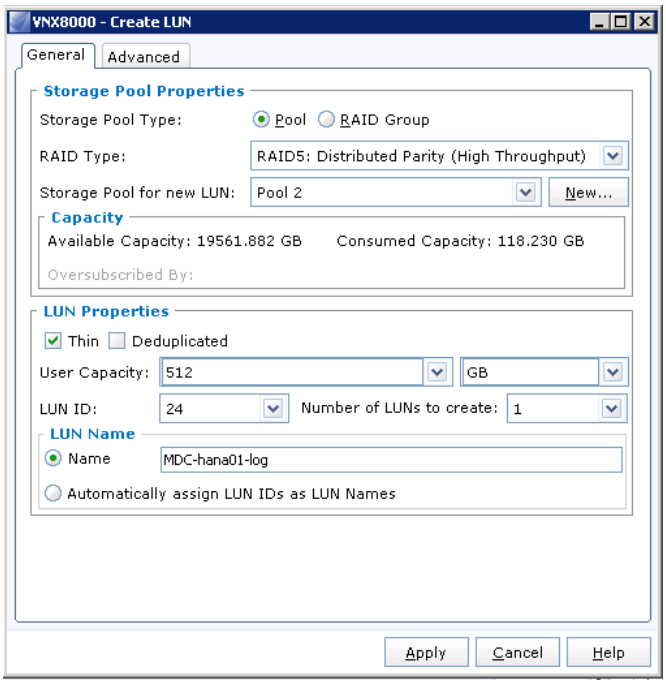

2. Right-click Pool 0
3. Select Create LUN
4. Enter 100 GB as the User Capacity
5. Click Name and enter <<var_ucs_mdc_hana1_name>>-boot
6. Click Apply
7. Click Yes
8. Click OK



9. Enter 1 TB as the User Capacity
10. Click Name and enter <<var_ucs_mdc_hana1_name>>-shared
11. Click Apply
12. Click Yes
13. Click OK




14. Click Cancel
15. Right-click Pool 2
16. Select Create LUN
17. Enter 512 GB as the User Capacity
18. Click Name and enter <<var_ucs_mdc_hana1_name>>-log
19. Click Apply
20. Click Yes
21. Click OK



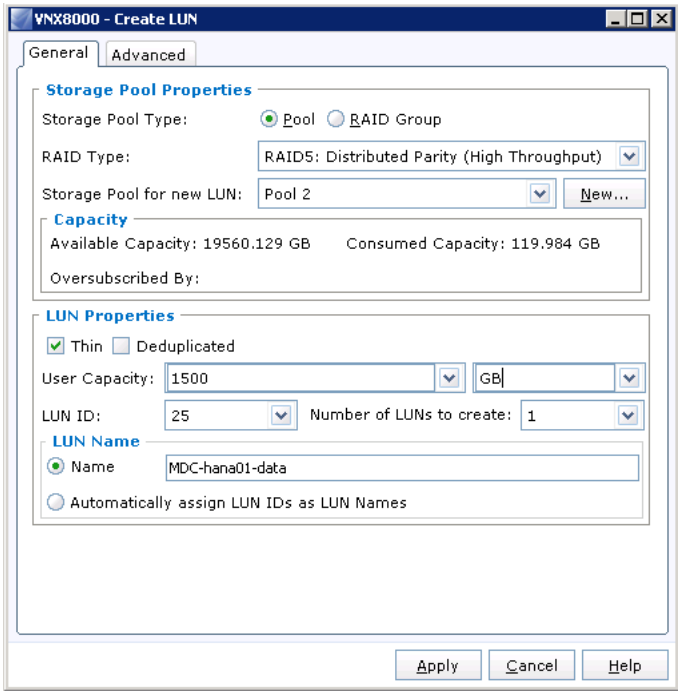

22. Enter 1.5 TB as the User Capacity

23. Click Name and enter <<var_ucs_mdc_hana1_name>>-data

24. Click Apply

25. Click Yes

26. Click OK

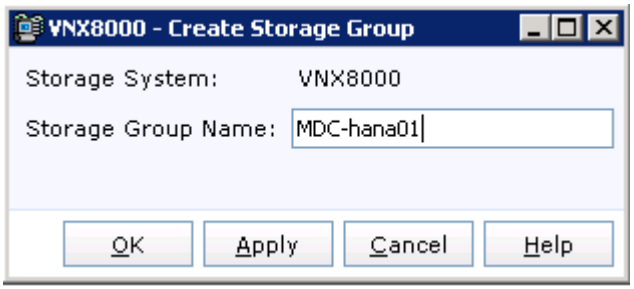



27. Click Cancel

## Create Storage-Group

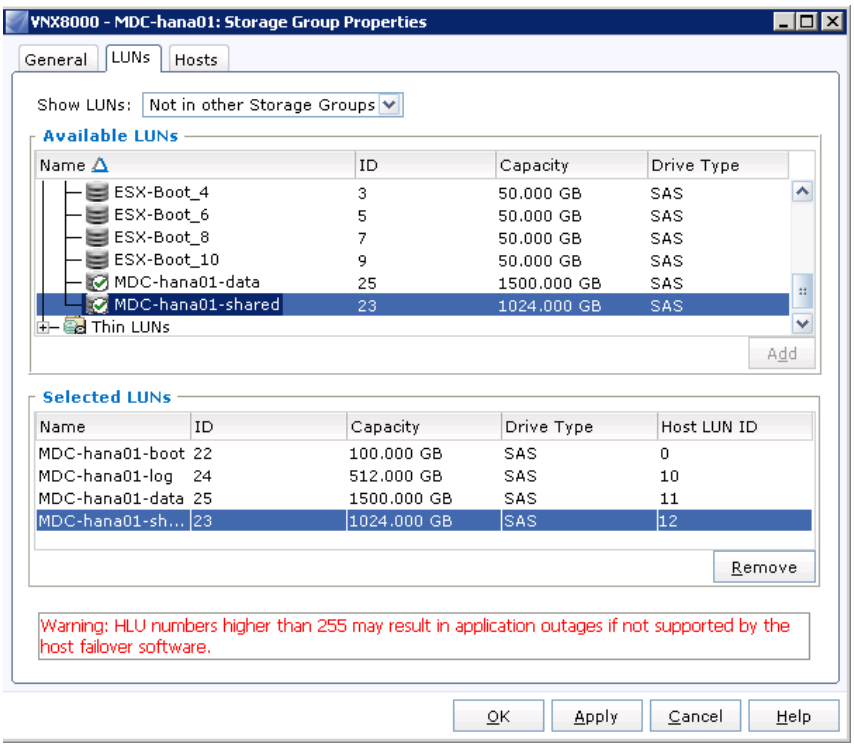
To create a storage group, complete the following steps:

1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_mdc_hana1_name>> as the Name
4. Click OK
5. Click Yes

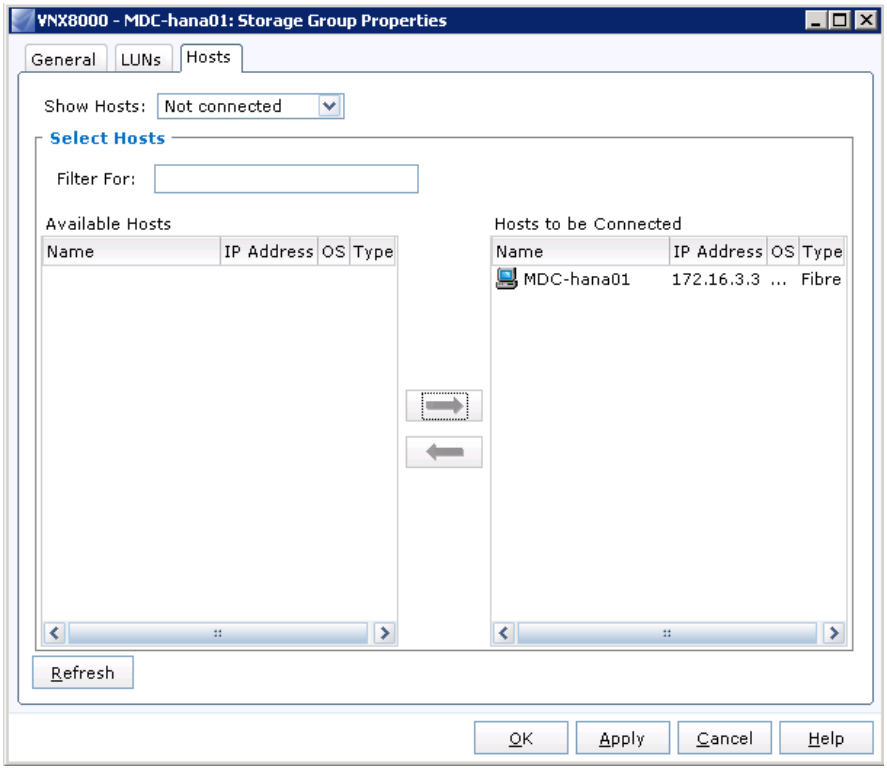



6. Click Yes
7. Select one of the four created LUNs and click Add

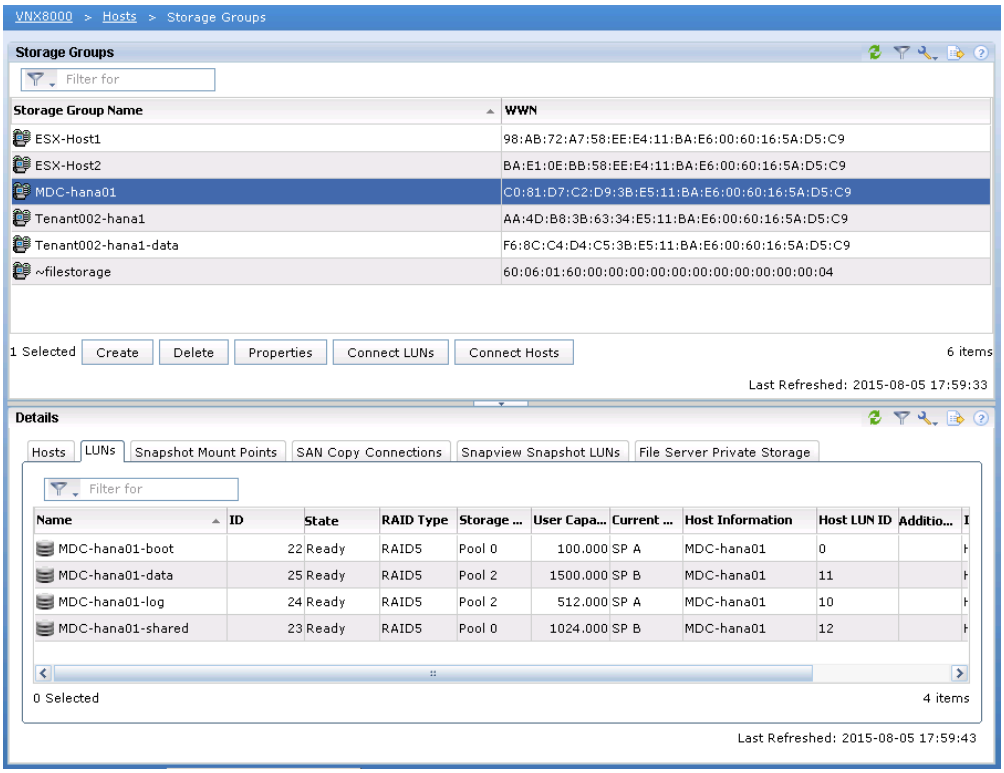
8. Repeat this for the other LUNs excepting the data LUN
9. Select 0 as the Host LUN ID for <<var_ucs_mdc_hana1_name>>-boot
10. Select 10 as the Host LUN ID for <<var_ucs_mdc_hana1_name>>-log
11. Select 11 as the Host LUN ID for <<var_ucs_mdc_hana1_name>>-data
12. Select 12 as the Host LUN ID for <<var_ucs_mdc_hana1_name>>-shared
13. Click Apply
14. Click Yes
15. Click OK




16. Click the Hosts Tab
17. Select <<var_ucs_mdc_hana1_name>> and click  Icon
18. Click OK
19. Click Yes
20. Click OK



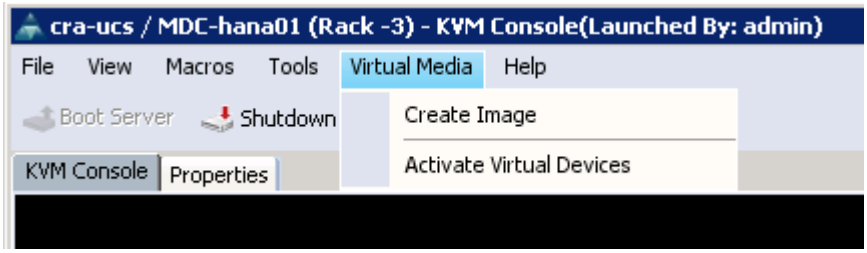

The Result is shown below:



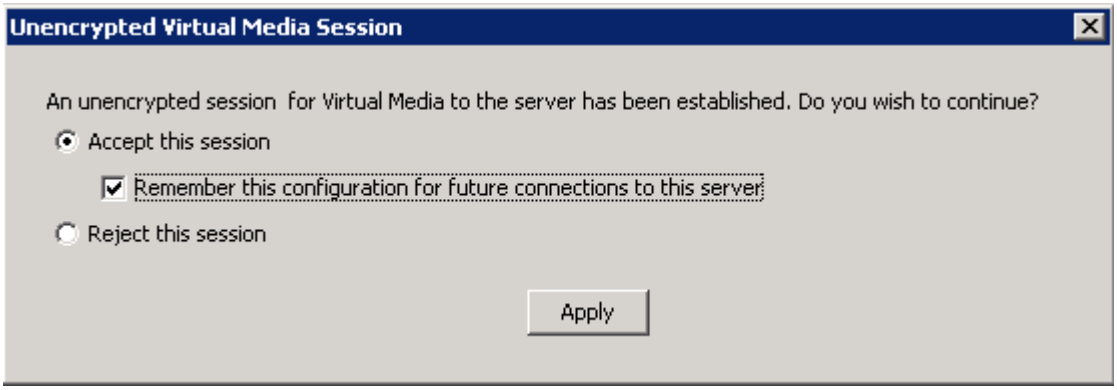
## Install the Operating System

To install the operating system, complete the following steps:

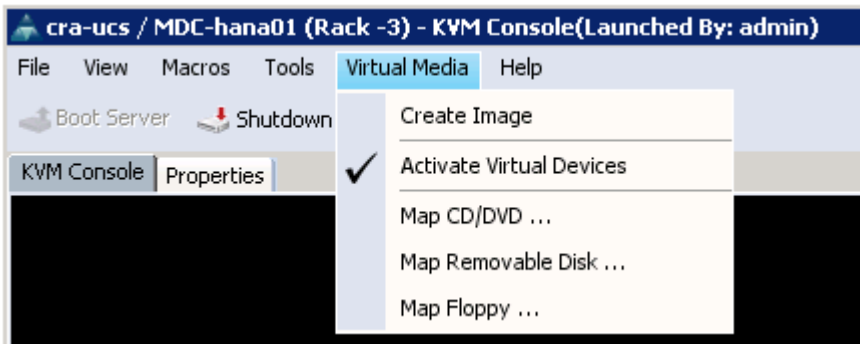
1. Return to the Cisco UCS Manager and select the Service Profile <<var_ucs_mdc_hana1_name>>
2. Click KVM Console
3. Click the Menu Virtual Media
4. Select Activate Virtual Devices




5. In the new Window, Select Accept this Session. If you like you can also select the Check-Box to Remember this setting
6. Click Apply



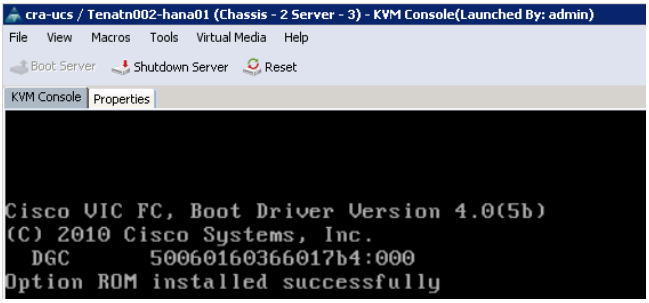

7. Click again on the Menu Virtual Media
8. Select Map CD/DVD...




9. Click Browse, and select the SUSE Linux Enterprise for SAP Installation ISO

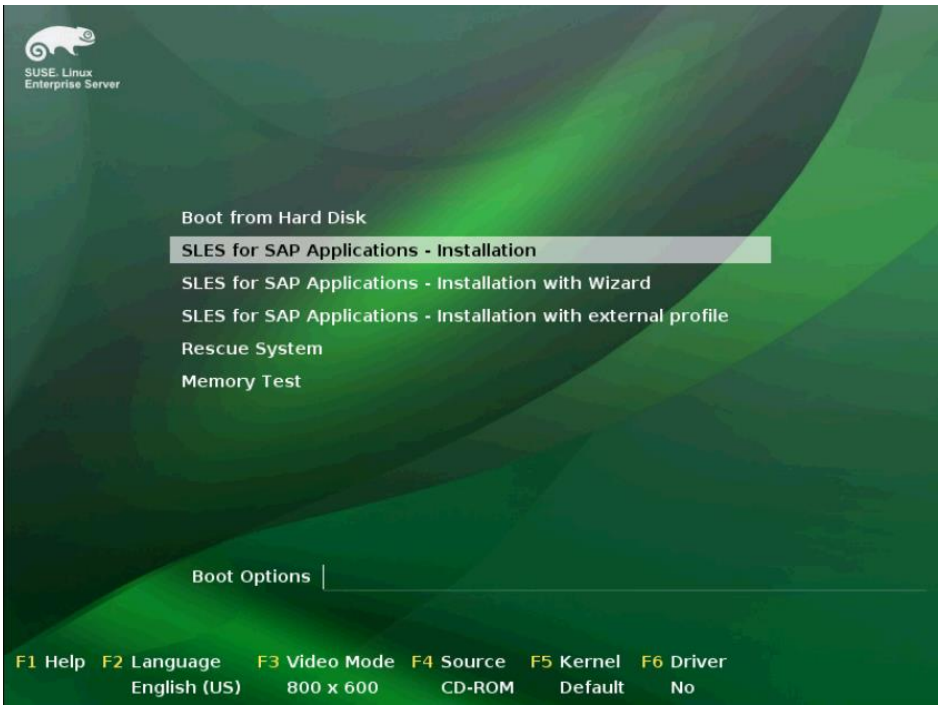
10. Click Map Device

11. Click Reset to reset the server. This will force the system to scan the SAN and get access to the LUNs on the EMC VNX.




12. The System will automatically boot from the ISO image

13. Select SLES for SAP Applications – Installation and press Enter

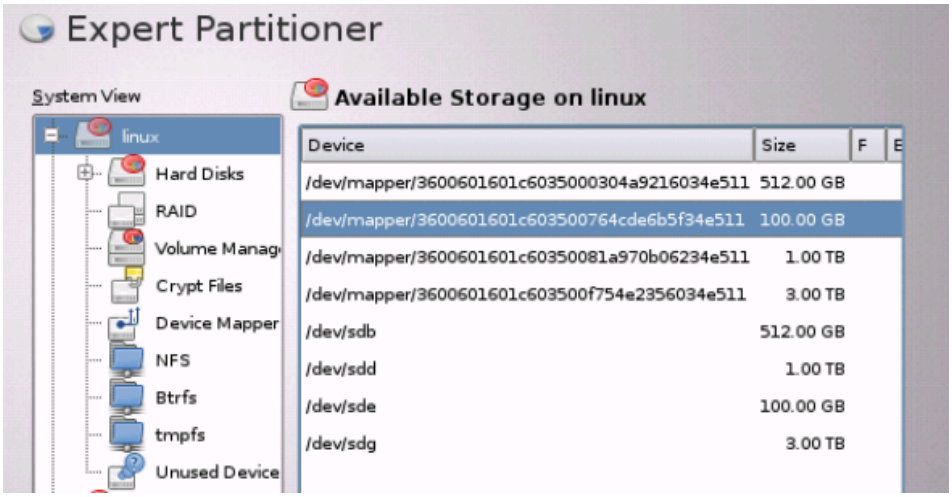



14. Follow the instructions on screen and select Yes to activate multipath

15. Please change the Partitioning as following:

16. Select Custom Partitioning (for Experts), click Next

17. Select the /dev/mapper device with the size of 100GB



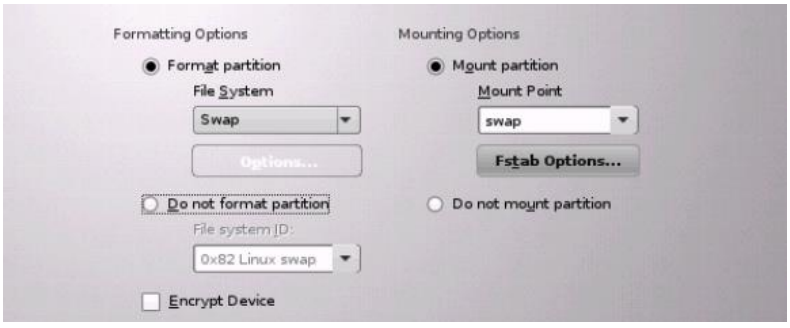

18. Right-click the device, select Add Partition.

19. Select Primary Partition, click Next

20. Use 98GB as the Size, click Next
21. Use Ext3 as the File System
22. Use / as the Mount Point
23. Click Finish

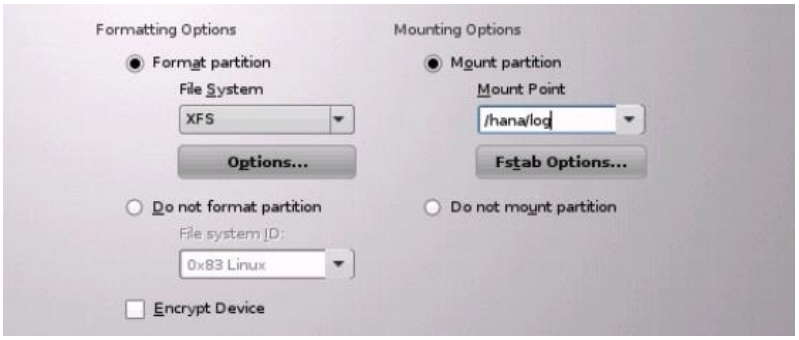



24. Right-click the same device
25. Select Add Partition
26. Select Primary Partition, click Next
27. Use 2GB as the Size, click Next
28. Use Swap as the File System
29. Use swap as the Mount Point
30. Click Finish




31. Click the Device with the size of 512GB
32. Right-click the Device and Select Add Partition
33. Select Primary Partition, click Next

34. Select Maximum Size, click Next
35. Use XFS as the File System
36. Use /hana/log as the Mount point
37. Click Finish




38. Click the Device with the size of 1.5TB
39. Right-click the Device and Select Add Partition
40. Select Primary Partition, click Next
41. Select Maximum Size, click Next
42. Use XFS as the File System
43. Use /hana/data as the Mount point
44. Click Finish




45. Click the Device with the size of 1TB
46. Right-click the Device and Select Add Partition
47. Select Primary Partition, click Next

48. Select Maximum Size, click Next

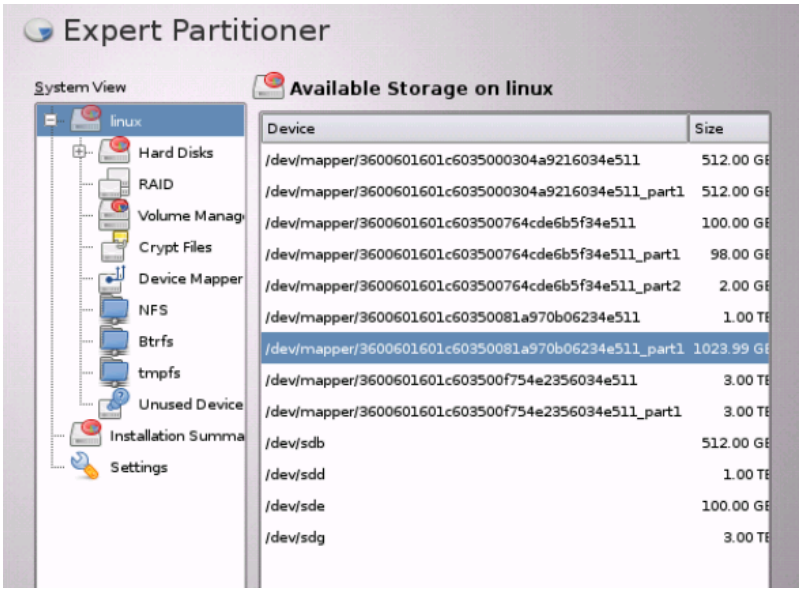
49. Use EXT3 as the File System

50. Use /hana/shared as the Mount point

51. Click Finish




The Partition Table is shown below:




52. Click Accept

53. Click Change, select Booting

54. Select Boot Loader Installation tab

55. Click Boot Loader Installation Details

56. Take care that the boot device is the first in the list

57. Click OK



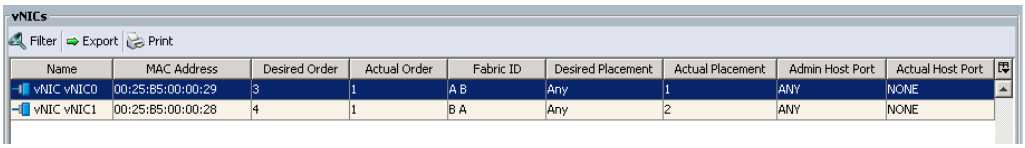

58. Click OK
59. Click Change, select Software
60. Unselect GNOME Desktop Environment
61. Select SAP HANA Server Base
62. Click OK
63. Click Accept
64. Click Change, select Default Runlevel
65. Select 3: Full multiuser with network
66. Click OK
67. Click Install
68. Click Install

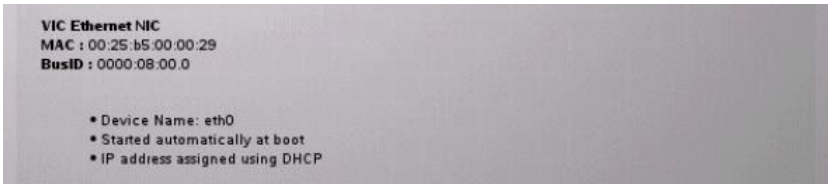


The Operating System will be installed as defined and the server reboots automatically.

69. After the reboot, please proceed with the system configuration
70. Use <<var_mgmt_passwd>> as the password for root
71. Use <<var_mdc_hana01_hostname>> as the hostname
72. Use <<var_mdc_domain>> as the domain. It is possible to use the end customer domain.
73. Disable the firewall for now.
74. Change the Network Settings as follows:

a. Select the interface connected to <<var_ucs_mdc_access_vlan_name>>, the best way is to check the MAC address in UCS Manager and on the operating system




b. Select Edit

c. Select Static assigned IP Address

d. Use <<var_mdc_hana01_access_ip>> as the IP Address

e. Use <<var_mdc_access_mask>> as the Subnet Mask

f. Click Next

g. Select the second NIC, click Edit

h. Select Static assigned IP Address

i. Use <<var_mdc_hana01_nfs_ip>> as the IP Address

j. Use <<var_nfs_mask>> as the Subnet Mask

k. Click the Routing Tab

l. Enter <<var_mdc_access_gw>> as the Default Gateway

m. Click OK

75. Proceed with the configuration using the defaults or your datacenter best practices.

## Enabling Data Traffic on vHBA3 and vHBA4

Now that the Cisco FNIC driver is loaded in the operating system, vHBA3 and vHBA4 are also logged into the MDS switches. For best performance of a SAP HANA Scale-Up system it is recommended to move the paths for the data volume from the single storage path zoning into the multi paths zoning.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_mdc-hana01-data>> vsan 10
```

```
zone name <<var_zone_mdc-hana01-data>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:0a
   exit

zoneset name CRA-EMC-A vsan 10
member <<var_zone_mdc-hana01-data>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_mdc-hana01 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0d
…
zone name zone_mdc-hana01-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
```

```
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:0c

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_t002-vhana1-data
  zone zone_mdc-hana01
  zone zone_mdc-hana01-data
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
Copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_mdc-hana01-data>> vsan 20
zone name <<var_zone_mdc-hana01-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:0c
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_mdc-hana01-data>>
exit
zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_mdc-hana01-data vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0d

zone name zone_mdc-hana01-data vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
```

```
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:0c

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_t002-vhana1-data
  zone zone_mdc-hana01
  zone zone_mdc-hana01-data
CRA-EMC-B#
```

4. Save the running configuration as startup configuration:

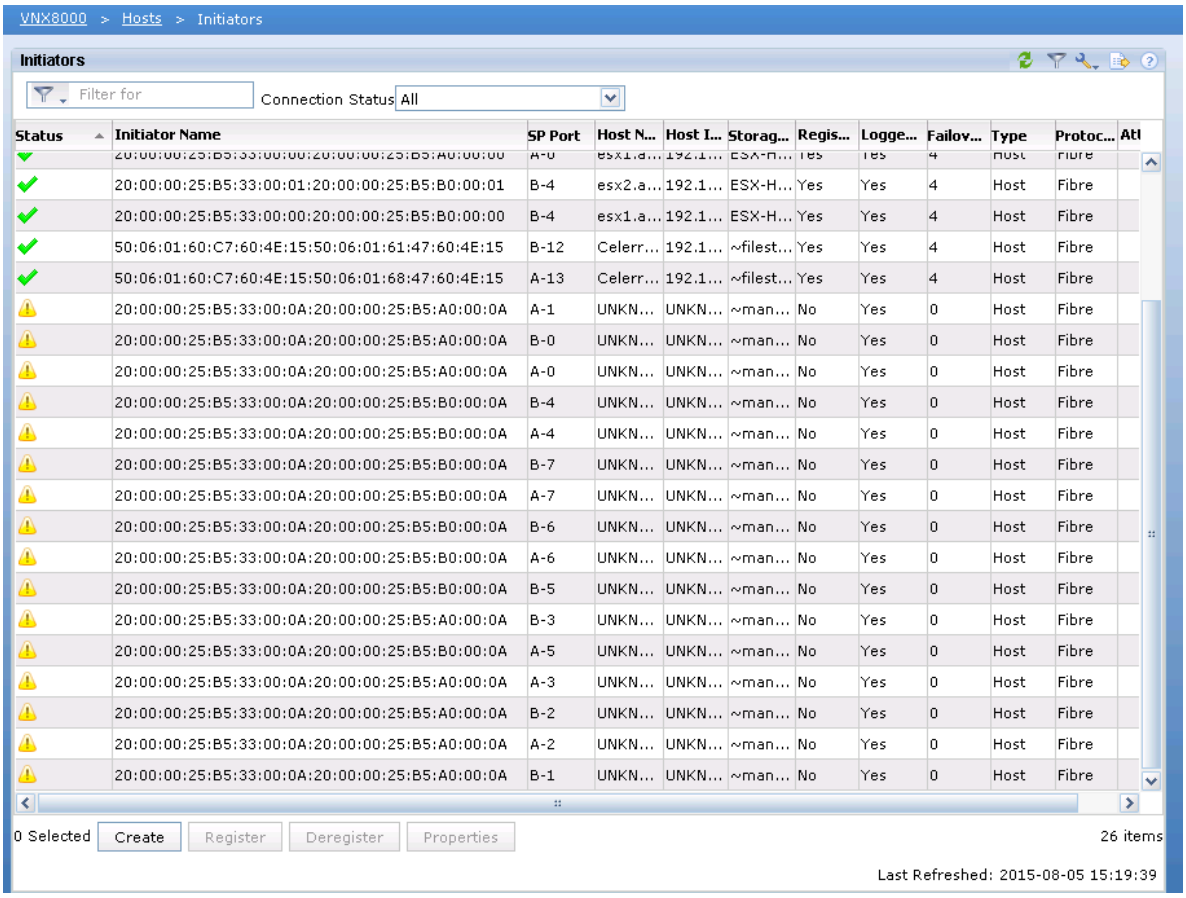
```
copy run start
```

## Configure EMC VNX

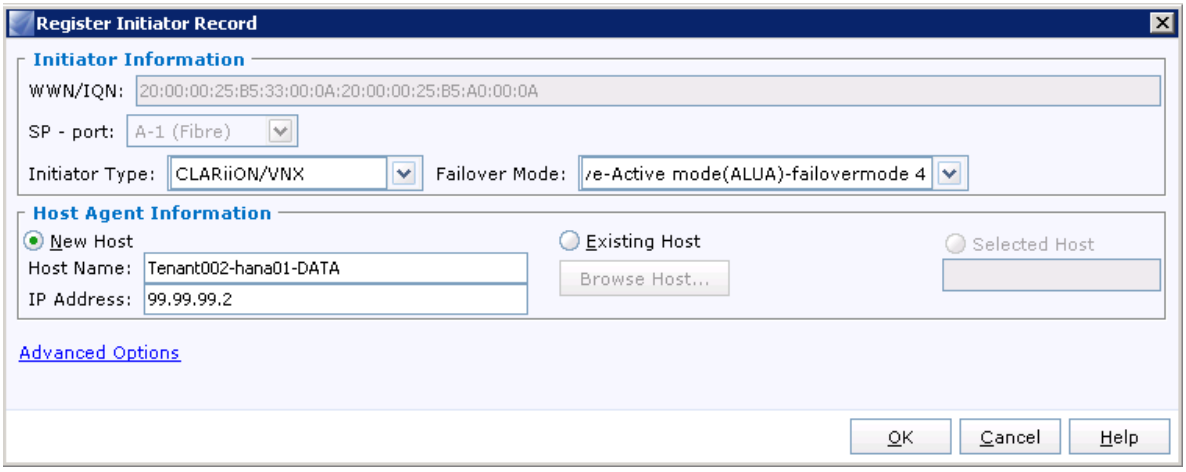
### Register Host

To register a host, complete the following steps:

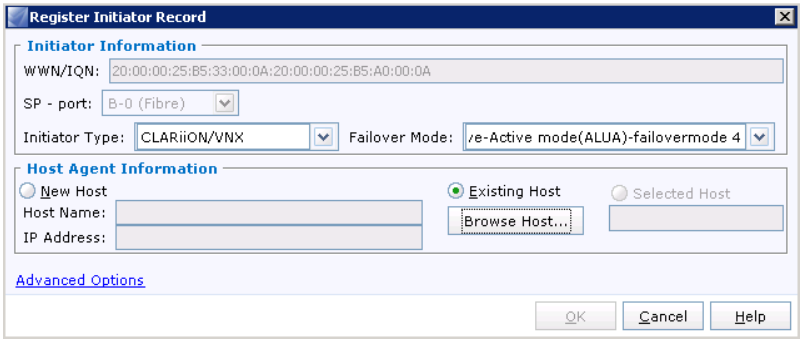
1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators



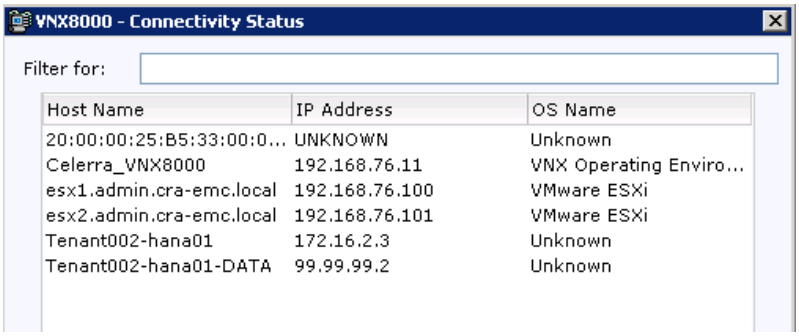

2. Select one of the unregistered entries for the host MDC-hana01, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Active mode(ALUA)-failovermode 4 as the Failover Mode
5. Enter <<var_ucs_mdc_hana1_name>>-data as the Host Name (indicates the relationship to the Service Profile)
6. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
7. Click OK
8. Click Yes
9. Click OK
10. Click OK




11. Select the second Entry for this host <<var_ucs_mdc_hana1_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and Click Browse Host




15. Select <<var_ucs_mdc_hana1_name>>-data and click OK




16. Click OK
17. Click Yes

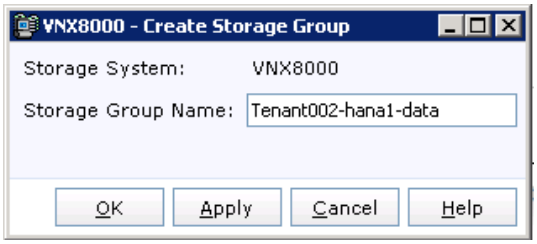
18. Click OK
19. Click OK

Repeat Step 10 to 18 for all remaining paths of this server in the list.

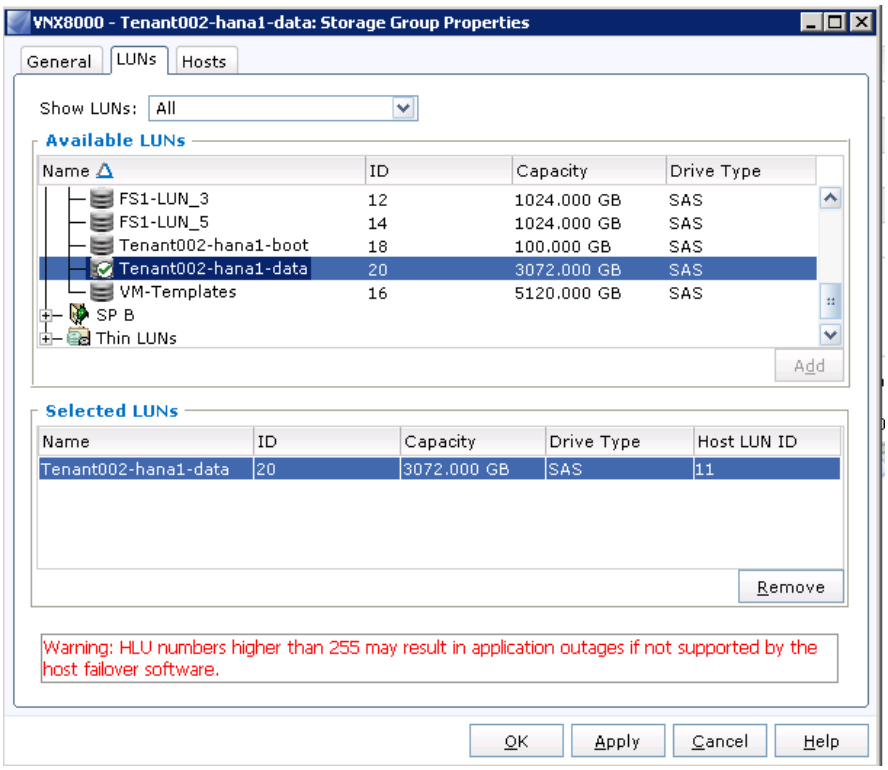
### Create Storage-Group

To create a storage group, complete the following steps:

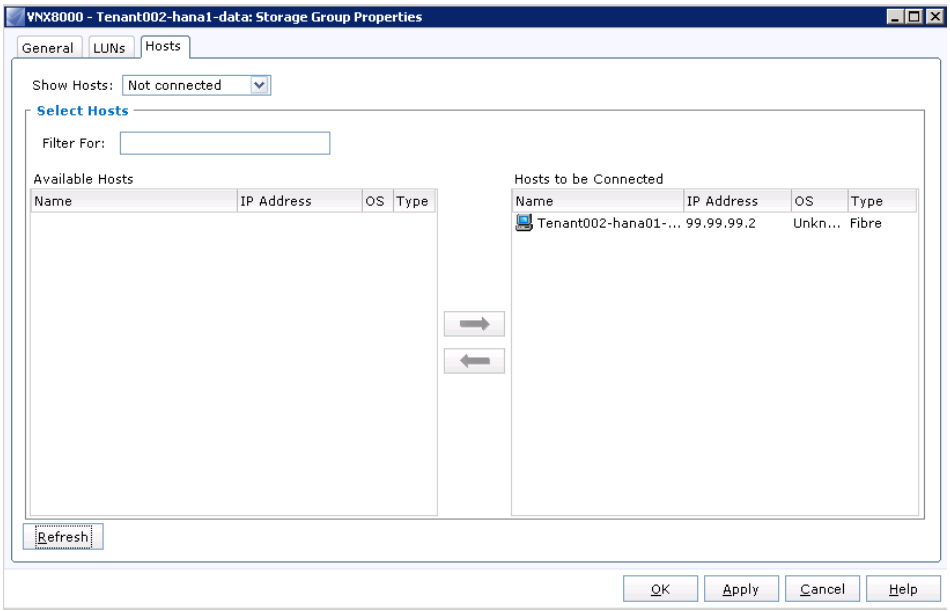
1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_mdc_hana1_name>>-data as the Name
4. Click OK
5. Click Yes



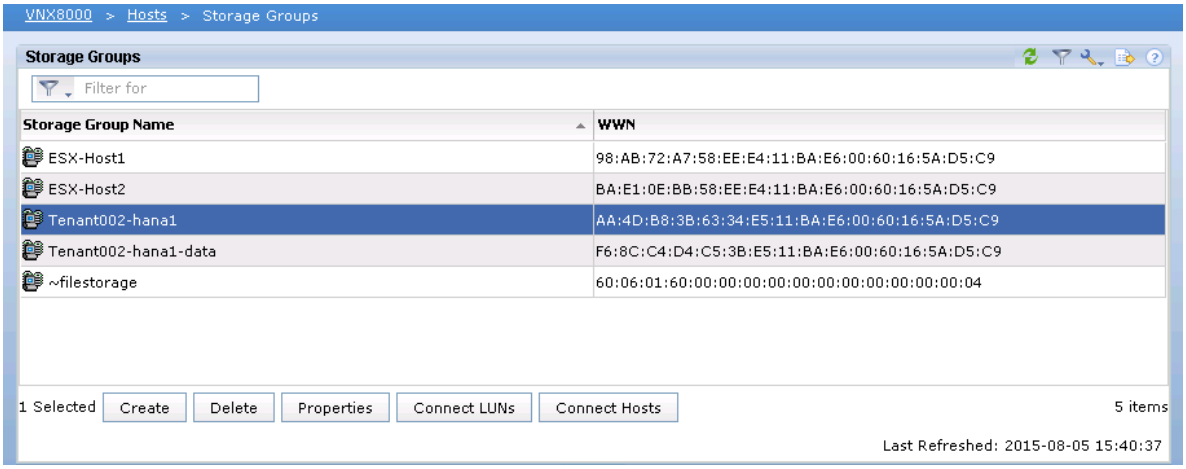

6. Click Yes
7. Select All from the Show LUNs Drop-Down menu, click OK
8. Select the Data-LUN from the list of LUNs and click Add
9. Select 11 as the Host LUN ID for <<var_ucs_mdc_hana1_name>>-data (the same ID as before)




10. Click the Hosts tab
11. Select <<var_ucs_mdc_hana1_name>>-data and click the icon
12. Click OK
13. Click Yes
14. Click OK



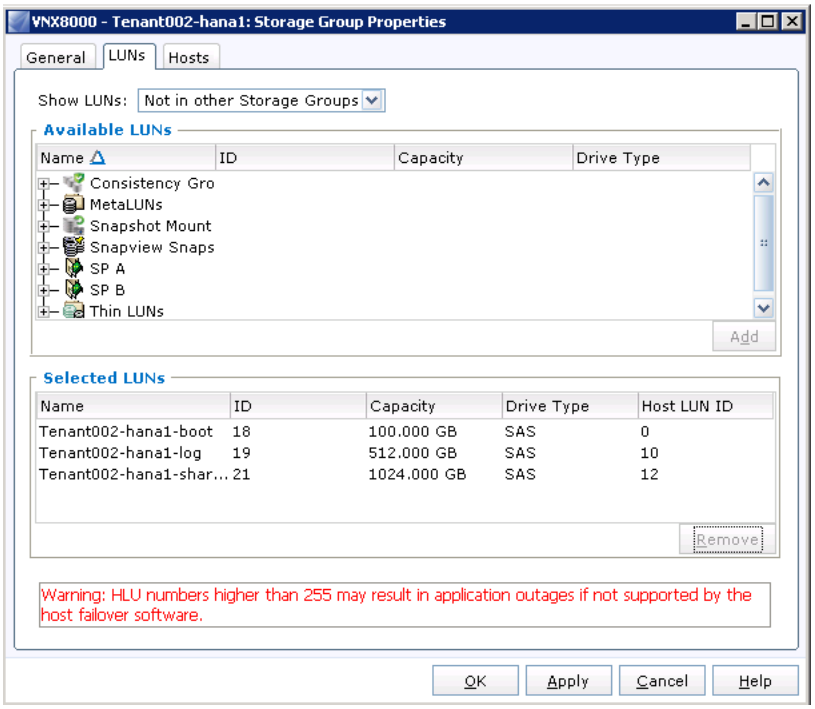

15. On the list of Storage Groups, select <<var_ucs_mdc_hana1_name>>, click Properties




16. Click the LUNs Tab

17. Select the data LUN from the below list “Selected LUNs”

18. Click Remove




19. Click OK
20. Click Remove LUNs from storage group
21. Click OK
22. Return to the server and boot/reboot the system

## Configure SUSE Linux for SAP HANA

To configure SUSE Linux for SAP HANA, complete the following steps:

1. Use a SSH client to logon to the installed system with the user root and the password <<var_mgmt_passwd>>.
2. Register the System at SUSE to get latest Patches.

The system must have access to the internet to proceed with this step!

```
suse_register -i -r -n -a email= <<email_address>> -a regcode-
sles=<<registration_code>>
```

3. Update the system with the following command

The system must have access to the internet to proceed with this step!

```
zypper update
```

Please follow the on-screen instructions to complete the update process. It is required to reboot the server and login to the system again.

4. Configure the Network Time Protocol with the following step

```
vi /etc/ntp.conf


server <<var_global_ntp_server_ip>>
fudge <<var_global_ntp_server_ip>> stratum 10
keys /etc/ntp.keys
trustedkey 1
```

5. Create User-Group sapsys

```
groupadd –g 401 sapsys
```

6. Change the permissions for the SAP HANA file systems

```
chgrp –R sapsys /hana
chmod –R 775 /hana
```

7. We recommend to disable Transparent Huge Pages and the swappiness on the system

```
vi /etc/init.d/after.local


 #!/bin/bash
# (c) Cisco Systems Inc. 2014
echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status
# set sappiness to 30 to aviod swapping
echo "Set swappiness to 30 to avoid swapping"
echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status
```

8. Based on different SAP Notes multiple entries in /etc/sysctl.conf are required

```
vi /etc/sysctl.conf


#SAP Note 1275776
vm.max_map_count = 2000000
```

```
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
net.ipv4.tcp_slow_start_after_idle = 0
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_slot_table_entries = 128
# Memory Page Cache Linit Feature SAP Note 1557506
vm.pagecache_limit_mb = 4096
vm.pagecache_limit_ignore_dirty = 1
```

9. Edit boot loader configuration file /etc/sysconfig/bootloader. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

```
intel_idle.max_cstate=0
```

10. Append the “intel_idle.max_cstate=0 processor.max_cstate=0” value to the kernel's parameter line in /boot/grub/menu.lst – 3.0.xxx-x.xx is the placeholder for your Kernel patch version

```
vi /boot/grub/menu.lst


title SLES for SAP Applications - 3.0.XXX-X.XX
root (hd0,0)
```

```
kernel /boot/vmlinuz-3.0.XXX-X.XX-default root=/dev/sda2 resume=/dev/sda1
splash=silent showopts intel_idle.max_cstate=0 processor.max_cstate=0

initrd /boot/initrd-3.0.XXX-X.XX-default
```

11. Reboot the server before continue with the next steps

```
reboot
```

## Install SAP HANA

To install SAP HANA, complete the following steps:

1. Mount the Software share to access the SAP HANA installation files

```
mkdir /software

mount 172.30.113.11:/FS_Software /software
```

Please use the SAP HANA Installation guide provided by SAP for the software revision you plan to install. The program to install SAP HANA Revision 100 is hdblcm located in the directory <Installation source>/DATA_UNITS/HDB_LCM_LINUX_X86_64.

```
cd /software/SAP/SPS10/REV100/DATA_UNITS/HDB_LCM_LINUX_X86_64

./hdblcm
```

2. The text-based installation menu launches

```
Select 1 for Install new system


Select 2 for All Components


Enter Installation Path: /hana/shared : Press Enter

Enter local host name: mdc-hana01: Press Enter

Do you want to add additional hosts to the system? N

Enter SAP HANA System ID: <<var_mdc_hana1_sid>>

Enter Instance Number:  <<var_mdc_hana1_nr>>

Select Database mode 2 for mutilple_containers

Select Database Isolation 2 for high

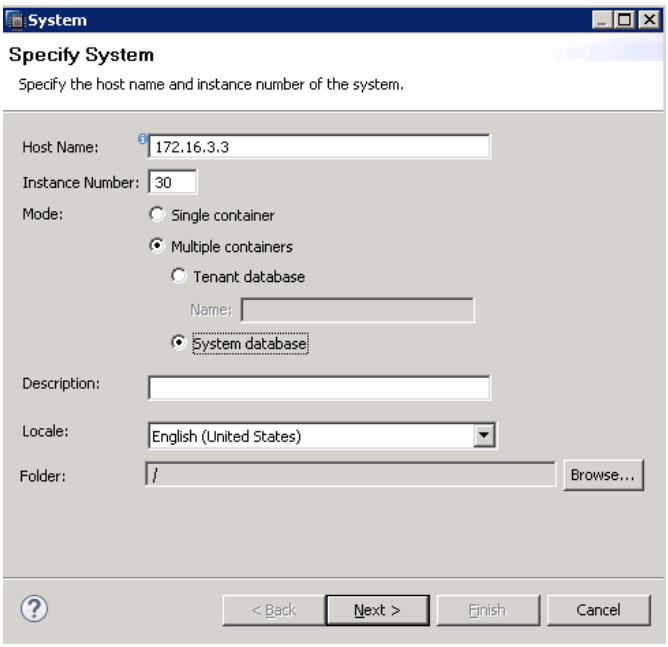
Select System Type: 4 for Custom
```

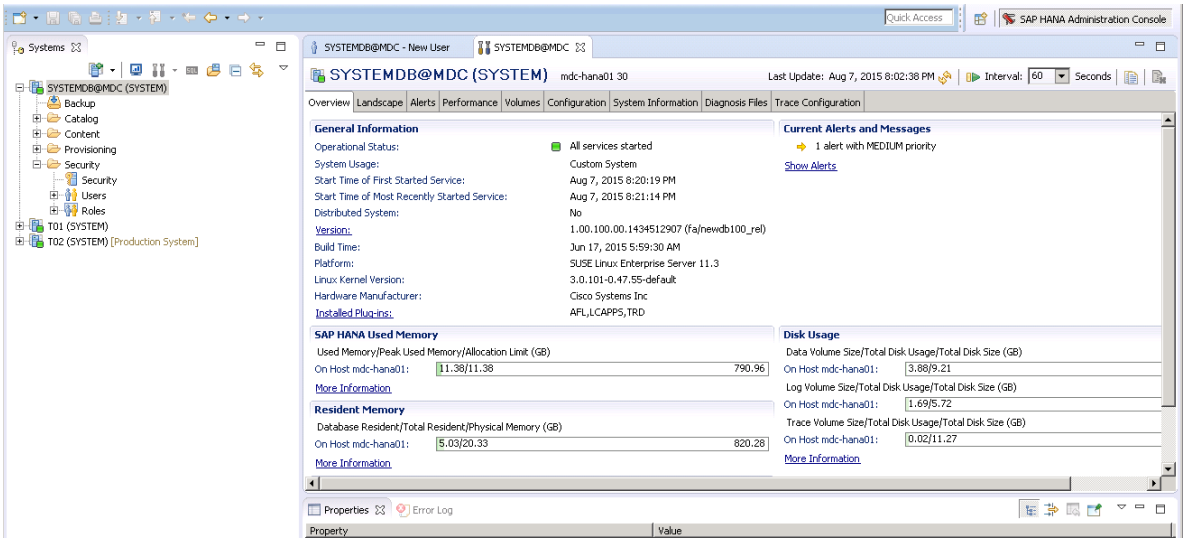
```
Enter Location for Data Volumes /hana/data/MDC: Press Enter
Enter Location for Log Volumes /hana/log/MDC: Press Enter
Restrict maximum memory allocation n : Press Enter
Enter Certificate Host name mdc-hana01 : Press Enter
Enter SAP Host Agent User (sapadm) password: <<var_mgmt_passwd>>
Confirm password
Enter System Administrator (mdcadm) password: <<var_mgmt_passwd>>
Confirm password
Enter System Administrator Home Directory /usr/sap/MDC/home : Press Enter
Enter System Administrator Login shell /bin/sh: Press Enter
Enter System Administrator User id 1003 : Press Enter
Enter Database User (SYSTEM) Password : <<var_mdc_hana1_sys_passwd>>
Confirm Passwd
Restart instance after machine reboot n : Press Enter
   Do you want to continue : y
```

## Test the Connection to SAP HANA

Use the SAP HANA Studio on a system with network access to the installed SAP HANA system and add the SAP HANA Database. The information you need is as follows:

- Hostname or IP address <<var_mdc_hana1_access_ip>>
- SAP HANA System Number <<var_mdc_hana1_nr>>
- Mode: Multiple Containers – System Database
- SAP HANA database user (default: SYSTEM)
- SAP HANA database user password <<var_mdc_hana1_sys_passwd>>




## Install SAP HANA Database Container

Since installing the SAP HANA MDC System with the security setting HIGH, every Tenant Database Container requires an own user on the operating system. The user must have sapsys as the primary group.

1. Log in to the operating system through Console or SSH as user root

2. Create the user for the new Tenant Database Container

```
useradd -g sapsys -m -d /home/<<var_hana-mdc1_db1_os-user>> <<var_hana-
mdc1_db1_os-user>>
```

3. Check that the user is created with the correct group

```
mdc-hana01:~ # su - <<var_hana-mdc1_db1_os-user>>

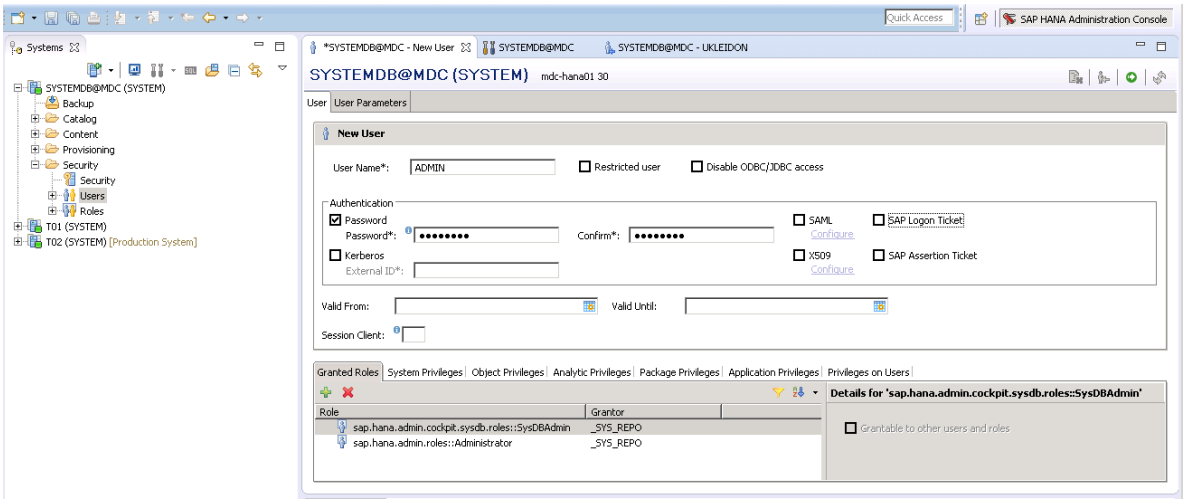
t03adm@mdc-hana01:~> id

uid=1003(t03adm) gid=401(sapsys) groups=401(sapsys),16(dialout),33(video)

t03adm@mdc-hana01:~> exit
```

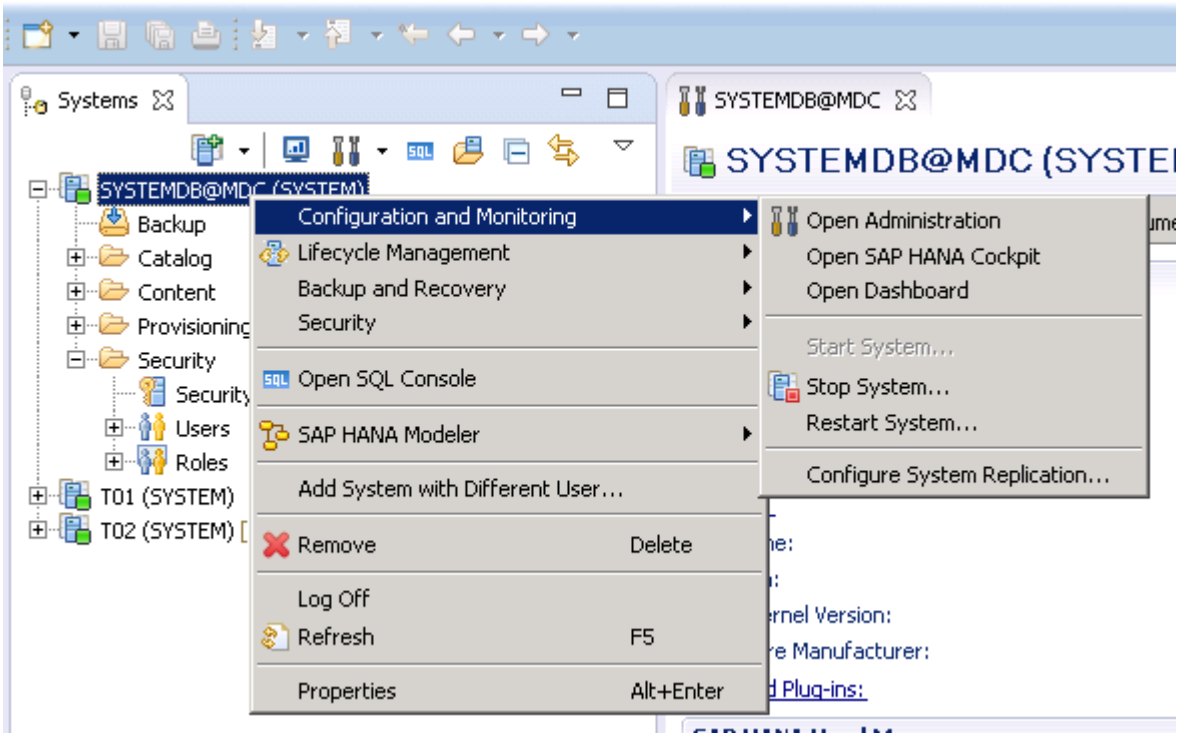
Creating a Tenant Container must be done with the SAP HANA Cockpit and a user with the role sap.hana.admin.cockpit.sysdb.roles::SysDBAdmin and sap.hana.admin.roles::Administrator.

4. Open the SAP HANA Studio
5. Go to SYSTEMDB@MDC > Security > Users. Right-click Users and Select New User
6. Enter <<var_hana-mdc1_admin>> as the User Name
7. Enter <<var_hana-mdc1_temp-passwd>> as the Password and Confirm it. The password must be changed at first login.
8. Add the Roles as specified before
9. Click the System Privileges tab
10. Add the Privilege DATABASE ADMIN
11. Press F8 (Deploy)



12. Right-click SYSTEM@MDC, Select Configuration and Monitoring

13. Select Open SAP HANA Cockpit

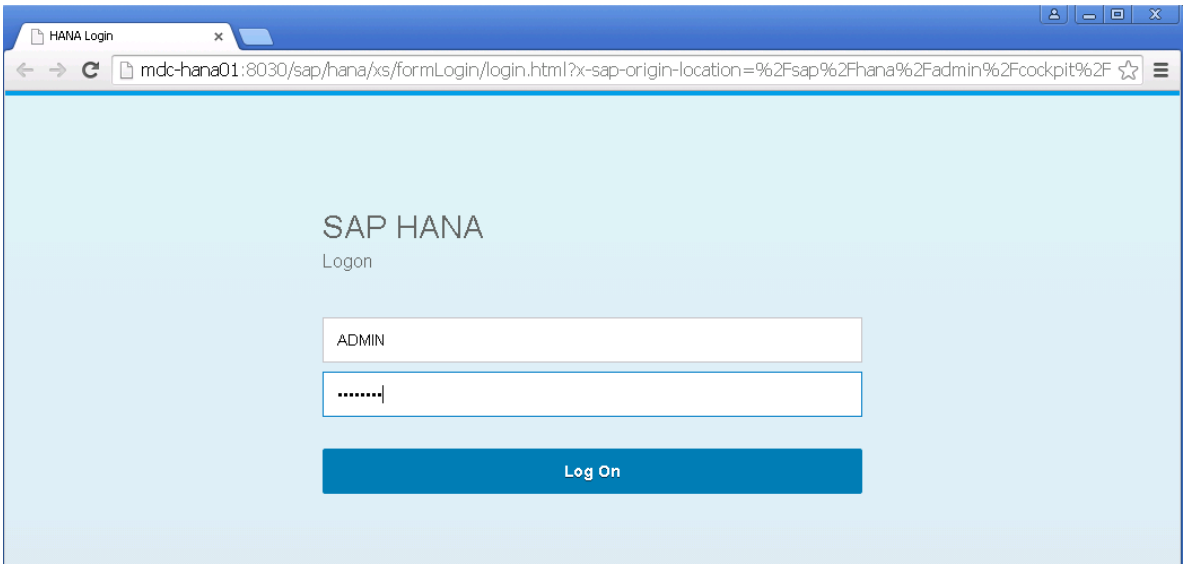



A New Web Browser window will start.

14. Enter <<var_hana-mdc1_admin>> as the User

15. Enter <<var_hana-mdc1_temp-passwd>> as the Password

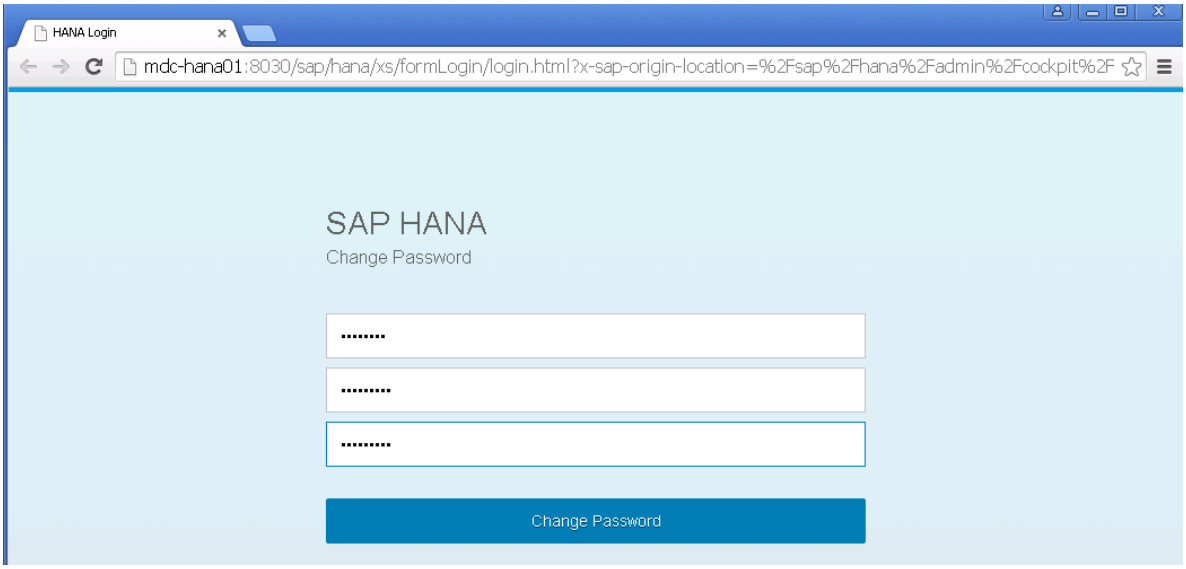
16. Click Log On



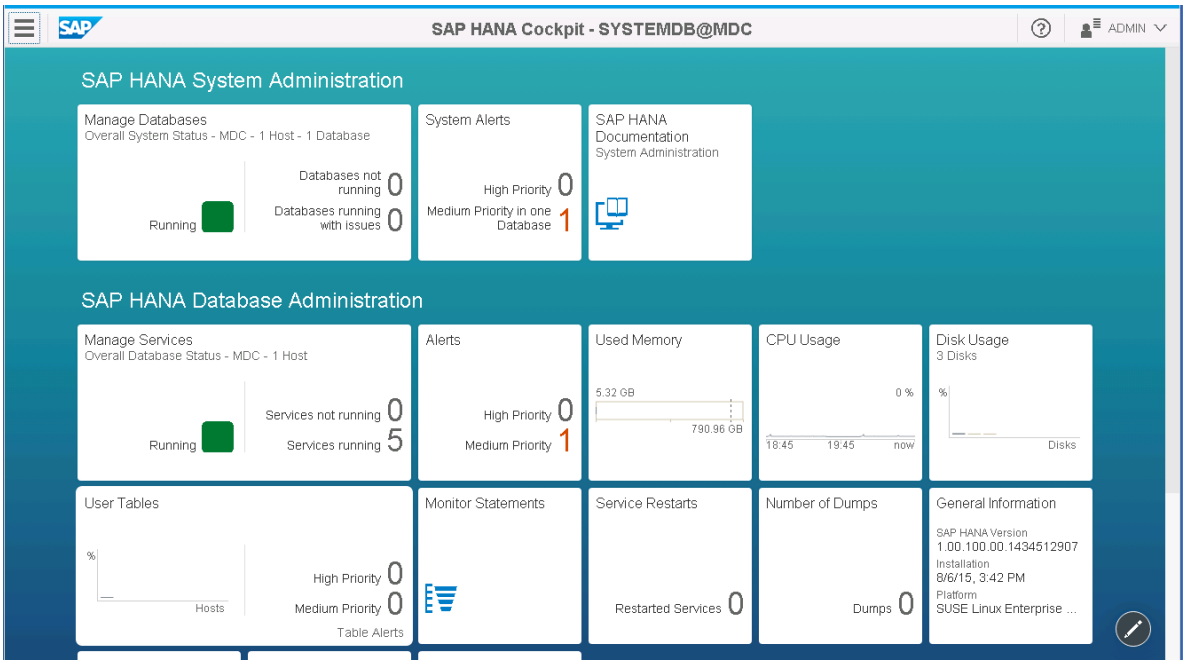

17. Enter <<var_hana-mdc1_temp-passwd>> as the Old Password

18. Enter <<var_hana-mdc1_admin_passwd>> and confirm it as the new Password

19. Click Change Password

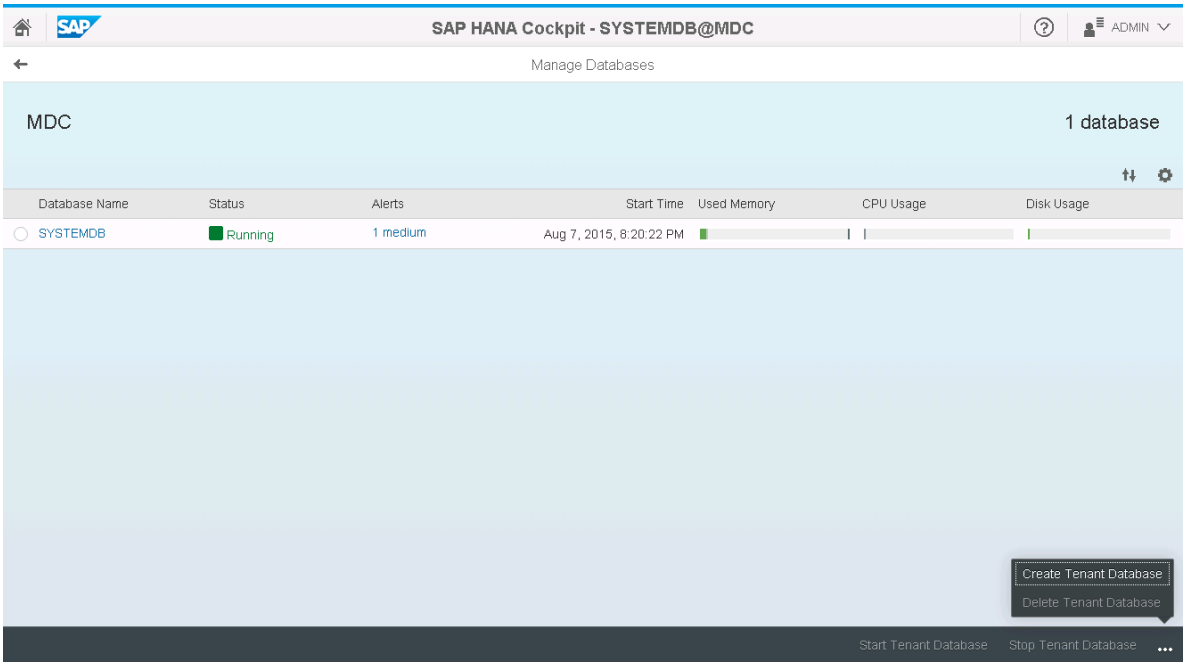



20. In the SAP HANA Cockpit Home Screen click Manage Databases in the SAP HANA System Administration Section (Top one)




21. Click the "..." icon in the lower right corner

22. Select Create Tenant Database



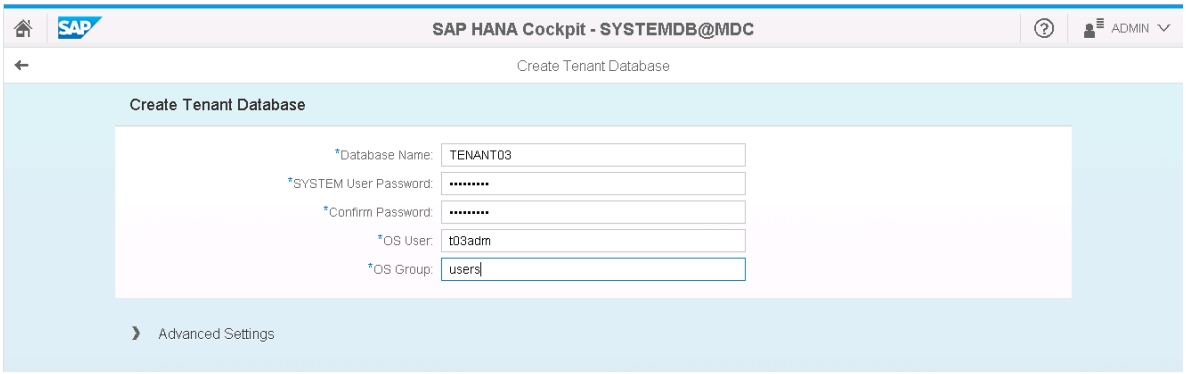

23. Enter <<var_hana-mdc1_db1_name>> as the Database Name

24. Enter <<var_hana-mdc1_db1_system_passwd>> as the password for the SYSTEM user

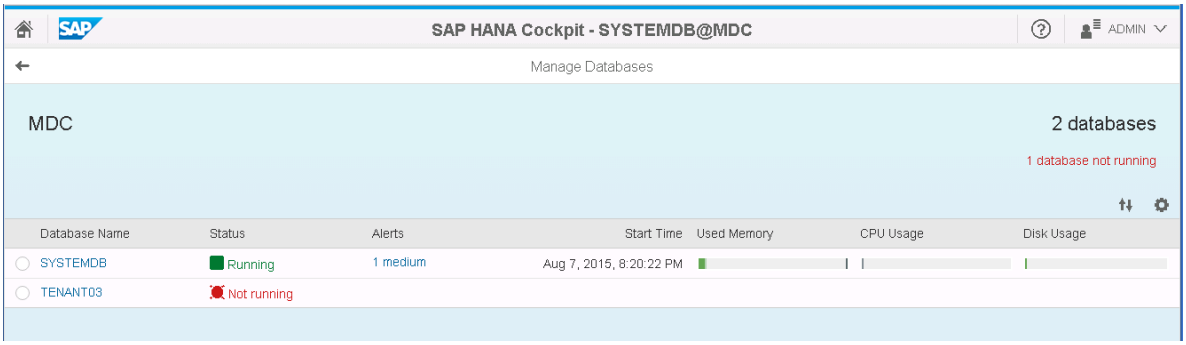
25. Enter <<var_hana-mdc1_db1_os-user>> the OS user created before (we used t03adm)

26. Enter a OS group other than sapsys (we used users)

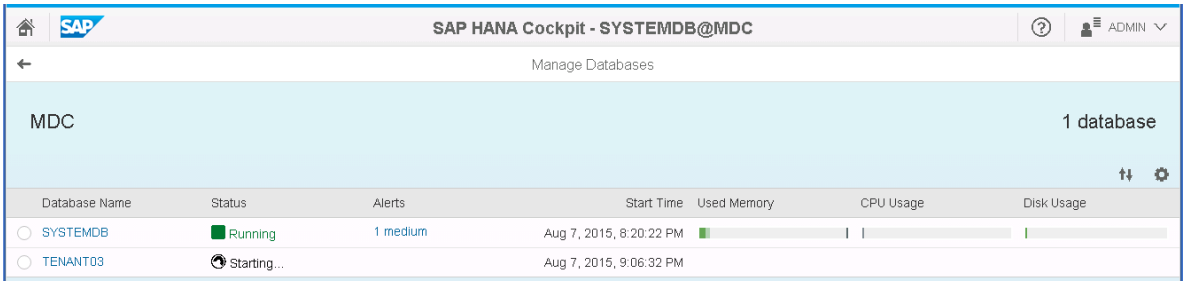
27. Click Create Tenant Database



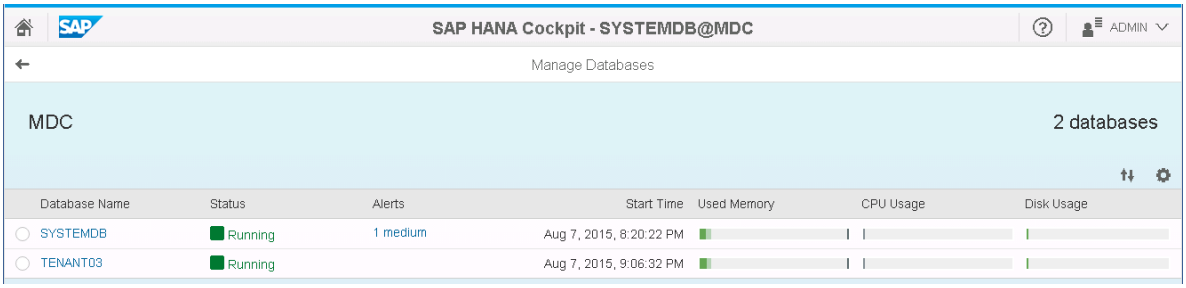

The database creation runs in the background.



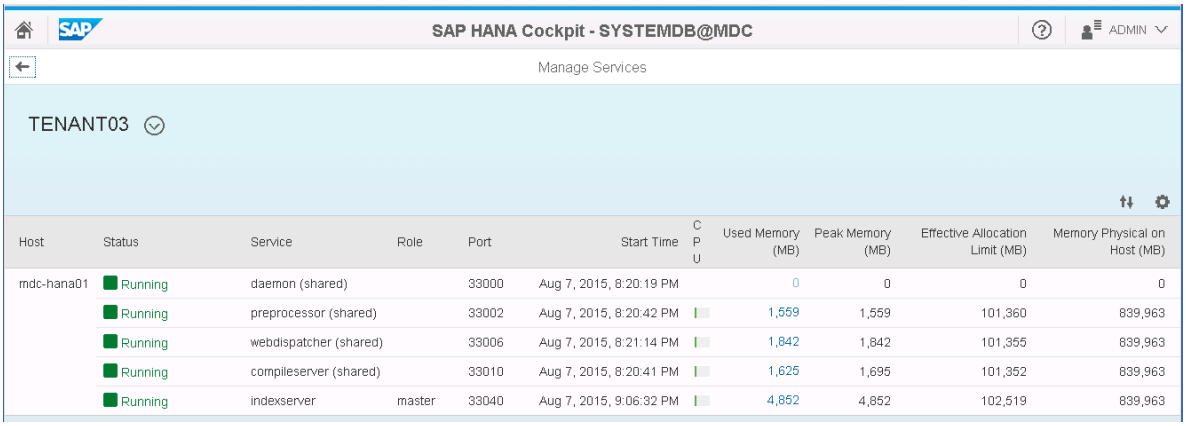

The database starts automatically after creation.




28. Click the Database Name



29. In the list of processes check the Port for the indexserver (here 33040)




| Host | Status | Service | Role | Port | Start Time | CPU | Used Memory (MB) | Peak Memory (MB) | Effective Allocation Limit (MB) | Memory Physical on Host (MB) |
|---|---|---|---|---|---|---|---|---|---|---|
| mdc-hana01 | Running | daemon (shared) | | 33000 | Aug 7, 2015, 8:20:19 PM | | 0 | 0 | 0 | 0 |
| | Running | preprocessor (shared) | | 33002 | Aug 7, 2015, 8:20:42 PM | | 1,559 | 1,559 | 101,360 | 839,963 |
| | Running | webdispatcher (shared) | | 33006 | Aug 7, 2015, 8:21:14 PM | | 1,842 | 1,842 | 101,355 | 839,963 |
| | Running | compileserver (shared) | | 33010 | Aug 7, 2015, 8:20:41 PM | | 1,625 | 1,695 | 101,352 | 839,963 |
| | Running | indexserver | master | 33040 | Aug 7, 2015, 9:06:32 PM | | 4,852 | 4,852 | 102,519 | 839,963 |

30. The connection to the new <<var_hana-mdc1_db1_name>> Database Container via a SQL client must use the network port of the indexserver +1, here 33040+1 = 33041.

```
hdbsql -n <host>:<port> -u <DB username>
```

```
hdbsql -n 173.16.3.3:33041 -u SYSTEM
```

```
C:\Program Files\sap\hdbclient>hdbsql -n 172.16.3.3:33041 -u SYSTEM
Password:

Welcome to the SAP HANA Database interactive terminal.

Type:  \h for help with commands
       \q to quit

hdbsql TENANT03=>
```

## Configure the Linux Firewall

To provide a basic access security to the SAP HANA containers it is recommended to configure the firewall on Linux. Enable the firewall in YAST and add the eth0 interface to the External Zone. Make sure that the ports for administrative tasks, like port 22 for ssh, are open.



The original attempt from SAP for the SAP HANA Multi Database Containers is to provide a flexible usage model for a single Client/Tenant. Therefore the security on the Operating System and Component level is not implemented. As soon a Clinent/Tenant has access to the OS he is able to reach all database containers. The only security provided here are the user and password in every database container.

To allow access to the tenant database container from a specific IP address or IP range you can use the following commands. For more information please use the iptables documentation provided by SUSE.

In this example the access to the database from the network 192.168.76.0/24 and from the host 170.1.6.1 is allowed.

```
iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33040 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options
```

```
iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33040 -j ACCEPT


iptables -A input_ext -s 170.1.6.1/32 -p tcp -m tcp --dport 33040 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options

iptables -A input_ext -s 170.1.6.1/24 -p tcp -m tcp --dport 33040 -j ACCEPT


iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33041 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options

iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33041 -j ACCEPT


iptables -A input_ext -s 170.1.6.1/32 -p tcp -m tcp --dport 33041 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options

iptables -A input_ext -s 170.1.6.1/24 -p tcp -m tcp --dport 33041 -j ACCEPT


iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33042 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options

iptables -A input_ext -s 192.168.76.0/24 -p tcp -m tcp --dport 33042 -j ACCEPT


iptables -A input_ext -s 170.1.6.1/32 -p tcp -m tcp --dport 33042 -m state --
state NEW -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-ACC " --log-tcp-
options --log-ip-options

iptables -A input_ext -s 170.1.6.1/24 -p tcp -m tcp --dport 33042 -j ACCEPT
```

## SAP HANA Scale-Up System with SAP HANA Dynamic Tiering

This use case describes the setup of two bare metal server to run a SAP HANA scale-up system on one and the SAP HANA Dynamic Tiering System (Sybase IQ) on the second server.

The high-level steps for this use case are as follows:

1. Create the access VLAN on Cisco Nexus 9000, and Cisco UCS.
2. Create Service Profile on Cisco UCS.
3. Define LUNs on the EMC VNX, register the server and configure the Storage-Group.
4. Install and Configure the Operating System.

5. Install SAP HANA.

6. Test the connection to the SAP HANA database.

## Workload Definition

The request to deploy this SAP HANA system has defined that the SAP HANA system must have a size of 1TB main memory and the SAP HANA Dynamic Tiering host must provide additional capacity of 5TB. Based on the use case and data set only 5-8 SAP HANA queries will hit the Dynamic Tiering node. This SAP HANA system is for production and has to run on RedHat Enterprise Linux.

## Requirements

For a SAP HANA database in a Scale-Up configuration with the SAP HANA Dynamic Tiering option the networks required are the access network, the Inter-Node communication network and the storage network (in this case via Fibre Channel). This use case also requires a /hana/shared file system which is accessible on both servers. SAP documented the option to use the SAP HANA node as an NFS server and the SAP HANA DT node as the NFS client. As we use a storage with NFS protocol support, the better option is to use the EMC VNX as the NFS server and both servers as NFS client. In this case a dedicated network for NFS is used.

To access the installation sources for SAP HANA and other applications the access to the NFS share on the EMC VNX storage is also configured – this can be temporary only until all applications are installed. All other networks are optional. For this use case no optional network is used. This is the first system for a tenant, so no existing network definition can be used. As this is for Non-Production the relaxed storage requirements apply. The following configuration is required:

Network: 1x Access Network with >=100 Mbit/sec

1x Inter-Node Network with 10 GBit/sec

1x NFS-Network for /hana/shared >= 1 GBit/sec

1x Global-NFS Network for installation sources

SAP HANA Node

Storage: 512GB for /hana/log, 3TB for /hana/data, 1TB for /hana/shared

An average of 300 MB/sec throughput can be used as the baseline. Dependent on the use case it can be less (default analytics) or much more (heavy Suite on HANA)

Memory: 1 TB

CPU: 4x Intel Xeon E7 v2 CPUs (Ivy Bridge)

SAP HANA Dynamic Tiering Node

CPU: 2.5 CPU cores per concurrent query hitting DT

8 queries x 2.5 cores = 20 cores

Storage: For Data: 5TB + ~15% for temp and overhead

For Log: 10x average daily change volume, we assume 20 GB change rate = 200GB

For RLV: 8GB/core x 20 cores = 160GB

An average of 50 MB/sec throughput per CPU core must be used as the baseline.

50 MB/sec x 20 cores = 1000 MB/sec

2-3 spinning disks or 0.4 SSD disks per CPU core

3 spinning disks x 20 cores = 60 disks

Memory: 8-16 GB per CPU core

12 GB x 20 cores = 240 GB main memory

The following Information is used to install SAP HANA with Dynamic Tiering for Tenant004 in this Cisco UCS Integrated Infrastructure for SAP HANA with EMC VNX Storage:

## Switch Configuration

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

1. On each Nexus 9000, enter configuration mode:

```
config terminal
```

2. From the configuration mode, run the following commands:

```
vlan <<var_t004_access_vlan_id>>
name T004-Access

vlan <<var_t004_internal_vlan_id>>
name T004-Internal

vlan <<var_t004_nfs_vlan_id>>
name T004-NFS
```

3. Add the VLAN to the VPC Peer-Link:

```
interface po1
switchport trunk allowed vlan add
<<var_t004_access_vlan_id>>,<<var_t004_internal_vlan_id>>,<<var_t004_nfs_vlan_id>
>
```

4. Add the VLAN to the Port Channels connected to the Cisco UCS:

```
interface po13,po14
```

```
switchport trunk allowed vlan add
<<var_t004_access_vlan_id>>,<<var_t004_internal_vlan_id>>,<<var_t004_nfs_vlan_id>
>
```

5. Add the VLAN to the EMC VNX DataMovers

```
interface po33,po34
switchport trunk allowed vlan add <<var_t004_nfs_vlan_id>>
```

6. Add the VLAN to the data center uplink

```
interface po99
switchport trunk allowed vlan add <<var_t004_access_vlan_id>>
```

7. Save the running configuration to start-up:

```
copy run start
```

8. Validate the configuration:

```
#show vpc
…
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,2031,2034,3001-3004,3204,3304

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
…
13   Po13   up     success     success                    3001-3004,3
                                                 204,3304
14   Po14   up     success     success                    3001-3004,3
                                                 204,3304
…
33   Po33   up     success     success                    177,2034,33
                                                          04
34   Po34   down*  success     success                    -
…

show vlan id 3004
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3004 Tenant004-Access                 active    Po1, Po13, Po14, Po99, Eth1/1
                                                Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                Eth1/9, Eth1/10, Eth1/15
                                                Eth1/16, Eth1/17, Eth1/18
```

```
VLAN Type         Vlan-mode
---- -----        ----------
3004 enet         CE

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ----------------------------------------


show vlan id 3204

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
3204 Tenant004-Internal              active    Po1, Po13, Po14, Eth1/5, Eth1/6
                                               Eth1/7, Eth1/8, Eth1/9, Eth1/10
                                               Eth1/15, Eth1/16, Eth1/17
                                               Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3204 enet         CE

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ----------------------------------------

show vlan id 3304

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
3304 Tenant004-NFS                   active    Po1, Po13, Po14, Po33, Po34
                                               Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                               Eth1/9, Eth1/10, Eth1/13
                                               Eth1/14, Eth1/15, Eth1/16
                                               Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3304 enet         CE

Remote SPAN VLAN
----------------
Disabled

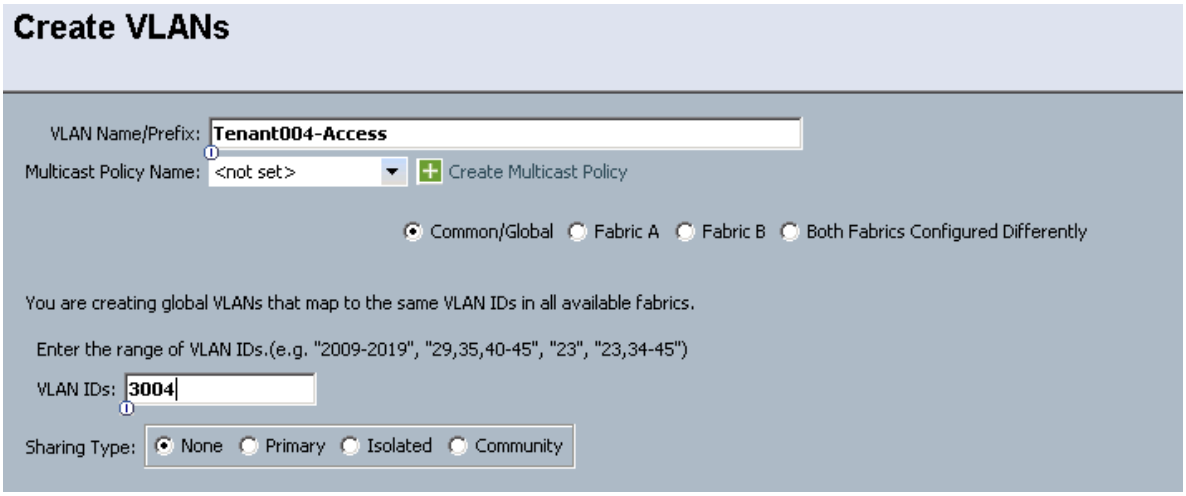
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ----------------------------------------
```

## Cisco UCS Configuration

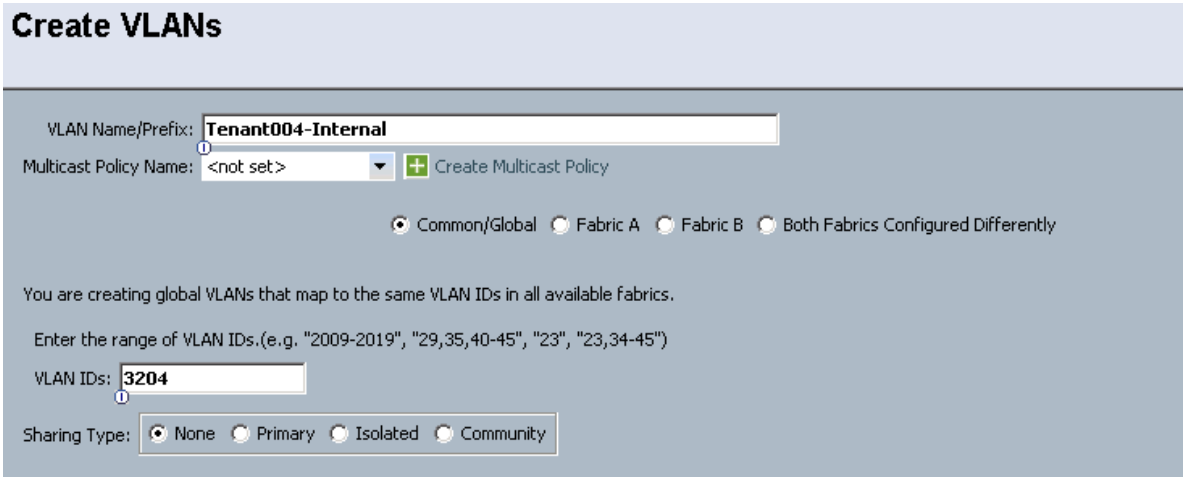
### Configure VLANs and VLAN-Group Membership

To create a VLAN, complete the following steps:

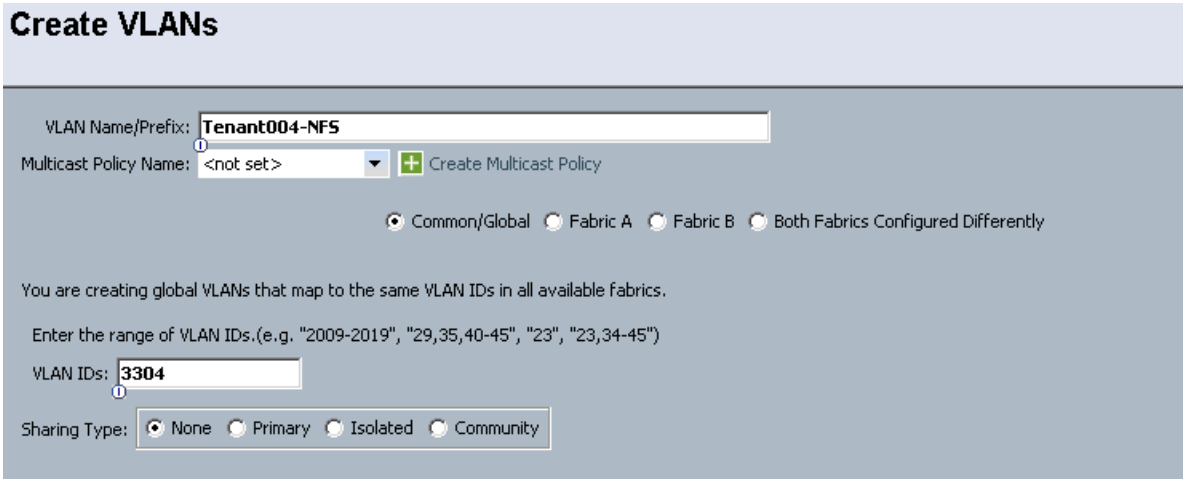
1. Log in to Cisco UCS Manager.
2. Go to LAN Tab > LAN Cloud > VLANs.
3. Right-click > Create VLANs.
4. Enter <<var_ucs_t004_access_vlan_name>> as the VLAN Name.
5. Enter <<var_t004_access_vlan_id>> as the VLAN ID.
6. Click OK.
7. Click OK.




8. Right-Click > Create VLANs
9. Enter <<var_ucs_t004_internal_vlan_name>> as the VLAN Name
10. Enter <<var_t004_internal_vlan_id>> as the VLAN ID
11. Click OK
12. Click OK

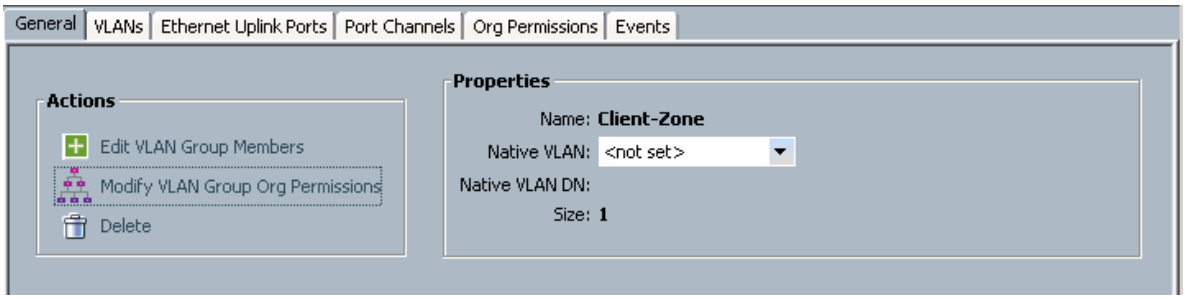



13. Right-Click > Create VLANs
14. Enter <<var_ucs_t004_nfs_vlan_name>> as the VLAN Name
15. Enter <<var_t004_nfs_vlan_id>> as the VLAN ID
16. Click OK
17. Click OK



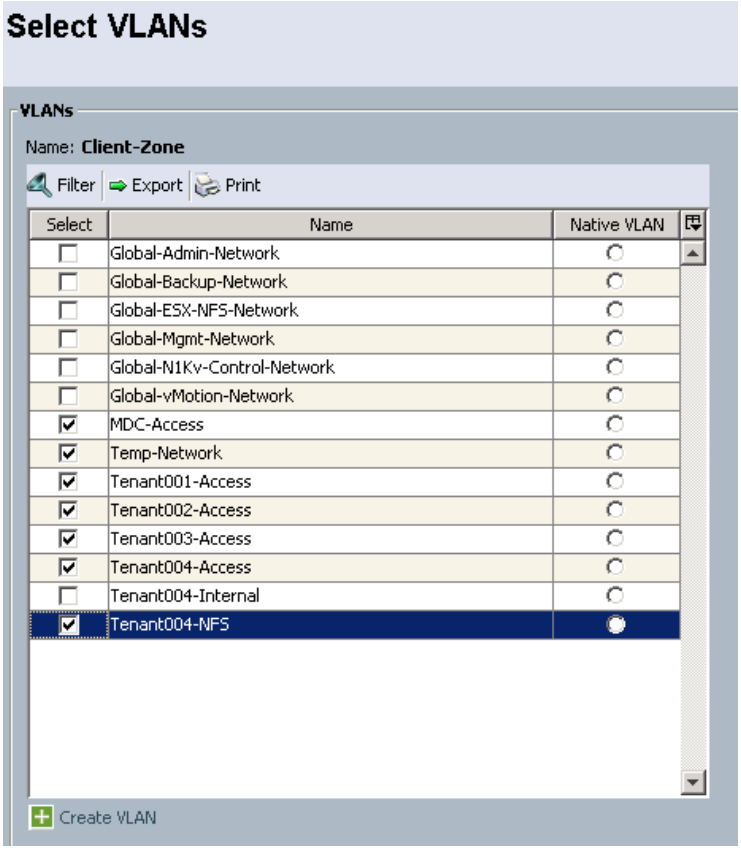

18. Go to LAN Tab > LAN Cloud > VLAN Groups.
19. Select VLAN group Client-Zone.
20. Click the Info Icon 

on the right side of the list.
21. Click Edit VLAN Group Members.



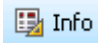

22. Select <<var_ucs_t004_access_vlan_name>> and <<var_ucs_t004_nfs_vlan_name>>.

23. Click Finish.



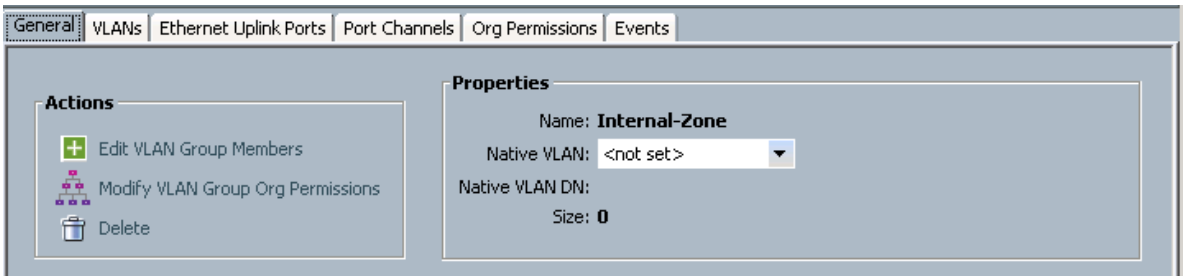

24. Click OK.

25. Select VLAN group Internal-Zone in the right pane

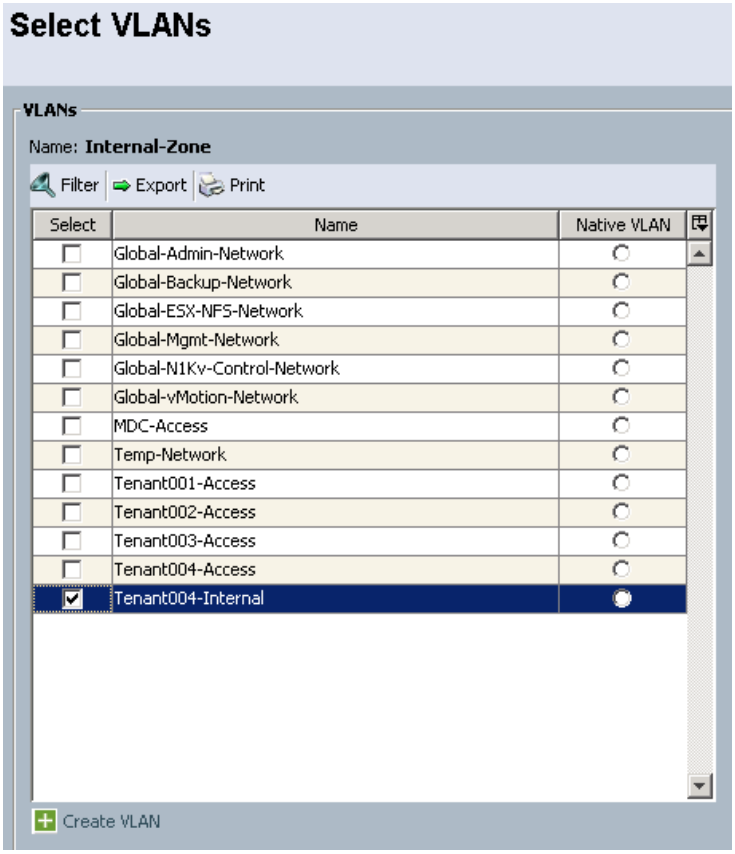
26. Click the Info Icon 

on the right side of the list

27. Click Edit VLAN Group Members




28. Select <<var_ucs_t004_internal_vlan_name>>
29. Click Finish
30. Click OK



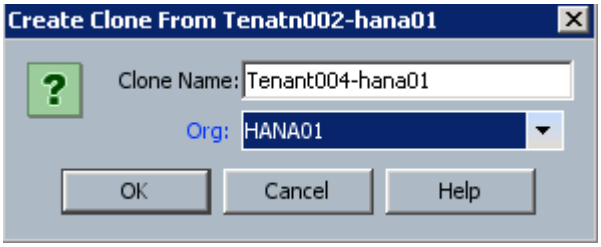

31. Click OK

## Create Service Profile for the SAP HANA node on a Cisco UCS B460 M4 or C460 M4 Server

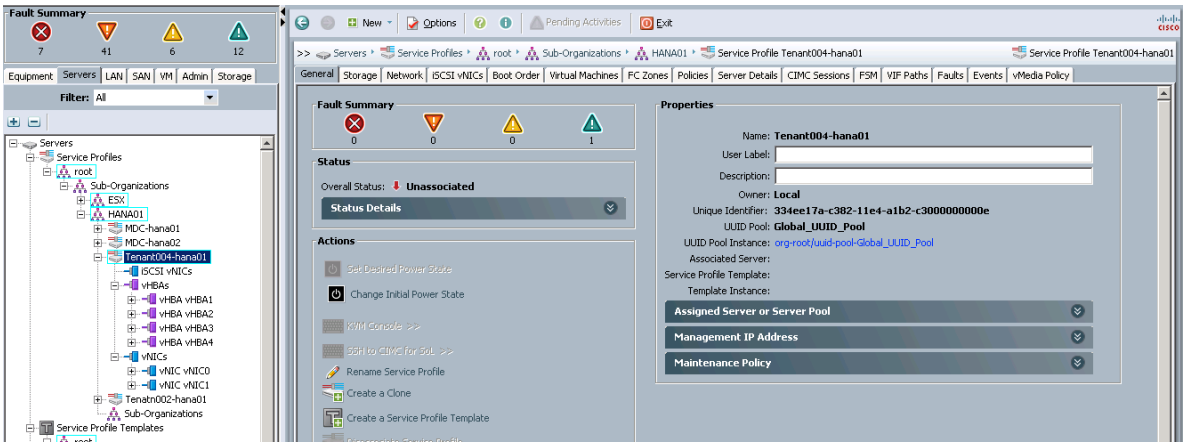
To create a service profile, complete the following steps:

1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. Select an existing Service Profile in the Sub-Organization

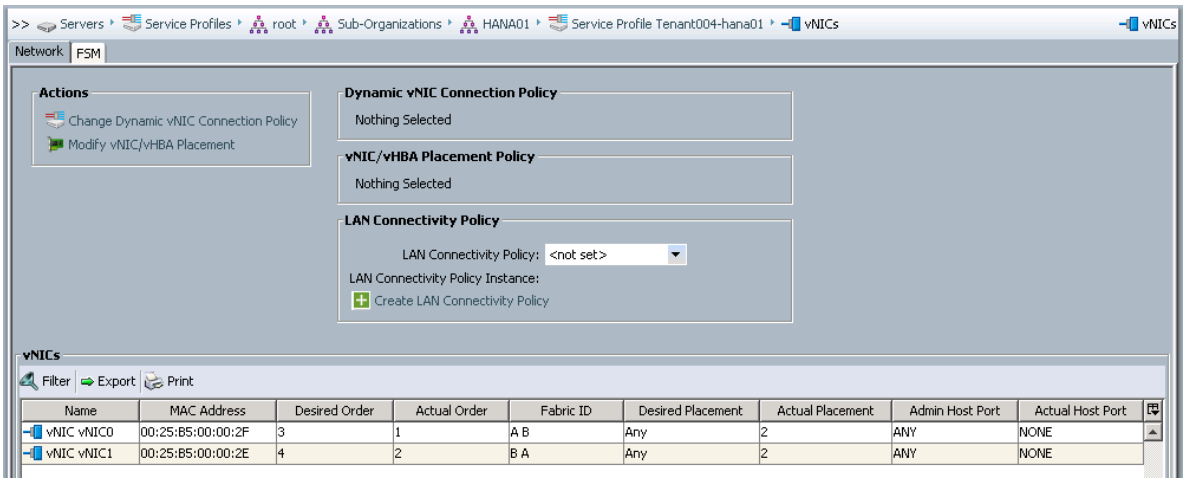
3. Click Create a Clone
4. Enter <<var_ucs_t004_hana1_sp_name>> as the Name
5. Select <<var_ucs_hana01_org>> as the Org
6. Click OK




7. The Service Profile is available immediately

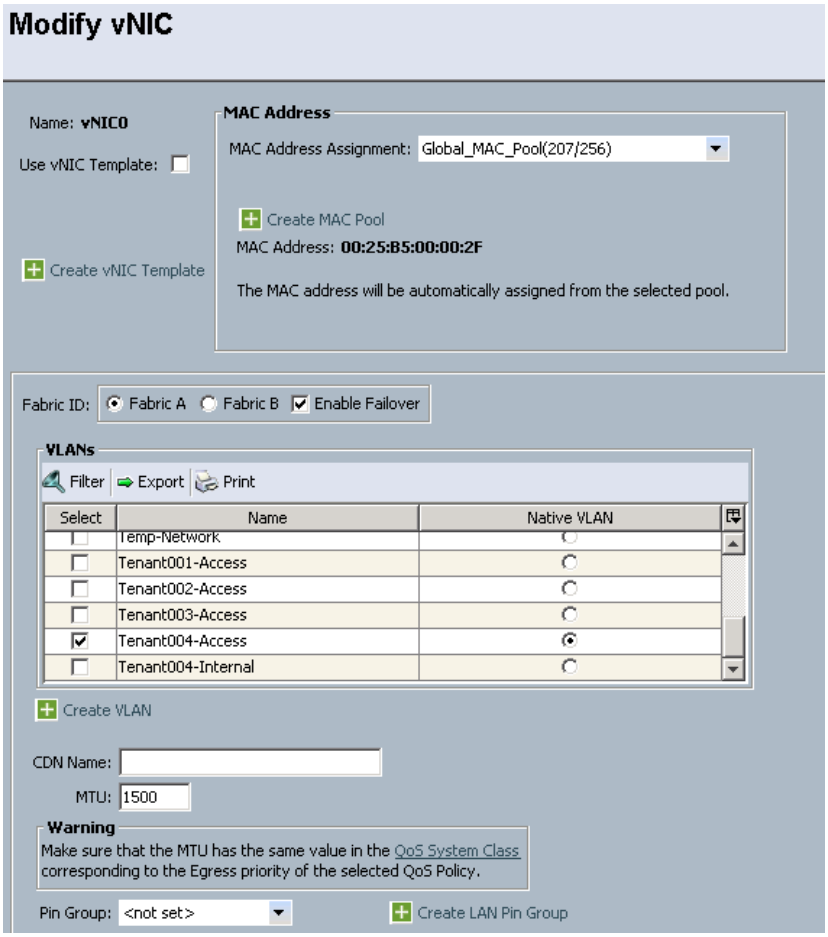



8. Click the Network Tab and select vNIC0
9. Click the Modify Icon



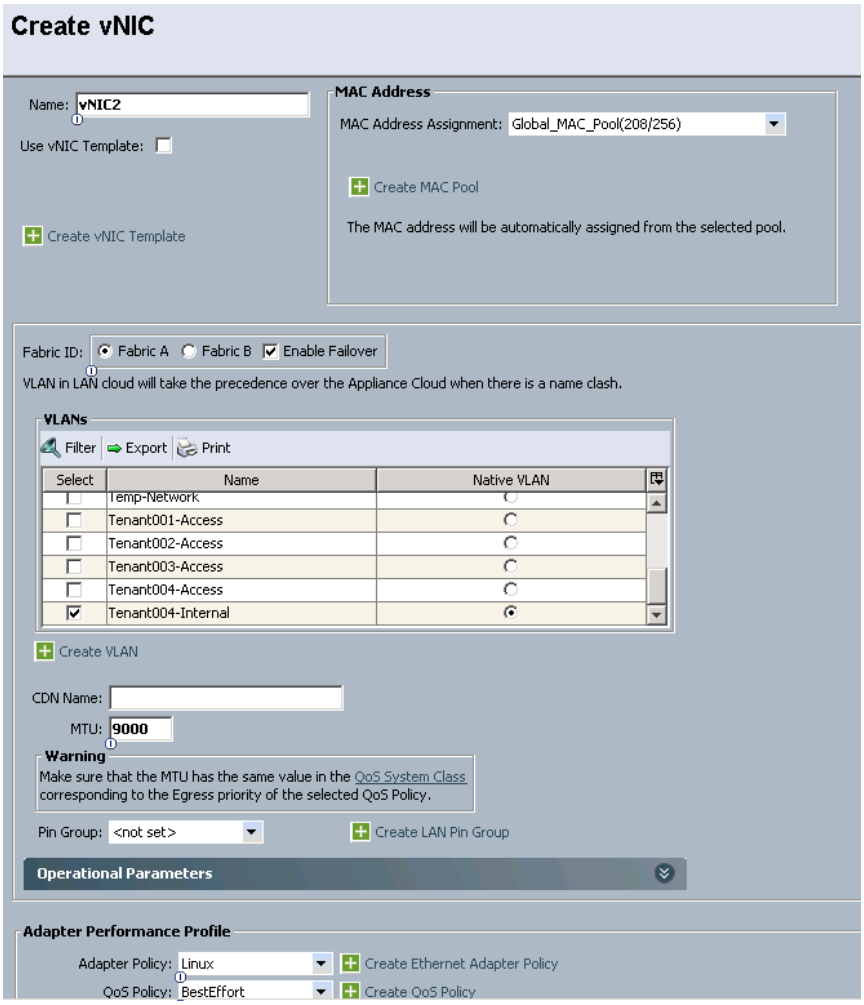

10. Select <<var_ucs_t004_access_vlan_name>> and make it the Native VLAN

11. Click OK



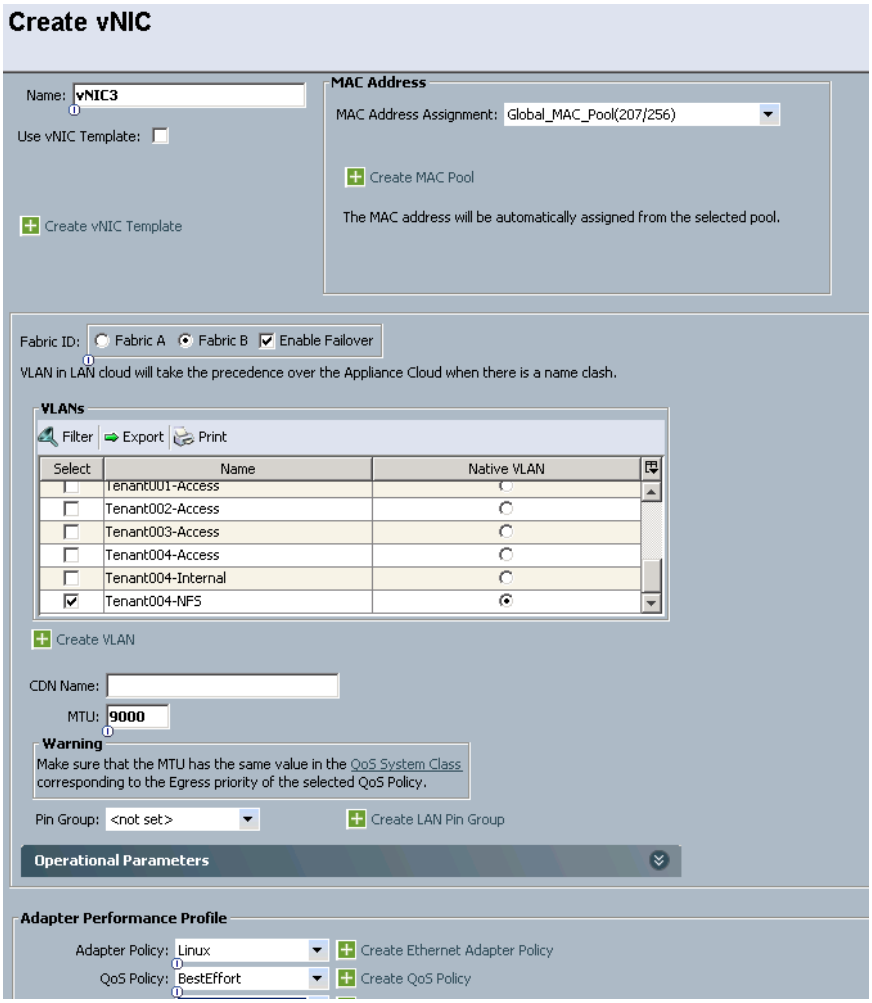

12. Click Add Icon

13. Enter vNIC2 as the Name
14. Select <<var_ucs_global_mac_pool_name>> from the MAC Address Assignment drop-down menu
15. Select Fabric A and Enable Failover In the Fabric ID section
16. Select <<var_ucs_t004_internal_vlan_name>> as the VLAN and make it the Native VLAN
17. Enter 9000 as the MTU
18. Select Linux as the Adapter Policy
19. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy

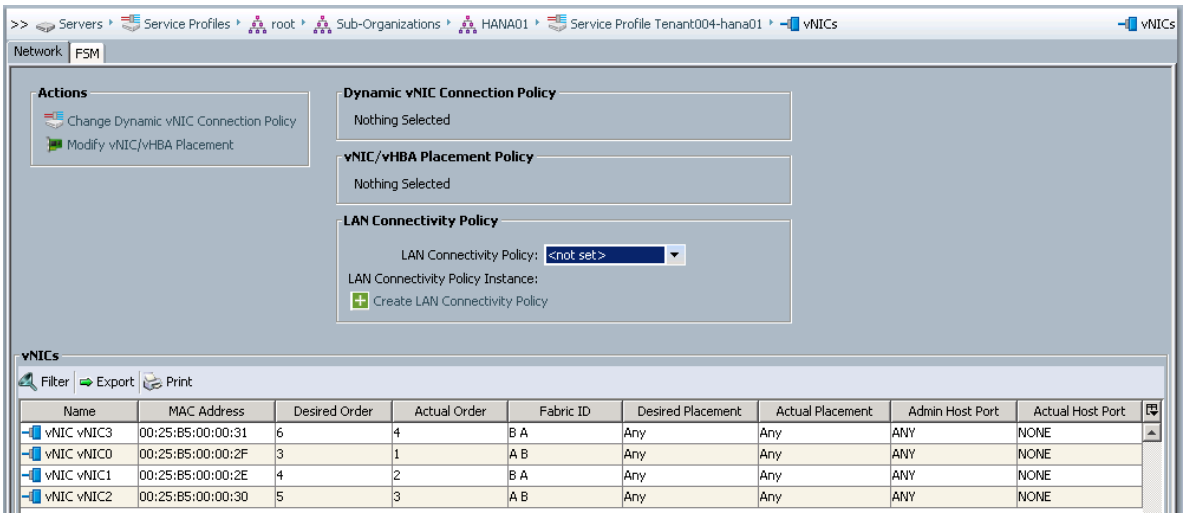



20. Click OK
21. Click Add Icon

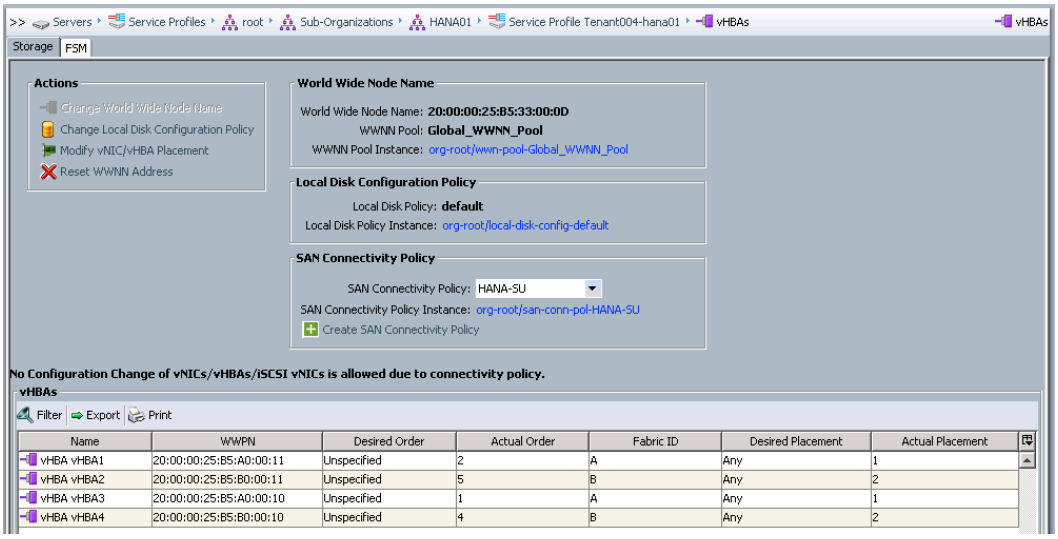
22. Enter vNIC3 as the Name
23. Select <<var_ucs_global_mac_pool_name>> from the MAC Address Assignment drop-down menu
24. Select Fabric B and Enable Failover In the Fabric ID section
25. Select <<var_ucs_t004_nfs_vlan_name>> as the VLAN and make it the Native VLAN
26. Enter 9000 as the MTU
27. Select Linux as the Adapter Policy
28. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy




29. Click OK
30. Click Save Changes
31. Click OK




32. Click the Storage Tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX



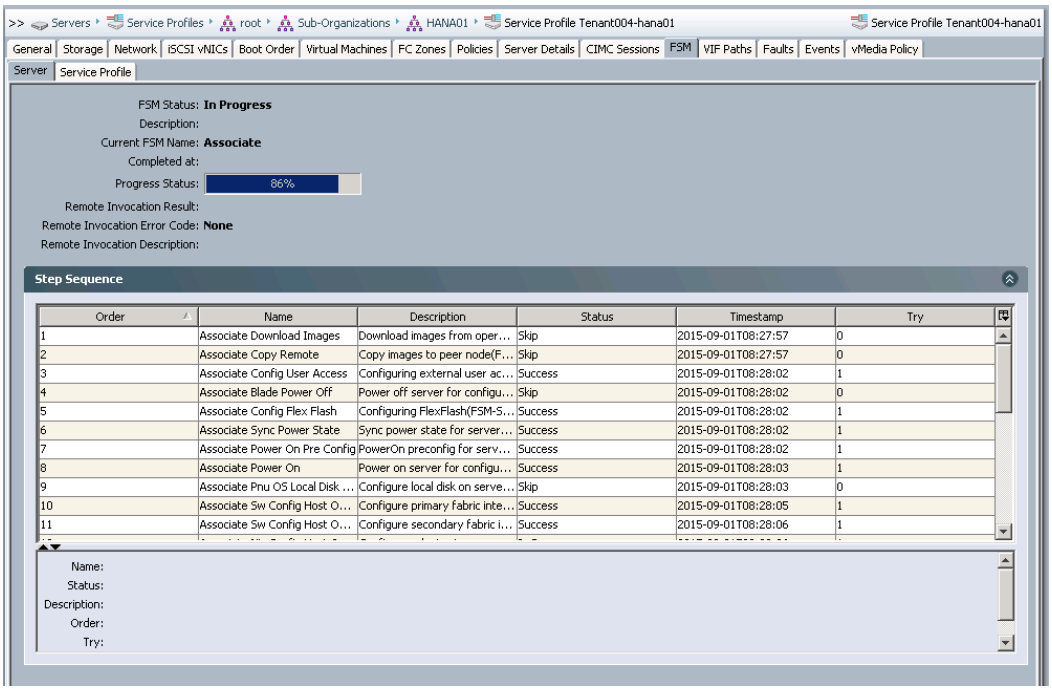

33. Select the General tab, Click Change Service Profile Association

34. Select “Select existing Server” from the Server Assignment drop-down menu

35. Select a server that meets the requirements, click OK

36. Click Yes

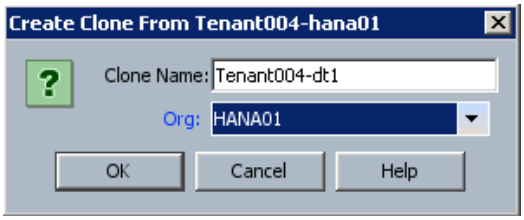
37. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.



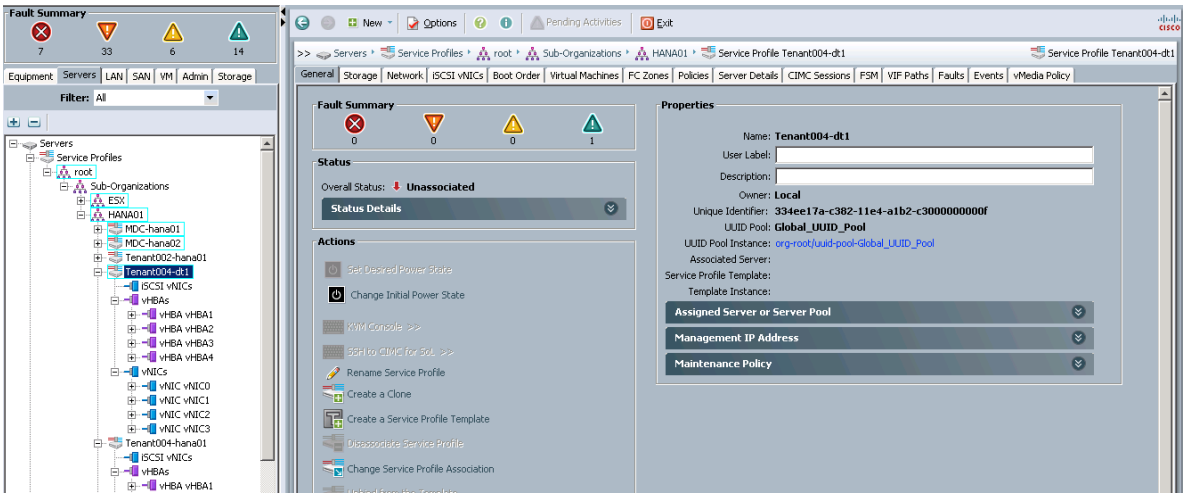

## Create Service Profile for the SAP HANA DT node on a Cisco UCS B200 M4 or C220 M4 Server

To create a service profile, complete the following steps:

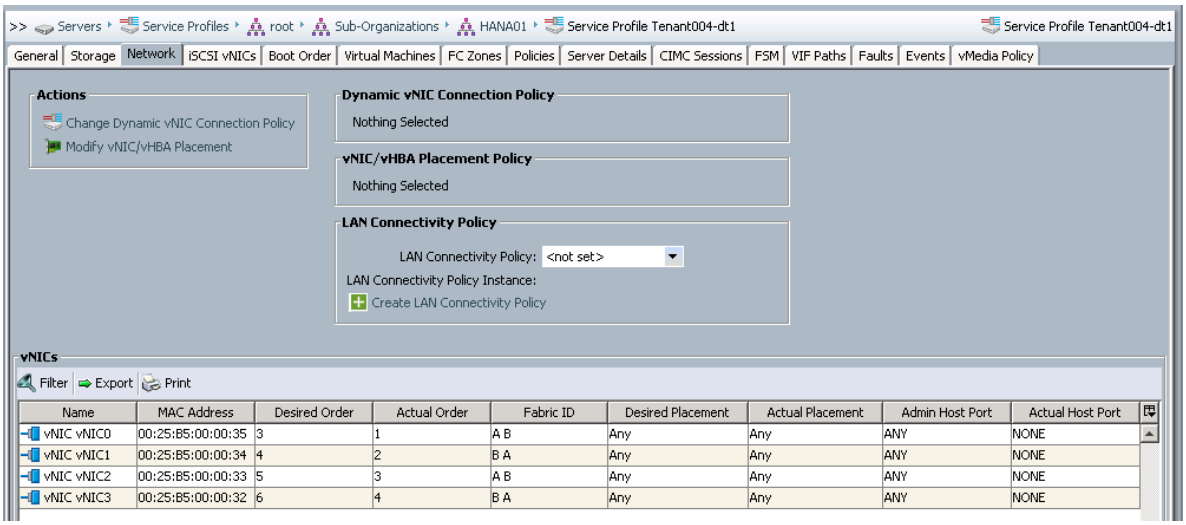
1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. Select the existing Service Profile of the SAP HANA Node <<var_ucs_t004_hana1_sp_name>>
3. Click Create a Clone
4. Enter <<var_ucs_t004_dt1_sp_name>> as the Name
5. Select <<var_ucs_hana01_org>> as the Org
6. Click OK



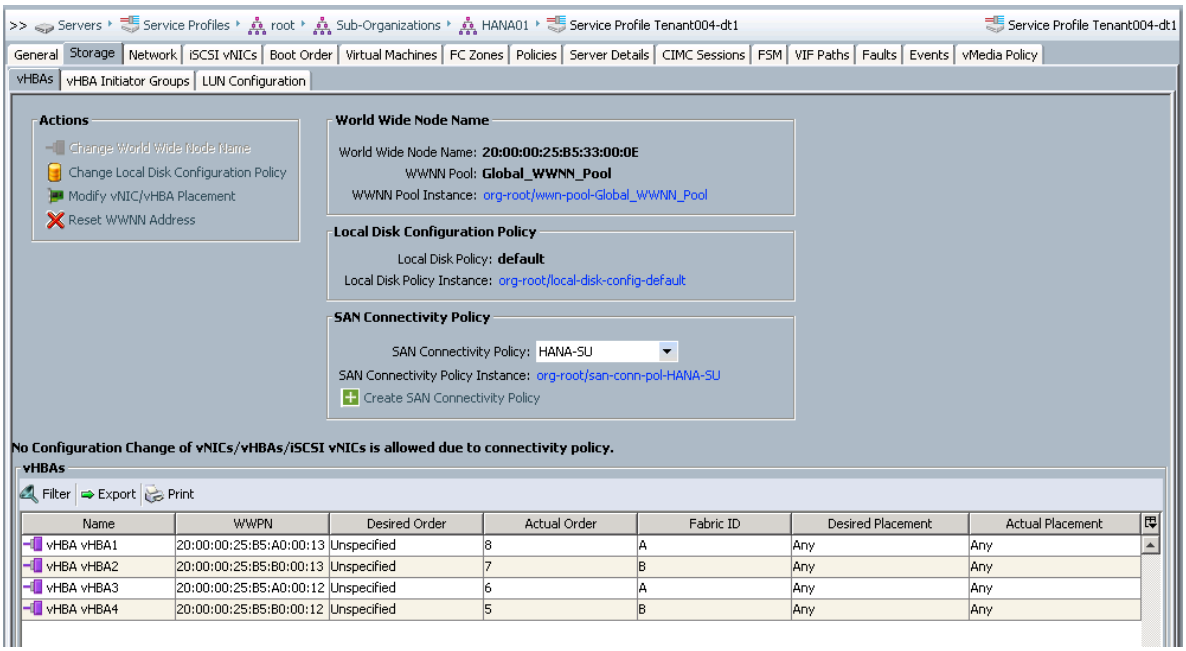

7. The Service Profile is available immediately



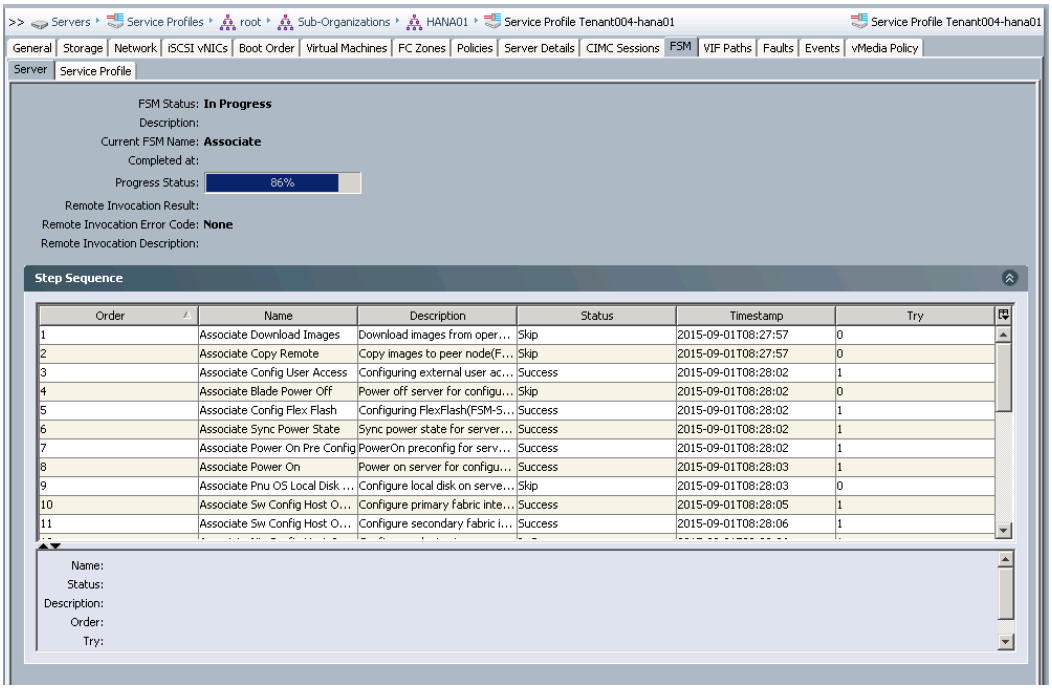

8. Click the Network Tab and check the MAC addresses, those are required to configure the interfaces on the operating system later in the process




9. Click the Storage tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX




10. Select the General tab, Click Change Service Profile Association
11. Select “Select existing Server” from the Server Assignment drop-down menu
12. Select a server that meets the requirements (Cisco UCS B200 or C2x0), click OK
13. Click Yes
14. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.




## Configure Cisco MDS Switches

For every Service Profile in the Cisco UCS one or more SAN Zones are required per Cisco MDS switch.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t004-hana01>> vsan 10
zone name <<var_zone_t004-hana01>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:11
   exit

zone clone zone_temp <<var_zone_t004-dt01>> vsan 10
zone name <<var_zone_t004-dt01>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:13
   exit
```

```
zoneset name CRA-EMC-A vsan 10
member <<var_zone_t004-hana01>>
member <<var_zone_t004-dt01>>
exit

zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

…
zone name zone_t004-dt01 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
```

```
    interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
    pwwn 20:00:00:25:b5:a0:00:13

  zone name zone_t004-hana01 vsan 10
    interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
    pwwn 20:00:00:25:b5:a0:00:11

  CRA-EMC-A#
  CRA-EMC-A# show zoneset brief
  zoneset name CRA-EMC-A vsan 10
    zone zone_esx-host1
    zone zone_esx-host2
    zone zone_esx-host3
    zone zone_esx-host4
    zone zone_esx-host5
    zone zone_esx-host6
    zone zone_esx-host7
    zone zone_esx-host8
    zone zone_esx-host9
    zone zone_esx-host10
    zone zone_t002-vhana1
    zone zone_MDC-hana01
    zone zone_t004-hana01
    zone zone_t004-dt01
  CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t004-hana01>> vsan 20
zone name <<var_zone_t004-hana01>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:11
   exit

zone clone zone_temp <<var_zone_t004-dt01>> vsan 20
zone name <<var_zone_t004-dt01>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:13
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_t004-hana01>>
exit

zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
```

```
…
zone name zone_t004-dt01 vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:13

zone name zone_t004-hana01 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:11

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_MDC-hana01
  zone zone_t004-hana01
```

```
  zone zone_t004-dt01
CRA-EMC-B#
```

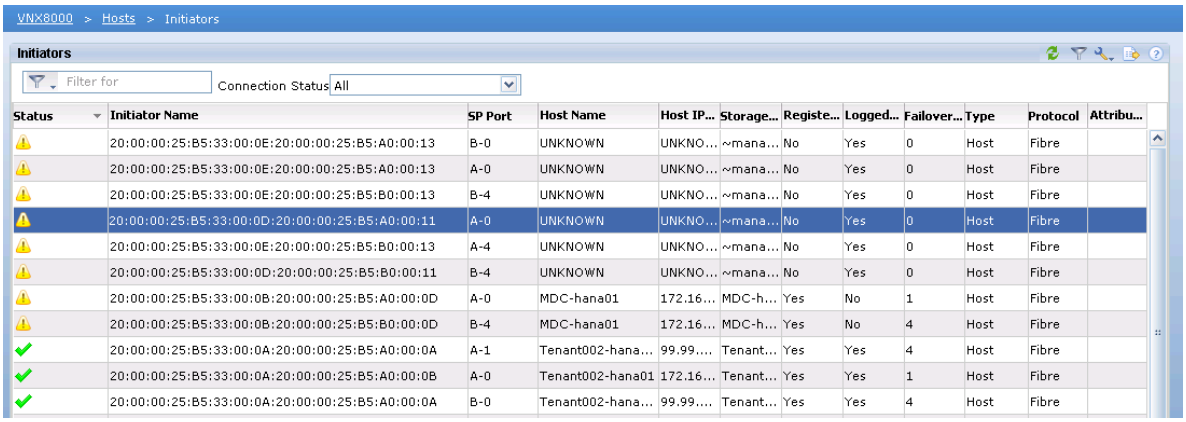
4. Save the running configuration as startup configuration

```
Copy run start
```

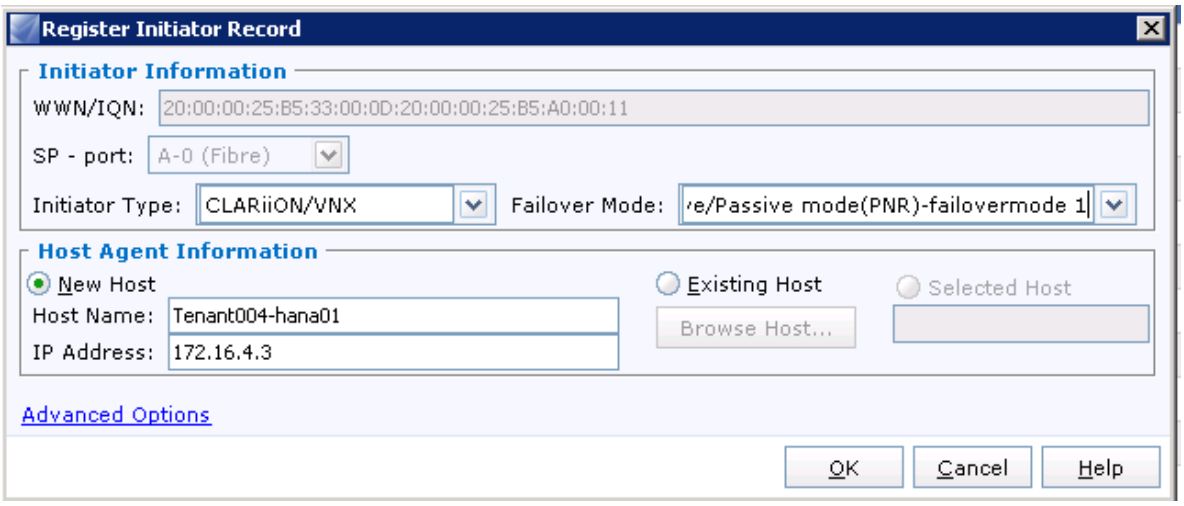
## Configure EMC VNX

### Register Host

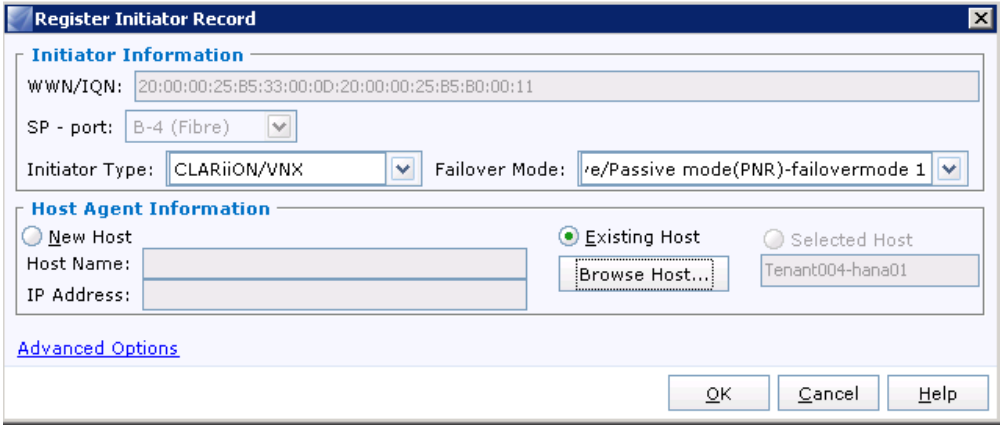
1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators



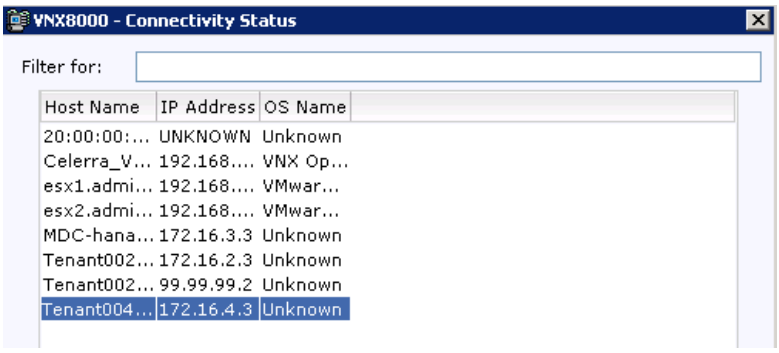

2. Select one of the unregistered entries for the host <<var_ucs_t004_hana1_name>>, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
5. Enter <<var_ucs_t004_hana1_name>> as the Host Name (indicates the relationship to the Service Profile)
6. Enter <<var_t004_hana1_access_ip>> as the IP Address
7. Click OK
8. Click Yes
9. Click OK
10. Click OK



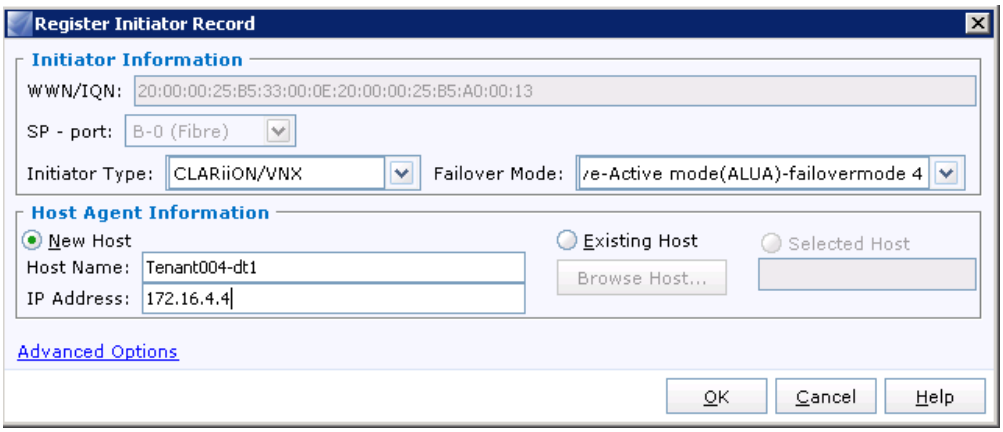

11. Select the second Entry for this host <<var_ucs_t004_hana1_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and Click Browse Host



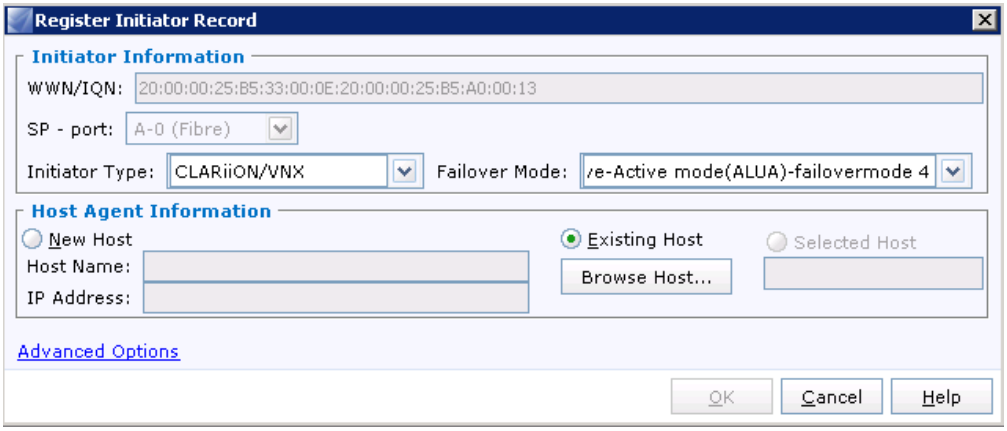

15. Select <<var_ucs_t004_hana1_name>> and click OK



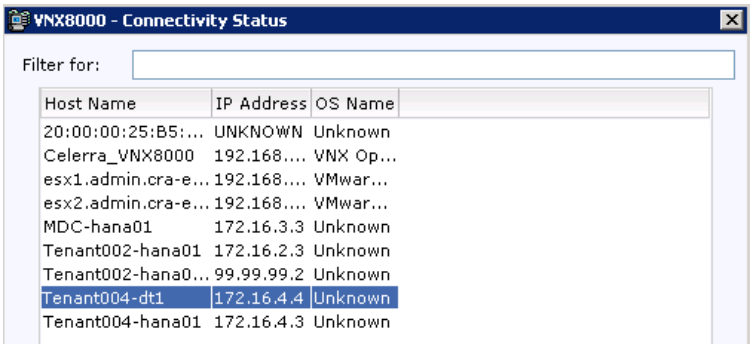
16. Click OK
17. Click Yes
18. Click OK
19. Click OK
20. Select one of the unregistered entries for the host <<var_ucs_t004_dt01_name>>, click Register
21. Select CLARiiON/VNX as the Initiator Type
22. Select Active/Active mode(ALUA)-failovermode 4 as the Failover Mode
23. Enter <<var_ucs_t004_dt1_name>> as the Host Name (indicates the relationship to the Service Profile)
24. Enter <<var_t004_dt1_access_ip>> as the IP Address
25. Click OK
26. Click Yes
27. Click OK
28. Click OK




29. Select the second Entry for this host <<var_ucs_t004_dt1_name>>, click Register
30. Select CLARiiON/VNX as the Initiator Type
31. Select Active/Active mode(ALUA)-failovermode 4 as the Failover Mode
32. Select Existing Host and click Browse Host




33. Select <<var_ucs_t004_dt1_name>> and click OK




34. Click OK

35. Click Yes

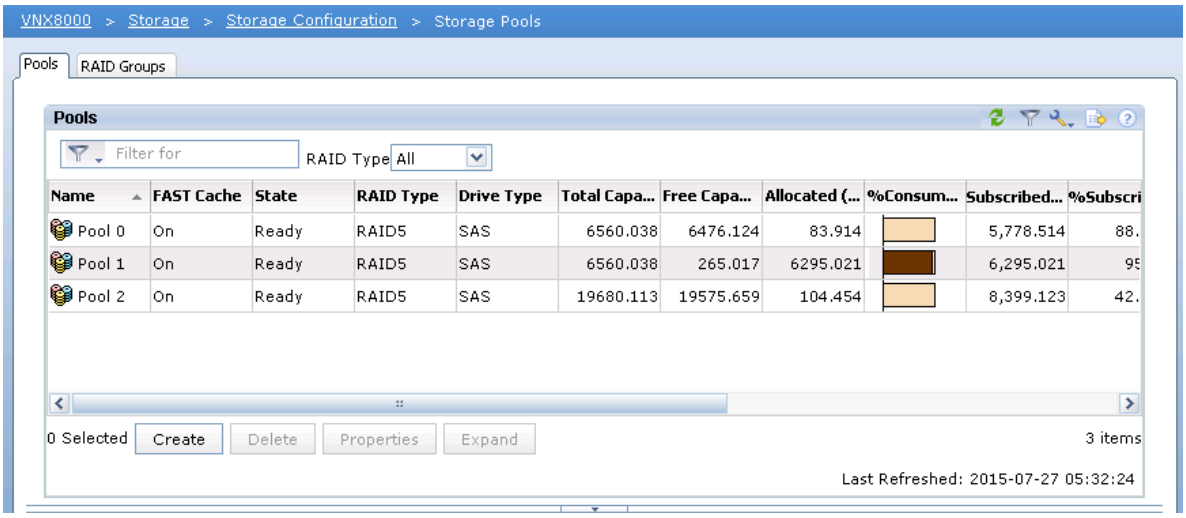
36. Click OK

37. Click OK

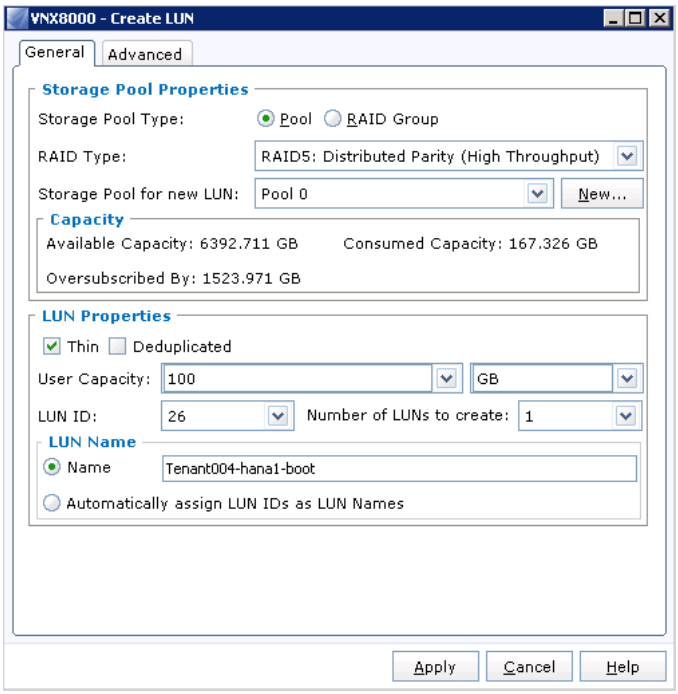
38. Repeate Step 28 to Step 36 for every entry of host <<var_ucs_t004_dt1_name>>.

## Create LUNs

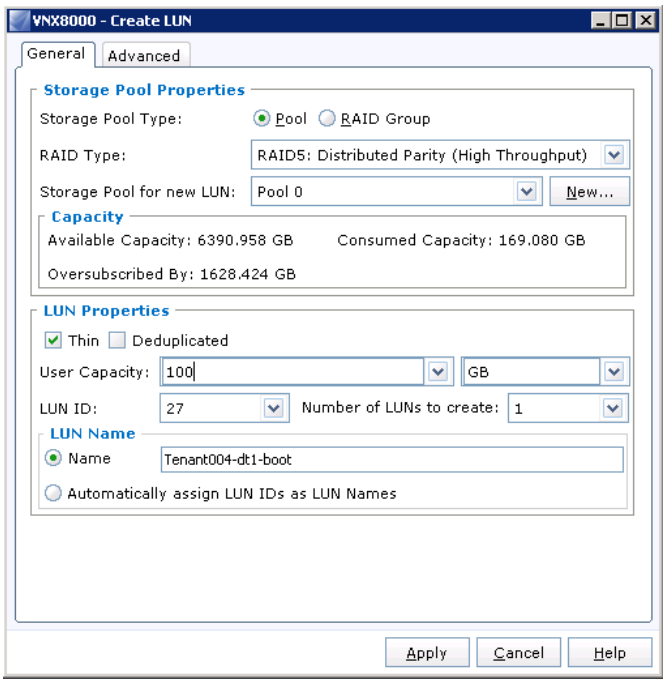
1. Navigate to Storage > Storage Pool



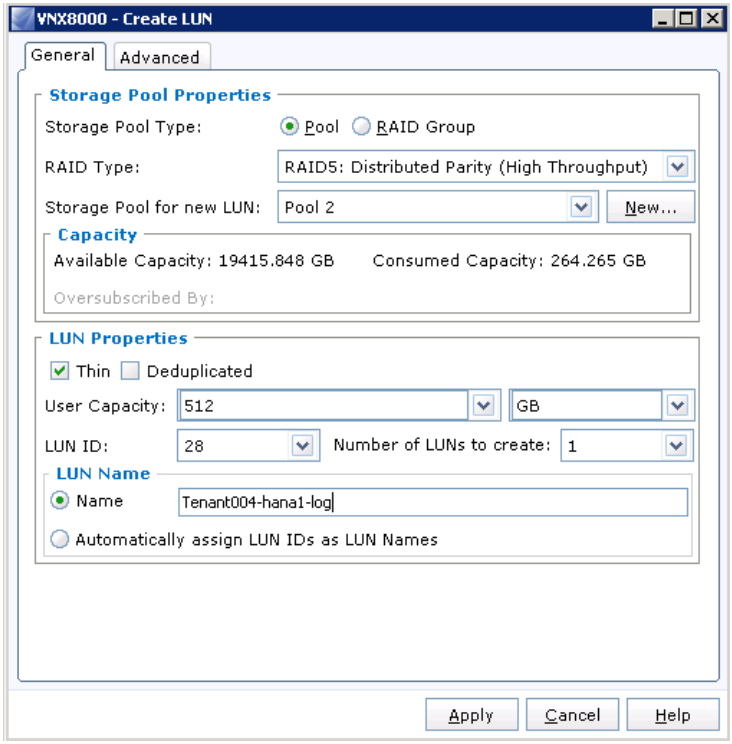

2. Right-Click Pool 0
3. Select Create LUN
4. Enter 100 GB as the User Capacity
5. Click Name and enter <<var_ucs_t004_hana1_name>>-boot
6. Click Apply
7. Click Yes
8. Click OK



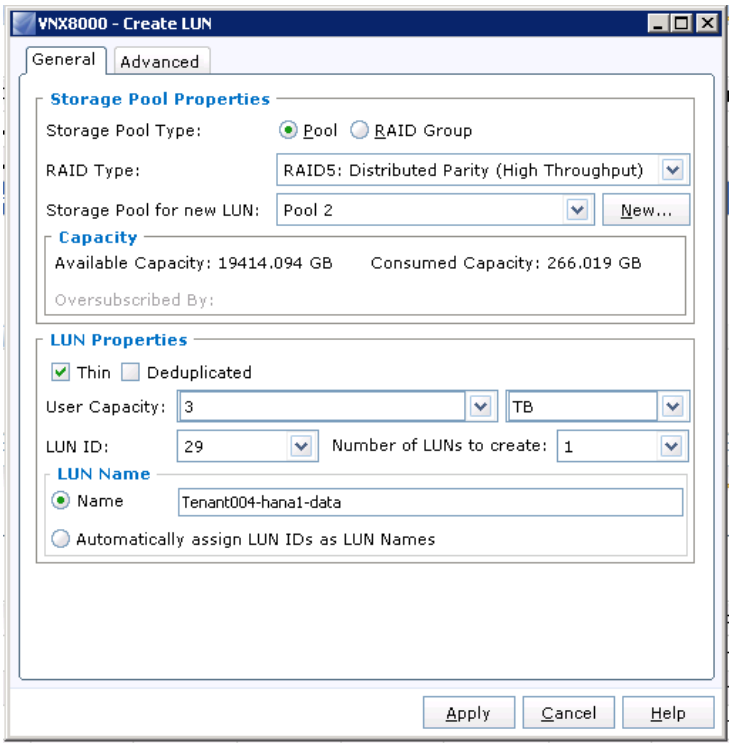

9. Enter 100 GB as the User Capacity
10. Click Name and enter <<var_ucs_t004_dt1_name>>-boot
11. Click Apply
12. Click Yes
13. Click OK




14. Click Cancel
15. Right-click Pool 2
16. Select Create LUN
17. Enter 512 GB as the User Capacity
18. Click Name and enter <<var_ucs_t004_hana1_name>>-log
19. Click Apply
20. Click Yes
21. Click OK




22. Enter 3 TB as the User Capacity
23. Click Name and enter <<var_ucs_t004_hana1_name>>-data
24. Click Apply
25. Click Yes
26. Click OK



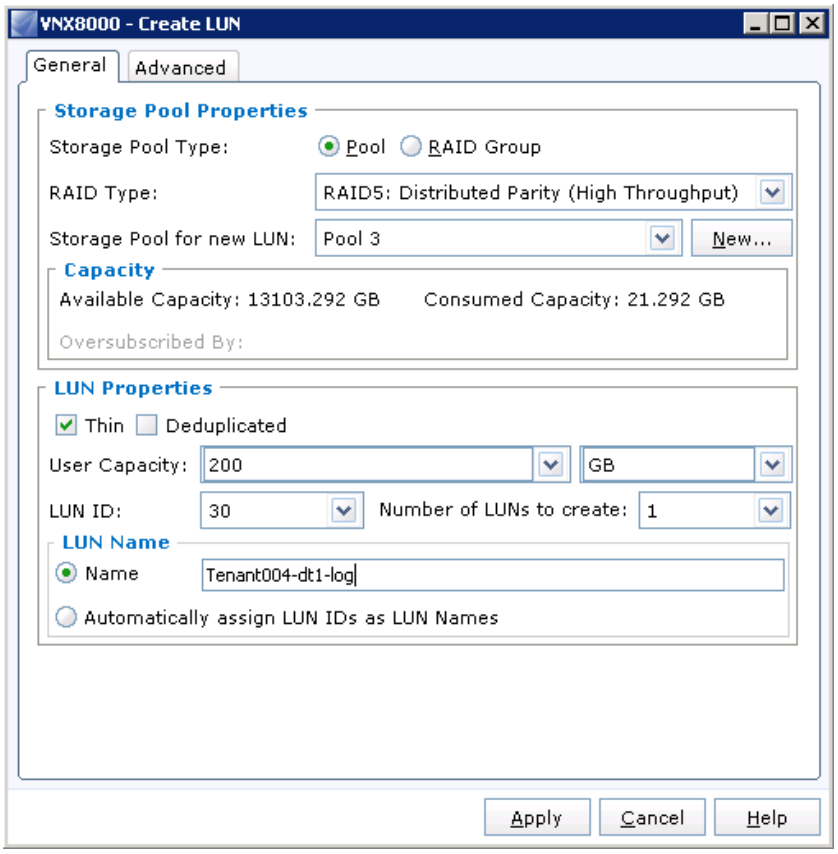

27. Click Cancel
28. In the Pools section click Create
29. In the Performance Section Select RAID5 (8+1) as the RAID configuration
30. Select 72 as Number of SAS Disks
31. Click the Advanced tab
32. Disable FAST Cache
33. Click OK
34. Click Yes
35. Click Yes
36. Click OK
37. Right-Click Pool 3
38. Select Create LUN
39. Enter 200 GB as the User Capacity

40. Click Name and enter <<var_ucs_t004_dt1_name>>-log

41. Click Apply

42. Click Yes

43. Click OK



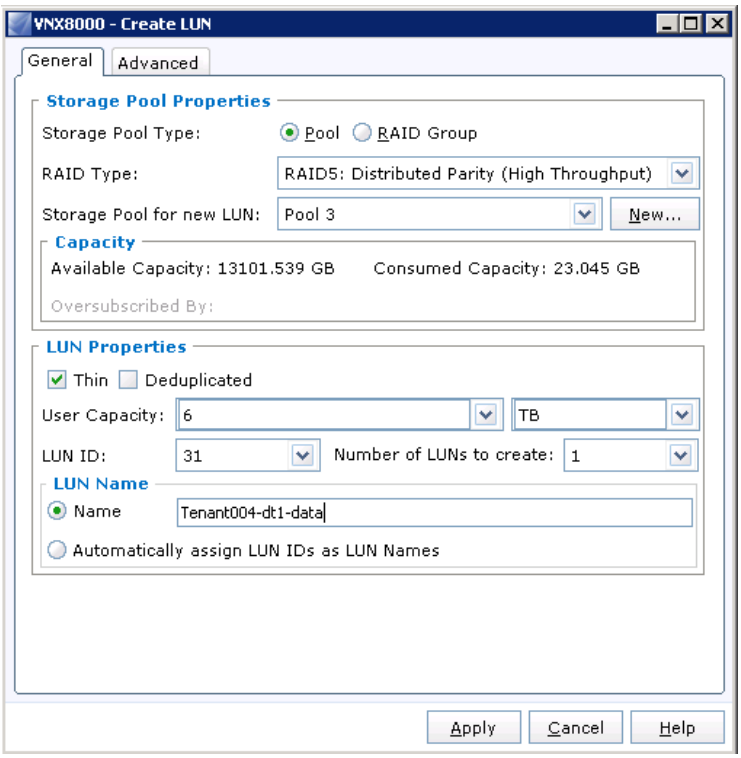

44. Enter 6 TB as the User Capacity

45. Click Name and enter <<var_ucs_t004_dt1_name>>-data

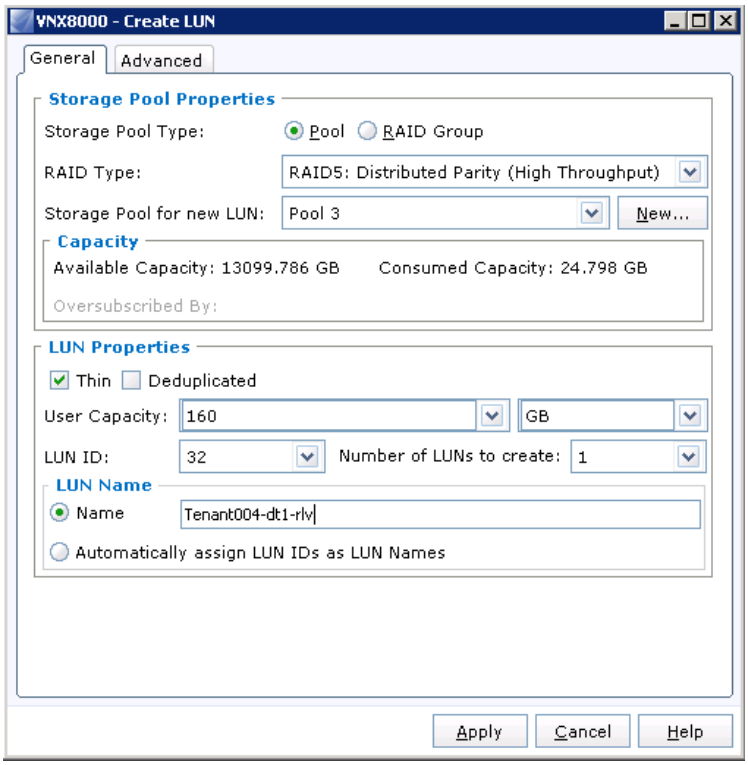
46. Click Apply

47. Click Yes

48. Click OK



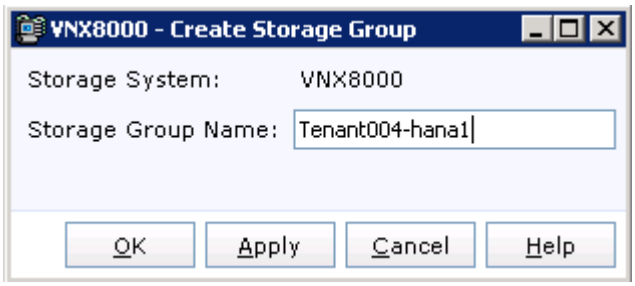

49. Enter 160 GB as the User Capacity
50. Click Name and enter <<var_ucs_t004_dt1_name>>-rlv
51. Click Apply
52. Click Yes
53. Click OK



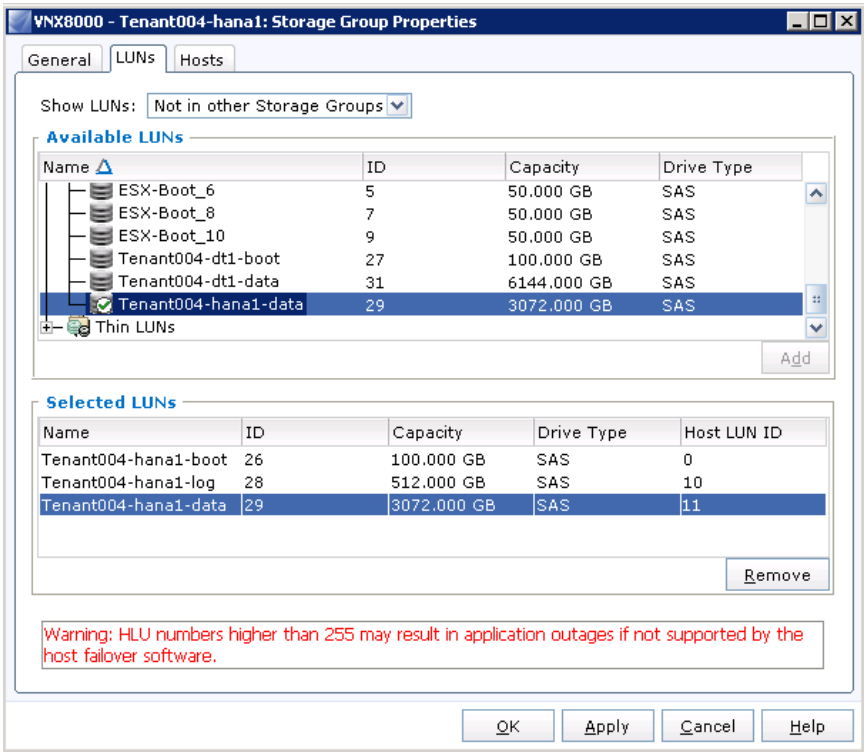

54. Click Cancel
55. Right-click Pool1, select Expand
56. Select a good number of additional disks based on the RAID configuration (5 or 9)
57. Click OK
58. Click Yes
59. Click OK

## Create Storage-Group

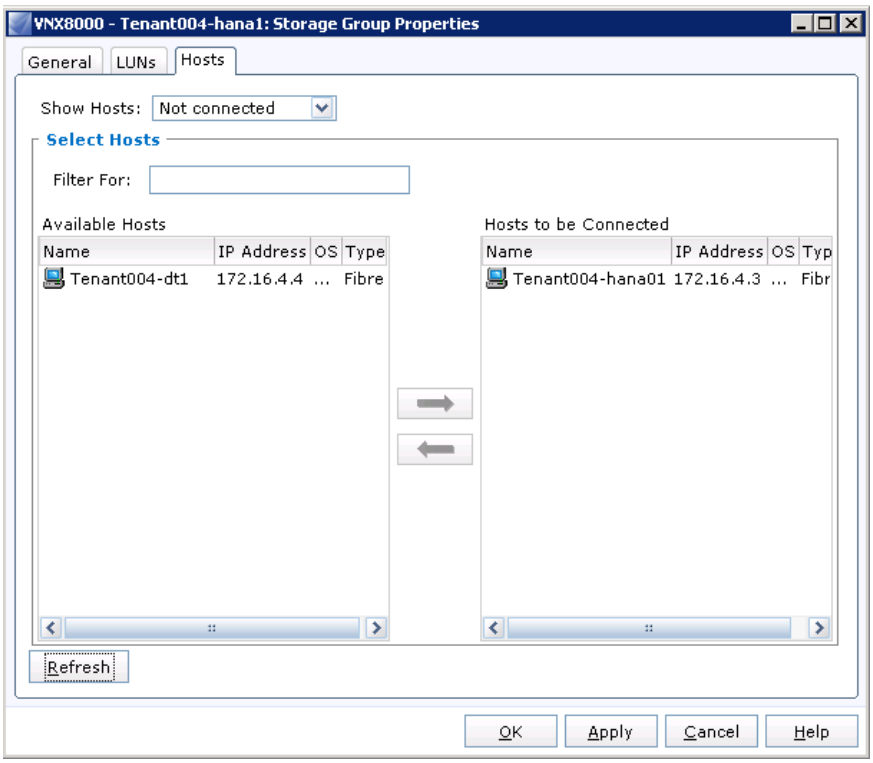
1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t004_hana1_sp_name>> as the Name
4. Click OK
5. Click Yes



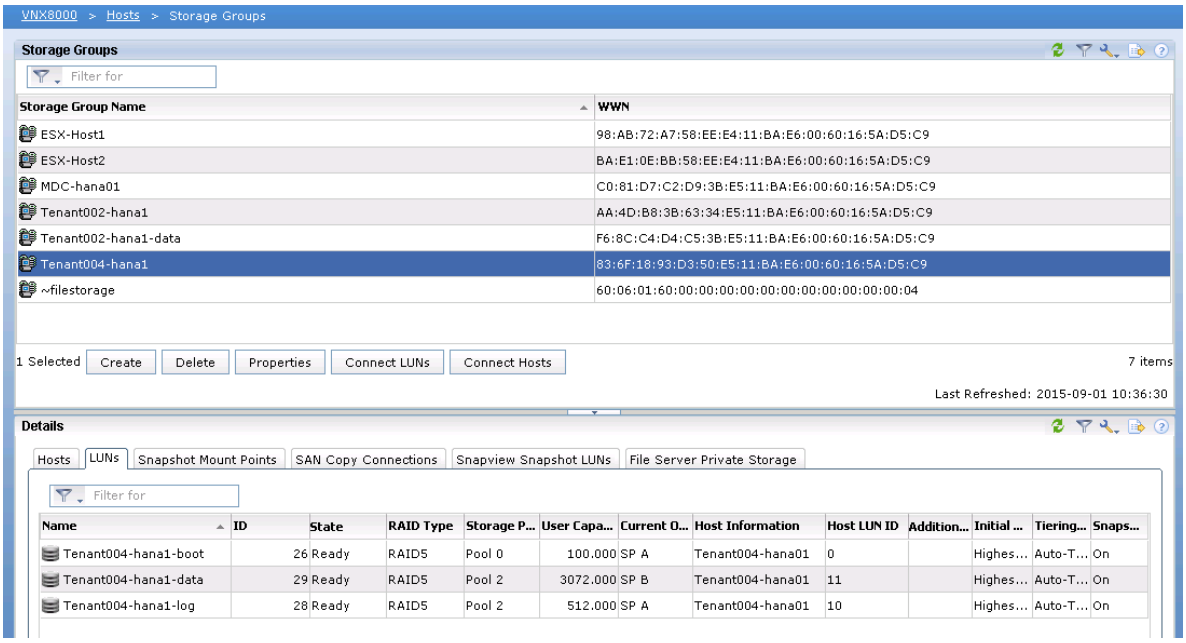

6. Click Yes
7. Select one of the three LUNs created and click Add
8. Repeat this for the other two LUNs
9. Select 0 as the Host LUN ID for <<var_ucs_t004_hana1_name>>-boot
10. Select 10 as the Host LUN ID for <<var_ucs_t004_hana1_name>>-log
11. Select 11 as the Host LUN ID for <<var_ucs_t004_hana1_name>>-data
12. Click Apply
13. Click Yes
14. Click OK



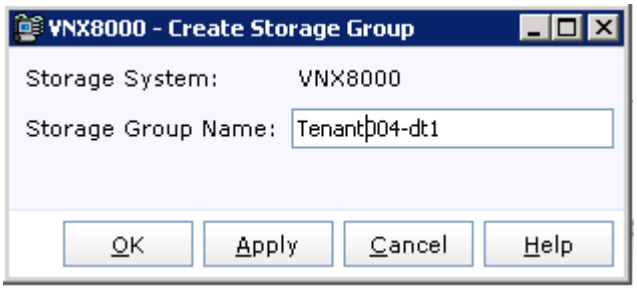
15. Click the Hosts tab
16. Select <<var_ucs_t004_hana1_name>> and click the -> icon
17. Click OK
18. Click Yes
19. Click OK




20. The result will look like the following

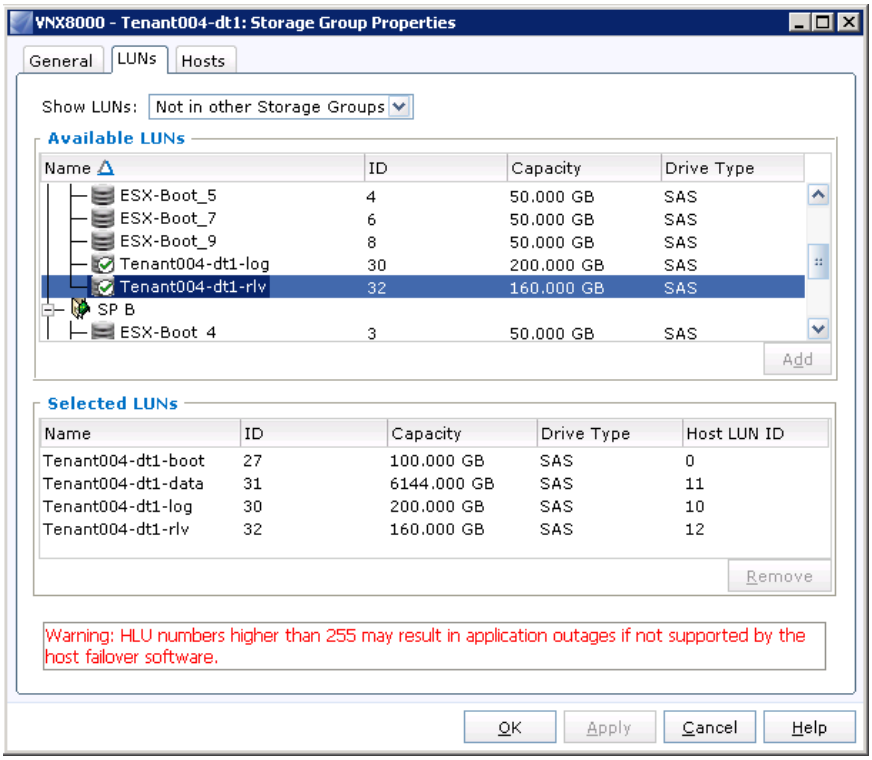



21. Click Create
22. Enter <<var_ucs_t004_dt1_sp_name>> as the Name
23. Click OK
24. Click Yes

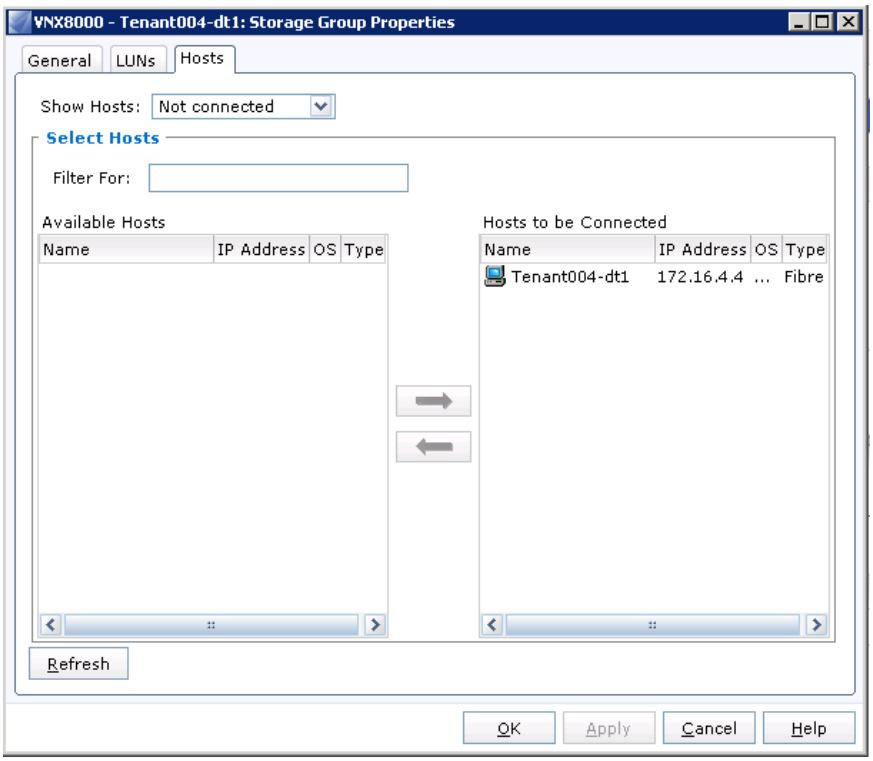



25. Click Yes
26. Select one of the three LUNs created and click Add
27. Repeat this for the other two LUNs
28. Select 0 as the Host LUN ID for <<var_ucs_t004_dt1_sp_name>>-boot
29. Select 10 as the Host LUN ID for <<var_ucs_t004_dt1_sp_name>>-log
30. Select 11 as the Host LUN ID for <<var_ucs_t004_dt1_sp_name>>-data

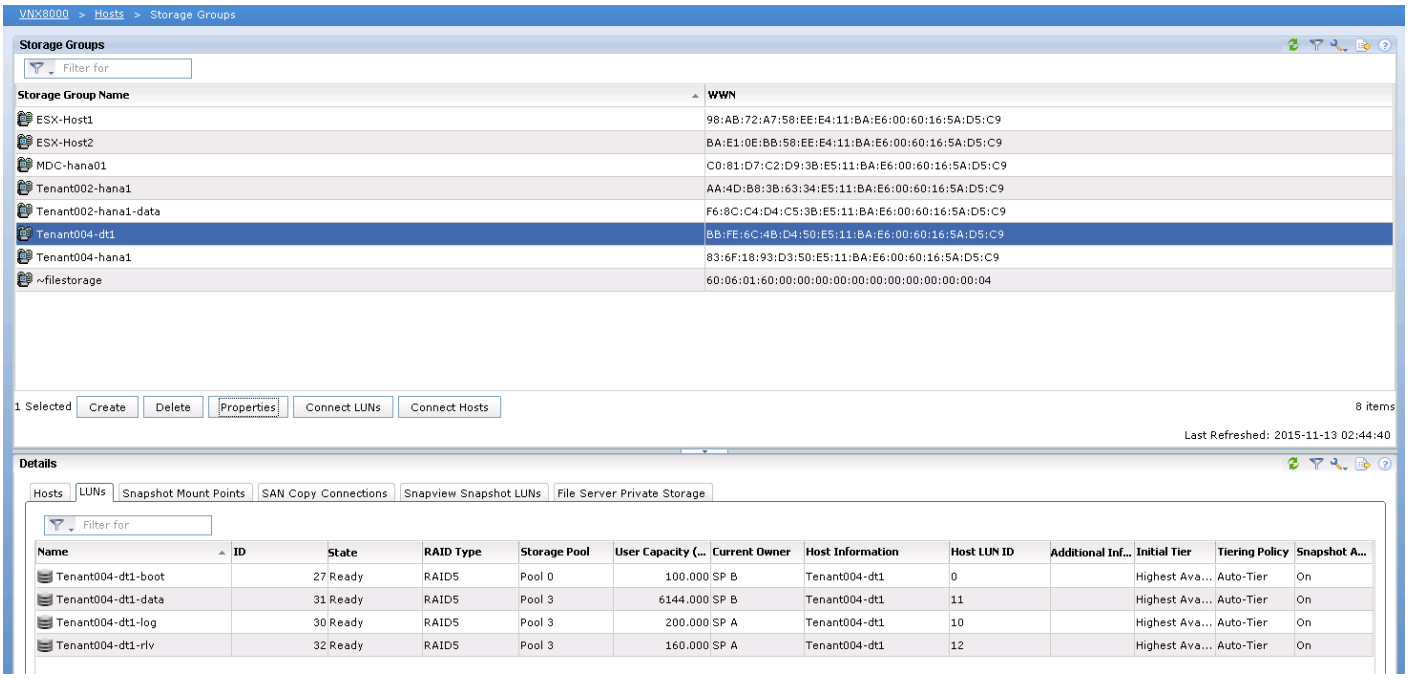
31. Select 12 as the Host LUN ID fo <<var_ucs_t004_dt1_sp_name>>-rlv
32. Click Apply
33. Click Yes
34. Click OK




35. Click the Hosts tab
36. Select <<var_ucs_t004_dt1_sp_name>> and click the -> icon
37. Click OK
38. Click Yes
39. Click OK




40. The result will look like the following

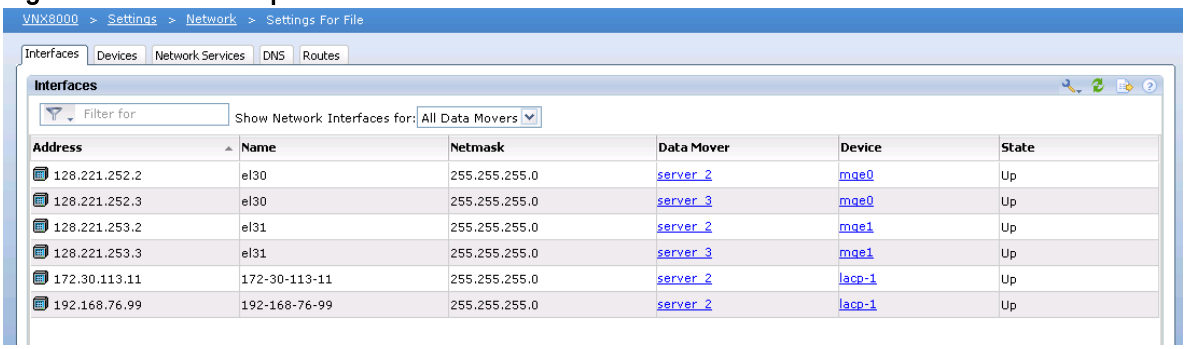



## Configure Network Interface

1. In EMC Unisphere GUI, Click Settings > Network > Settings for File

2. In the Interface tab, click Create

**Figure 336 EMC Unisphere – Interfaces**




3. Enter <<var_vnx_tenant004_nfs_storage_ip>> as the Address
4. Enter <<var_vnx_tenant004_if_name>> as the Name
5. Enter <<var_tenant004_nfs_mask>> as the Netmask
6. Enter 9000 as the MTU
7. Enter <<var_t004_access_vlan_id>> as the VLAN ID
8. Click OK

## Configure Filesystem and NFS Share

To create the Filesystem and NFS share for /hana/shared on the VNX storage, complete the following steps:

1. In EMC Unisphere GUI, Click Storage > Storage Configuration > File Systems
2. In the File Systems tab, click Create
3. Enter <<var_vnx_t004_fs_name>> as the File System Name
4. Enter 1 TB as the Storage Capacity
5. Click OK

Figure 337 EMC Unisphere – Create File System

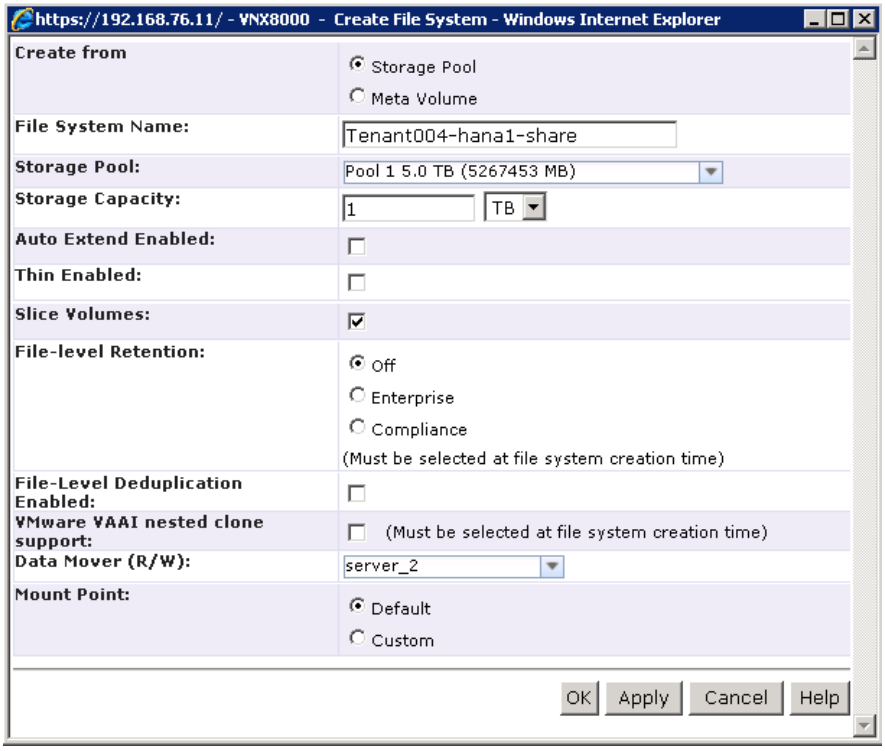
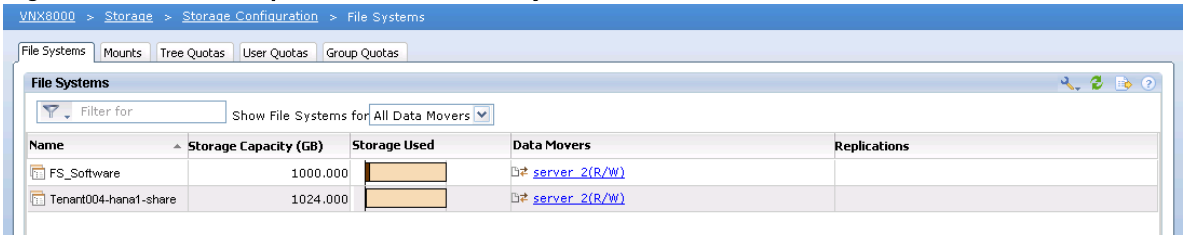
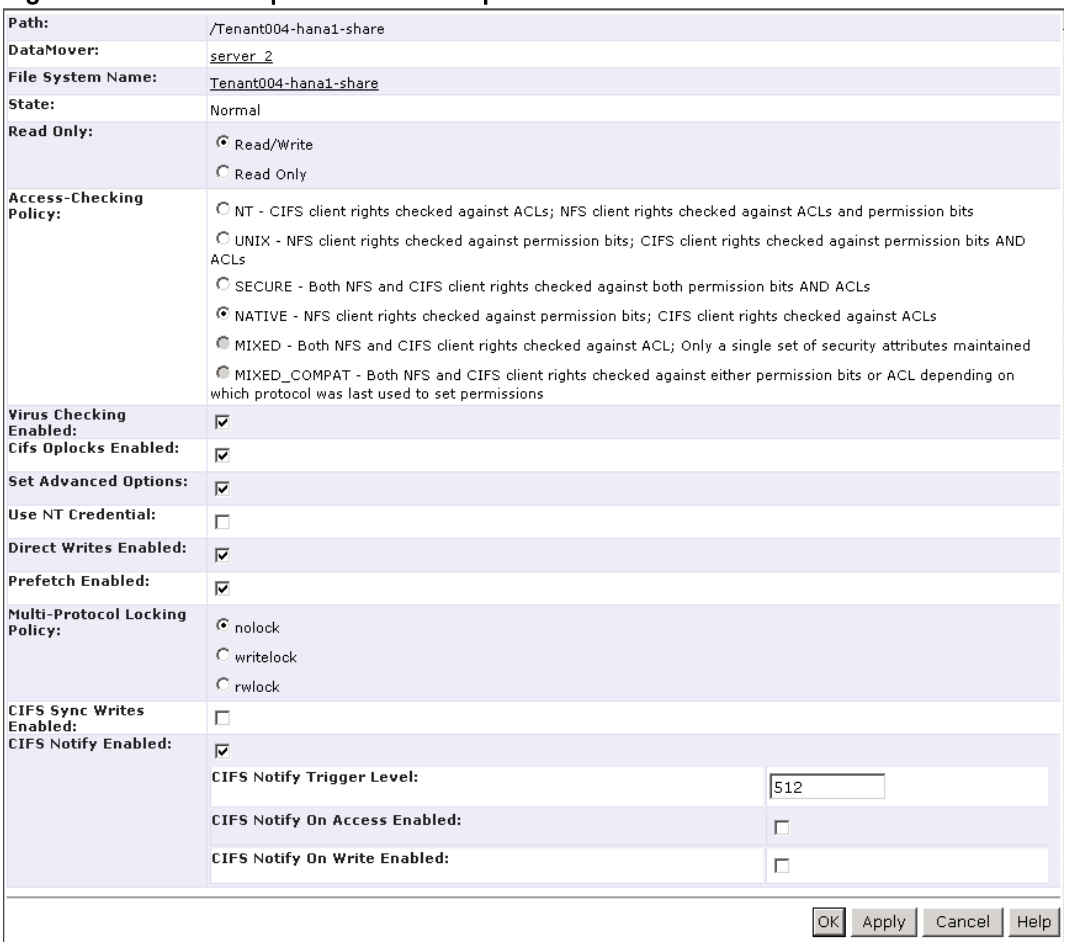



Figure 338 EMC Unisphere - List of File Systems




6. Click the Mounts tab
7. Select the path <<var_vnx_t004_fs_name>>
8. Click Properties
9. From the mount properties. Make sure Read/Write is selected and Native Access policy is selected.
10. Select the Set Advanced Options check box
11. Check the Direct Writes Enabled check box
12. Click OK

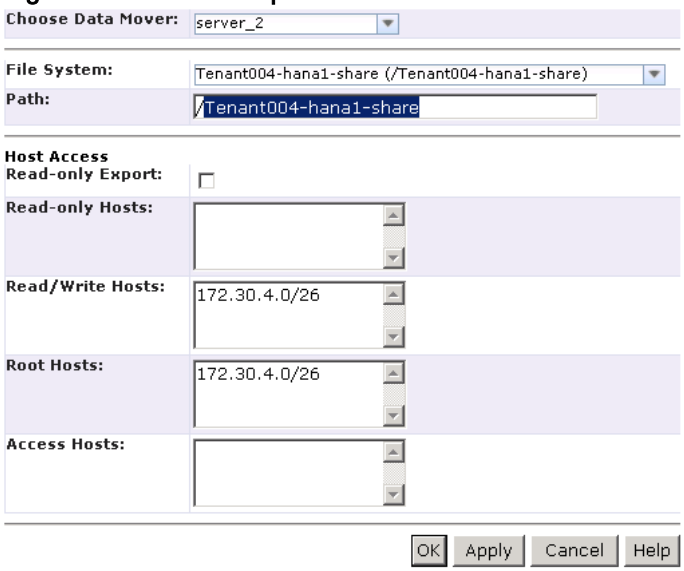
Figure 339 EMC Unisphere Mount Properties




## Create NFS Share

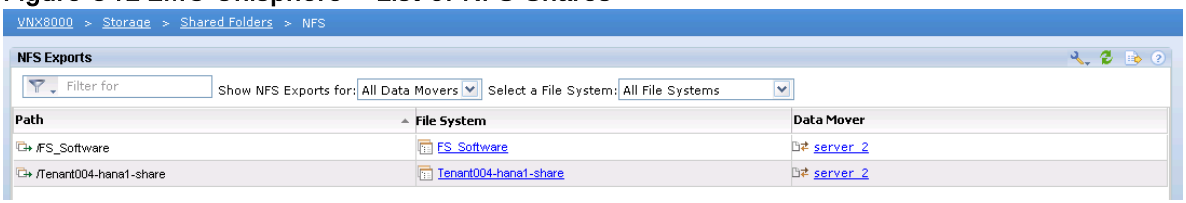
1. Select Storage > Shared Folders > NFS
2. Click Create.
3. Select server_2 from the drop-down menu
4. Select <<var_vnx_t004_fs_name>> from drop-down menu
5. Enter <<var_vnx_t004_share_name>> as the Path
6. Enter <<var_vnx_t004_network>> with the related netmask to Read/write hosts and Root hosts
7. Click OK

Figure 340 EMC Unisphere - Create NFS Share




8. The result will look like the following

Figure 341 EMC Unisphere - List of NFS Shares




The storage configuration for this SAP HANA use case is completed and the Operating system can be installed.

## Install the Operating System

The following steps show the configuration of the Operating systems on the SAP HANA node and the SAP HANA DT node in addition to the basic OS installation.

### SAP HANA Node

1. Follow the steps documented in the Section “Operating System Installation and Configuration” to install the operating system

2. Use a SSH client to login to the newly installed system as root

3. Configure the network interfaces

Add or change the entries in the file(s) as shown. Please do not change the UUID entry

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1 (or eth3)

ONBOOT=yes
NM_CONTROLLED=no
```

```
BOOTPROTO=none
MTU=9000
IPADDR=172.30.113.43
PREFIX=24
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth1"

vi /etc/sysconfig/network-scripts/ifcfg-eth2 (or eth4)

UUID=2949da7d-0782-4238-ba4a-7a88e74b6ab7
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=192.168.4.3
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth2"

vi /etc/sysconfig/network-scripts/ifcfg-eth3 (or eth5)

ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=172.30.4.3
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth3"
```

4. Restart the network stack

```
# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down interface eth2:                              [  OK  ]
Shutting down interface eth3:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Determining if ip address 172.16.4.3 is already in
use for device eth0...
                                                           [  OK  ]
Bringing up interface eth1:  Determining if ip address 172.30.113.43 is already
in use for device eth1...
                                                           [  OK  ]
Bringing up interface eth2:  Determining if ip address 192.168.4.3 is already in
use for device eth2...
                                                           [  OK  ]
Bringing up interface eth3:  Determining if ip address 172.30.4.3
 is already in use for device eth3...
```

```
                                                                [  OK  ]
```

5. List the available multi pathed disks

```
# ls /dev/mapper/36*

/dev/mapper/3600601601c6035000cfb3a4fd050e511
/dev/mapper/3600601601c60350014cb6e0dc550e511
/dev/mapper/3600601601c60350014cb6e0dc550e511p1
/dev/mapper/3600601601c60350014cb6e0dc550e511p2
/dev/mapper/3600601601c603500581d858dd050e511
```

6. Check with df or pvdisplay which mapper device is used for the operating system. For all unused devices run fdisk –l <device> to see the capacity.

```
# fdisk -l /dev/mapper/3600601601c6035000cfb3a4fd050e511

Disk /dev/mapper/3600601601c6035000cfb3a4fd050e511: 549.8 GB, 549755813888 bytes
255 heads, 63 sectors/track, 66837 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c5f6a

# fdisk -l /dev/mapper/3600601601c603500581d858dd050e511

Disk /dev/mapper/3600601601c603500581d858dd050e511: 3298.5 GB, 3298534883328
bytes
255 heads, 63 sectors/track, 401024 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

7. Create the file systems for SAP HANA

```
# mkfs.xfs /dev/mapper/3600601601c6035000cfb3a4fd050e511

meta-data=/dev/mapper/3600601601c6035000cfb3a4fd050e511 isize=256    agcount=4,
agsize=33554432 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=134217728, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=65536, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0


# mkfs.xfs /dev/mapper/3600601601c603500581d858dd050e511

meta-data=/dev/mapper/3600601601c603500581d858dd050e511 isize=256    agcount=4,
agsize=201326592 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=805306368, imaxpct=5
```

```
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=393216, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

8. Mount /hana/shared

The /hana/shared file system is a shared filesystem and must be mounted on the SAP HANA node and on the SAP HANA Dynamic Tiering node. For this the file system /Tenant004-hana1-share NFS share was created on the VNX storage.

9. Add the following line at the end of /etc/fstab file

```
172.30.4.6:/Tenant004-hana1-share   /hana/shared      nfs   defaults    0 0
```

10. Create the mount point /hana/shared

```
mkdir –p /hana/shared
```

11. Mount the File System

```
mount /hana/shared

chgrp sapsys /hana/shared

chmod 775 /hana/shared
```

12. Mount the file systems

```
echo /dev/mapper/3600601601c6035000cfb3a4fd050e511 /hana/log xfs defaults 1 1 >>
/etc/fstab

echo /dev/mapper/3600601601c603500581d858dd050e511 /hana/data xfs defaults 1 1 >>
/etc/fstab

mkdir /hana/log

mkdir /hana/data

mkdir /hana/log_es

mkdir /hana/data_es

mount /hana/log

mount /hana/data

chgrp sapsys /hana/*

chmod 775 /hana/*
```

13. Enter the required information into the hosts file

```
Vi /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6


#
# Access Network
#
172.16.4.3      t004-hana01.t004.cra-emc.local  t004-hana01
172.16.4.4      t004-dt01.t004.cra-emc.local    t004-dt01
#
# Global NFS
#
172.30.113.43   t004-hana01-nfs
172.30.113.44   t004-dt01-nfs
#
# Storage Network
#
172.30.4.3      t004-hana01-st
172.30.4.4      t004-dt01-st
172.30.4.6      t004-nfs01
#
# Internal Network
#
192.168.4.3     t004-hana01-int
192.168.4.4     t004-dt01-int
```

14. Exchange the ssh key between all hosts for the SAP HANA system. This is required for remote login without a password.

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:01:04:a6:f1:67:05:01:da:33:b1:53:69:d5:f3:9b [MD5] root@t004-hana01
The key's randomart image is:
+--[ RSA 2048]----+
|      . =+*=o.   |
|       B +oo  o  |
|      o B.o .  o |
|         * . .  .|
|        S . .   o|
|         .     E |
|                 |
|                 |
|                 |
+--[MD5]----------+
```

```
ssh-copy-id –i /root/.ssh/id_rsa.pub t004-dt01

root@t004-dt01’s password:
Now try logging into the machine, with "ssh 't004-dt01'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

15. Reboot the system:

```
Reboot
```

### SAP HANA Dynamic Tiering Node

1. Follow the steps documented in the Section “Operating System Installation and Configuration” to install the operating system

2. Use a SSH client to login to the newly installed system as root

3. Configure the Network Interfaces

Add or change the entries in the file(s) as shown. Please do not change the UUID entry

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1 (or eth3)

ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=172.30.113.44
PREFIX=24
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth1"

vi /etc/sysconfig/network-scripts/ifcfg-eth2 (or eth4)

UUID=2949da7d-0782-4238-ba4a-7a88e74b6ab7
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=192.168.4.4
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth2"

vi /etc/sysconfig/network-scripts/ifcfg-eth3 (or eth5)

ONBOOT=yes
```

```
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=172.30.4.4
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth3"
```

4. Restart the network stack

```
# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down interface eth2:                              [  OK  ]
Shutting down interface eth3:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Determining if ip address 172.16.4.4 is already in
use for device eth0...
                                                           [  OK  ]
Bringing up interface eth1:  Determining if ip address 172.30.113.44 is already
in use for device eth1...
                                                           [  OK  ]
Bringing up interface eth2:  Determining if ip address 192.168.4.4 is already in
use for device eth2...
                                                           [  OK  ]
Bringing up interface eth3:  Determining if ip address 172.30.4.4 is already in
use for device eth3...
                                                           [  OK  ]
```

5. List the available multi pathed disks

```
# ls /dev/mapper 36*

/dev/mapper/3600601601c60350053ebfb71d350e511
/dev/mapper/3600601601c60350055181ee8d250e511
/dev/mapper/3600601601c60350095042818d050e511
/dev/mapper/3600601601c60350095042818d050e511p1
/dev/mapper/3600601601c60350095042818d050e511p2
/dev/mapper/3600601601c603500a43a9f0ed350e511
```

6. Check with df or pvdisplay which mapper device is used for the operating system. For all unused devices run fdisk –l <device> to see the capacity.

```
# fdisk –l dev/mapper/3600601601c60350053ebfb71d350e511

Disk /dev/mapper/3600601601c60350053ebfb71d350e511: 171.8 GB, 171798691840 bytes
255 heads, 63 sectors/track, 20886 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0007ae3e
```

```
# fdisk -l /dev/mapper/3600601601c60350055181ee8d250e511

Disk /dev/mapper/3600601601c60350055181ee8d250e511: 214.7 GB, 214748364800 bytes
255 heads, 63 sectors/track, 26108 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0004a816


# fdisk -l /dev/mapper/3600601601c603500a43a9f0ed350e511

Disk /dev/mapper/3600601601c603500a43a9f0ed350e511: 6597.1 GB, 6597069766656
bytes
255 heads, 63 sectors/track, 802048 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

7. Create the file systems for SAP HANA

```
# mkfs.xfs /dev/mapper/3600601601c60350053ebfb71d350e511

meta-data=/dev/mapper/3600601601c60350053ebfb71d350e511 isize=256    agcount=4,
agsize=10485760 blks
         =               sectsz=512   attr=2, projid32bit=0
data     =               bsize=4096   blocks=41943040, imaxpct=25
         =               sunit=0      swidth=0 blks
naming   =version 2      bsize=4096   ascii-ci=0
log      =internal log   bsize=4096   blocks=20480, version=2
         =               sectsz=512   sunit=0 blks, lazy-count=1
realtime =none           extsz=4096   blocks=0, rtextents=0


# mkfs.xfs /dev/mapper/3600601601c60350055181ee8d250e511

meta-data=/dev/mapper/3600601601c60350055181ee8d250e511 isize=256    agcount=4,
agsize=13107200 blks
         =               sectsz=512   attr=2, projid32bit=0
data     =               bsize=4096   blocks=52428800, imaxpct=25
         =               sunit=0      swidth=0 blks
naming   =version 2      bsize=4096   ascii-ci=0
log      =internal log   bsize=4096   blocks=25600, version=2
         =               sectsz=512   sunit=0 blks, lazy-count=1
realtime =none           extsz=4096   blocks=0, rtextents=0


# mkfs.xfs /dev/mapper/3600601601c603500a43a9f0ed350e511

meta-data=/dev/mapper/3600601601c603500a43a9f0ed350e511 isize=256    agcount=6,
agsize=268435455 blks
         =               sectsz=512   attr=2, projid32bit=0
data     =               bsize=4096   blocks=1610612730, imaxpct=5
         =               sunit=0      swidth=0 blks
naming   =version 2      bsize=4096   ascii-ci=0
```

```
log      =internal log   bsize=4096   blocks=521728, version=2
         =               sectsz=512   sunit=0 blks, lazy-count=1
realtime =none           extsz=4096   blocks=0, rtextents=0
```

8. Mount /hana/shared

The /hana/shared file system is a shared filesystem and must be mounted on the SAP HANA node and on the SAP HANA Dynamic Tiering node. For this the file system /Tenant004-hana1-share NFS share was created on the VNX storage.

9. Add the following line at the end of /etc/fstab file

```
172.30.4.6:/Tenant004-hana1-share   /hana/shared      nfs   defaults    0 0
```

10. Create the mount point /hana/shared

```
mkdir –p /hana/shared
```

11. Mount the File System

```
mount /hana/shared

chgrp sapsys /hana/shared

chmod 775 /hana/shared
```

12. Mount the file systems

```
echo /dev/mapper/3600601601c60350053ebfb71d350e511/hana/rvl_es xfs defaults 1 1
>> /etc/fstab

echo /dev/mapper/3600601601c60350055181ee8d250e511 /hana/log_es xfs defaults 1 1
>> /etc/fstab

echo /dev/mapper/3600601601c603500a43a9f0ed350e511 /hana/data_es xfs defaults 1 1
>> /etc/fstab

mkdir /hana/rvl_es

mkdir /hana/log_es

mkdir /hana/data_es

mkdir /hana/log

mkdir /hana/data

mount /hana/rvl_es

mount /hana/log_es

mount /hana/data_es

chgrp sapsys /hana/*

chmod 775 /hana/*
```

13. Enter the required information into the hosts file

```
Vi /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6


#
# Access Network
#
172.16.4.3      t004-hana01.t004.cra-emc.local  t004-hana01
172.16.4.4      t004-dt01.t004.cra-emc.local    t004-dt01
#
# Global NFS
#
172.30.113.43   t004-hana01-nfs
172.30.113.44   t004-dt01-nfs
#
# Storage Network
#
172.30.4.3      t004-hana01-st
172.30.4.4      t004-dt01-st
172.30.4.6      t004-nfs01
#
# Internal Network
#
192.168.4.3     t004-hana01-int
192.168.4.4     t004-dt01-int
```

14. Exchange the ssh key between all hosts for the SAP HANA system. This is required for remote login without a password.

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:01:04:a6:f1:67:05:01:da:33:b1:53:69:d5:f3:9b [MD5] root@t004-dt01
The key's randomart image is:
+--[ RSA 2048]----+
|      . =+*=o.   |
|       B +oo  o  |
|      o B.o .  o |
|         * . .  .|
|        S . .   o|
|         .     E |
|                 |
|                 |
|                 |
```

```
+--[MD5]----------+

ssh-copy-id –i /root/.ssh/id_rsa.pub t004-hana01

root@t004-hana01’s password:
Now try logging into the machine, with "ssh 't004-hana01'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

15. Reboot the system:

```
Reboot
```

## Enabling data traffic on vHBA3 and vHBA4 (SAP HANA Node)

Now that the Cisco FNIC driver is loaded in the operating system, vHBA3 and vHBA4 are also logged into the MDS switches. For best performance of a SAP HANA Scale-Up system it is recommended to move the paths for the data volume from the single storage path zoning into the multi paths zoning.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_t004-hana1-data>> vsan 10
zone name <<var_zone_t004-hana1-data>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:10
   exit


zoneset name CRA-EMC-A vsan 10
member <<var_zone_t004-hana1-data>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
```

```
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_t004-hana1 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:11
…
zone name zone_t004-hana1-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:10

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
```

```
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t004-hana1
  zone zone_t004-hana1-data
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
Copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_t004-hana1-data>> vsan 20
zone name <<var_zone_t004-hana1-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:10
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_t004-hana1-data>>
exit
zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
```

```
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_t004-hana1 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:11

zone name zone_t004-hana1-data vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:10

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
```

```
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t004-hana1
  zone zone_t004-hana1-data
CRA-EMC-B#
```

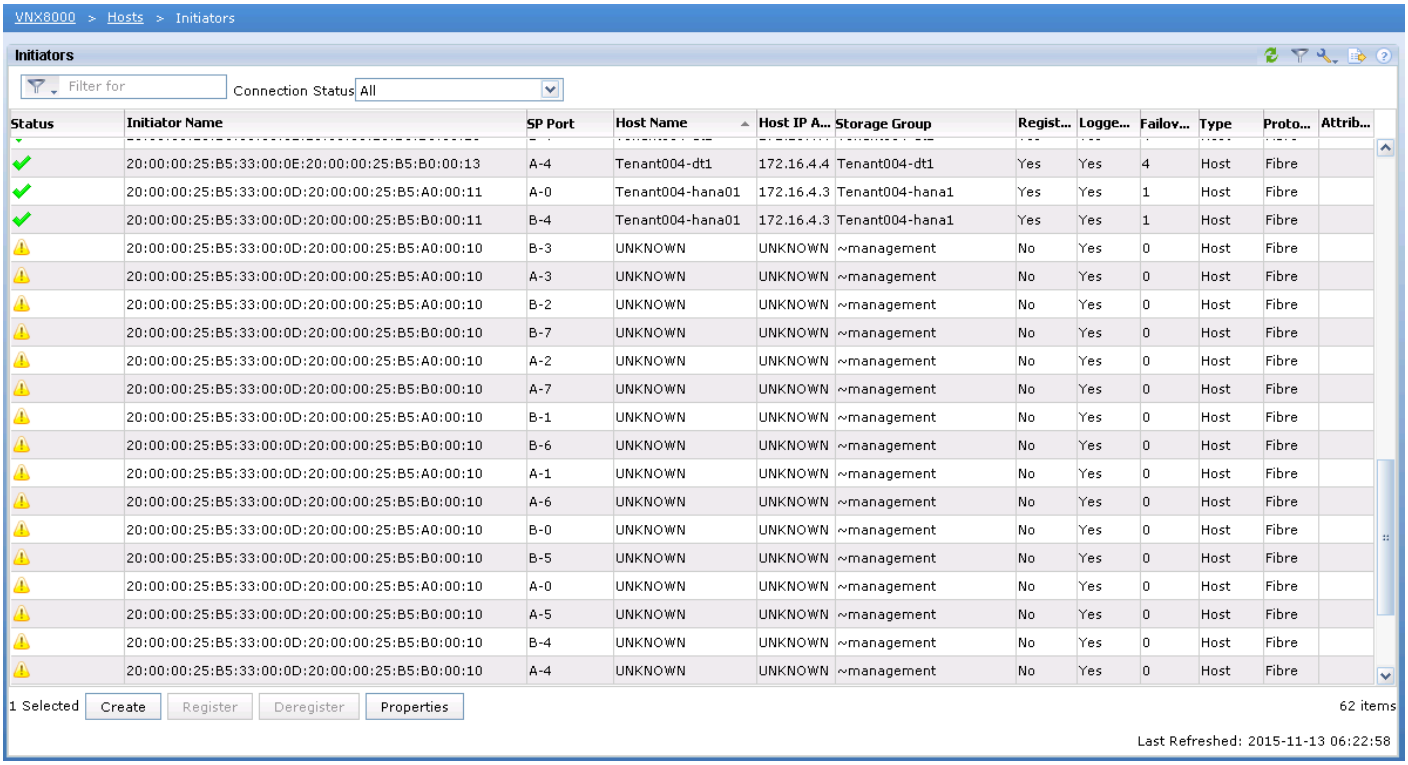
4. Save the running configuration as startup configuration:

```
copy run start
```

## Configure EMC VNX

### Register Host

1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators

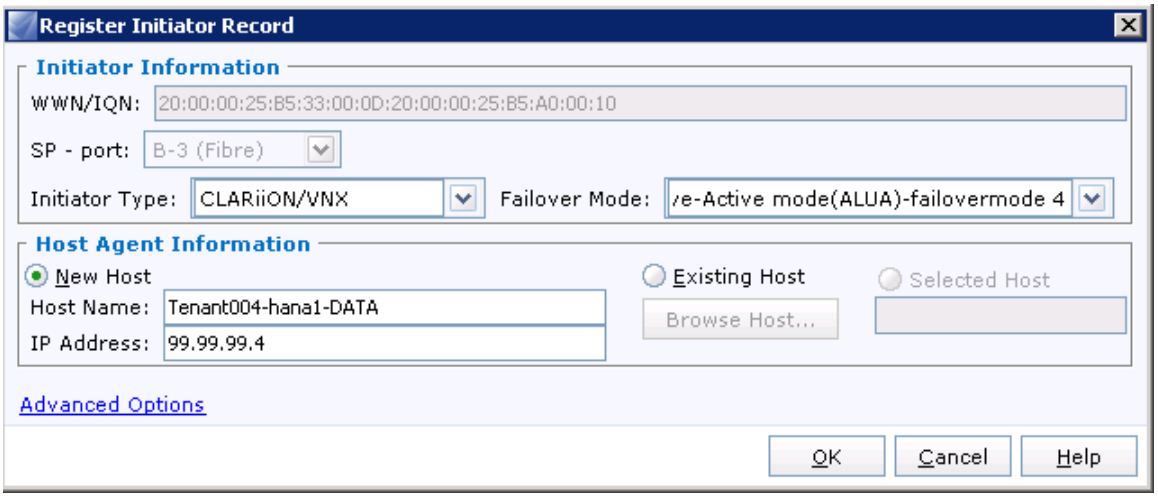



2. Select one of the unregistered entries for the host Tenant004-hana01, click Register

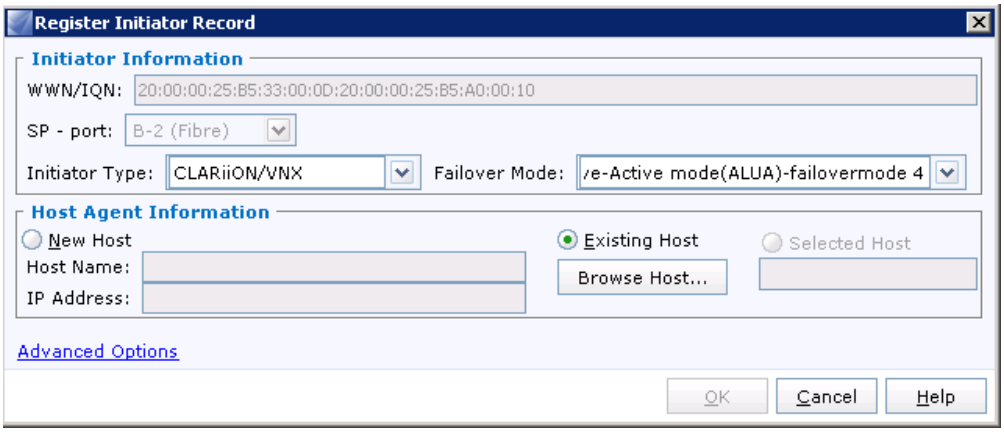
3. Select CLARiiON/VNX as the Initiator Type

4. Select Active/Active mode(ALUA)-failovermode 4 as the Failover Mode

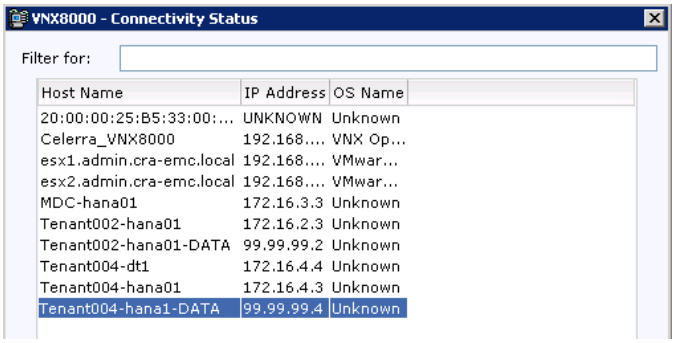
5. Enter <<var_ucs_t004_hana1_sp_name>>-data as the Host Name (indicates the relationship to the Service Profile)
6. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
7. Click OK
8. Click Yes
9. Click OK
10. Click OK




11. Select the second Entry for this host <<var_ucs_t004_hana1_sp_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and click Browse Host



15. Select <<var_ucs_t004_hana1_sp_name>>-data and click OK

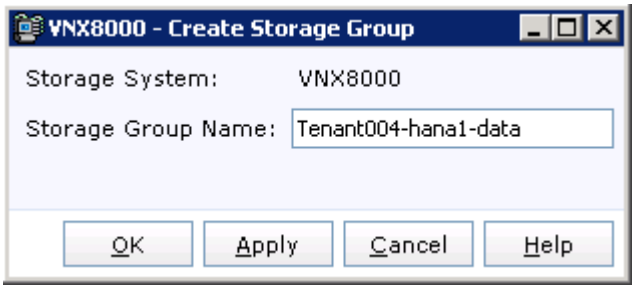



16. Click OK
17. Click Yes
18. Click OK
19. Click OK

Repeat Step 10 to 18 for all remaining paths of this server in the list.

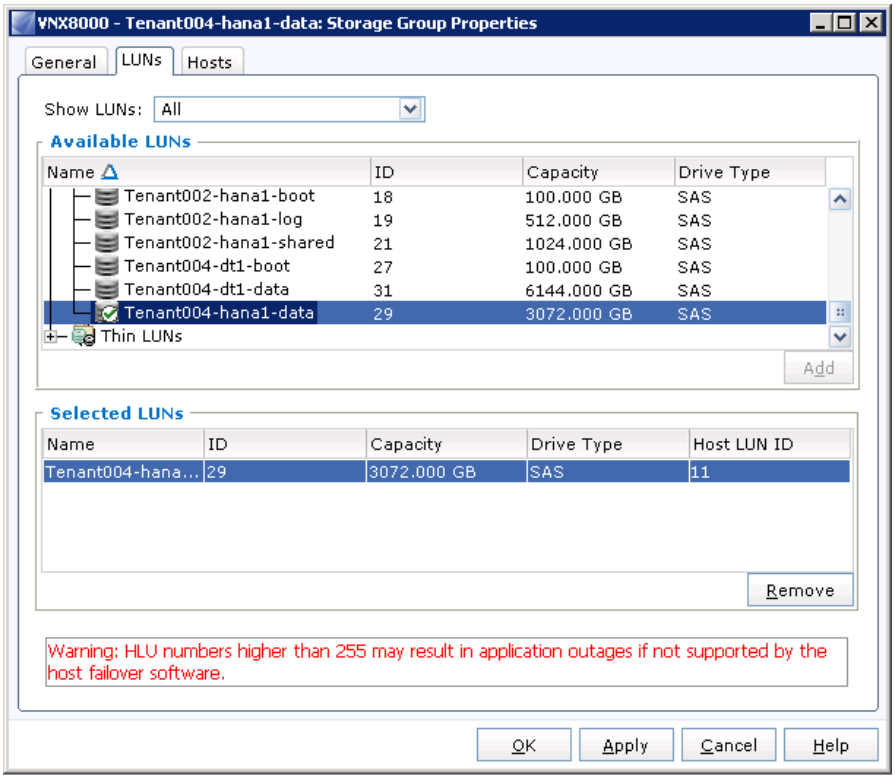
## Create Storage-Group

1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t004_hana1_sp_name>>-data as the Name
4. Click OK
5. Click Yes




6. Click Yes
7. Select All from the Show LUNs drop-down menu, click OK
8. Select the Data-LUN from the list of LUNs and click Add

9. Select 11 as the Host LUN ID for <<var_ucs_t004_hana1_sp_name>>-data (the same ID as before)



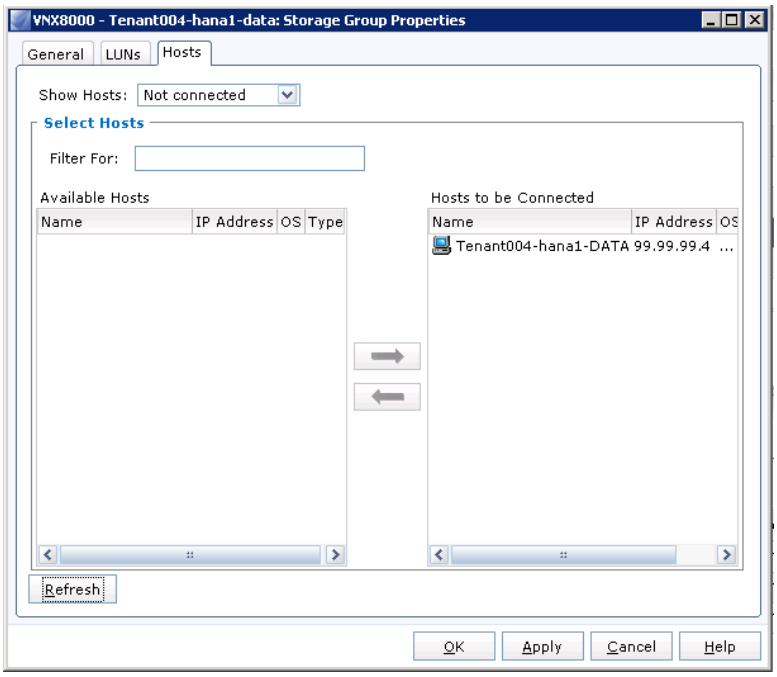

10. Click the Hosts tab

11. Select <<var_ucs_t004_hana1_sp_name>>-data and click the -> Icon

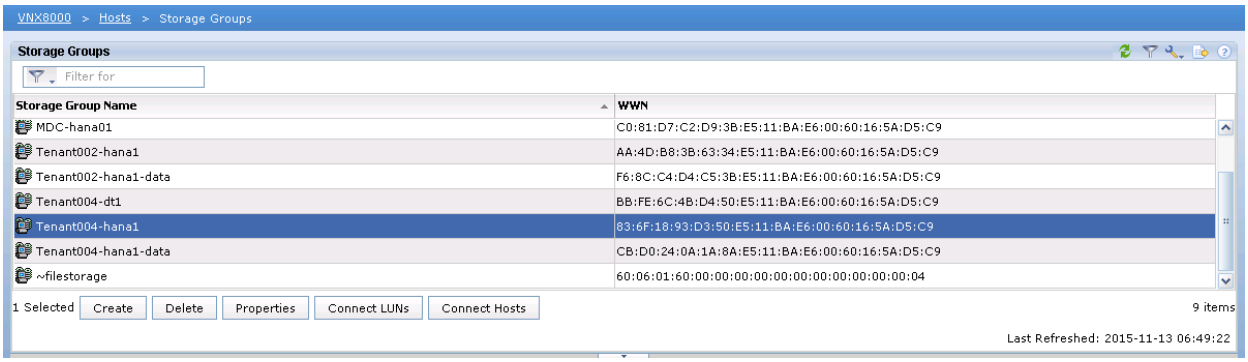
12. Click OK

13. Click Yes

14. Click OK



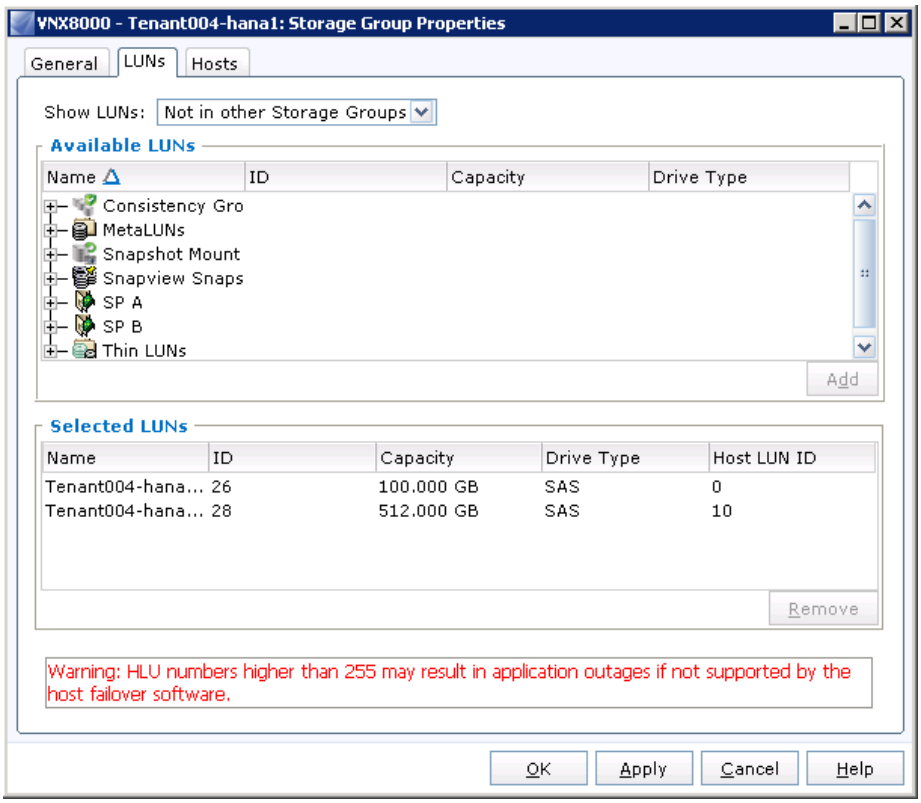

2. From Storage Groups, select <<var_ucs_t004_hana1_sp_name>>, click Properties




15. Click the LUNs Tab

16. Select the data LUN from the below list “Selected LUNs”

17. Click Remove




18. Click OK
19. Click Remove LUNs from storage group
20. Click OK
21. Go back to the server and boot/reboot the system

## Install SAP HANA

1. Mount the Software share to access the SAP HANA installation files

```
mkdir /software
mount 172.30.113.11:/FS_Software /software
```

Prepare NFS mounts for SAP HANA DT

2. On the Dynamic Tiering Node add the following lines to /etc/exports

```
/hana/data_es     172.30.4.0/29(rw,no_root_squash)
/hana/log_es      172.30.4.0/29(rw,no_root_squash)
```

3. On the HANA Node add the following lines to /etc/exports

```
/hana/data    172.30.4.0/29(rw,no_root_squash)
/hana/log     172.30.4.0/29(rw,no_root_squash)
```

Cross-Mount the data and log file systems

4. On the Dynamic Tiering Node add the following lines to /etc/fstab

```
172.30.4.3:/hana/data   /hana/data      nfs     defaults    0 0
172.30.4.3:/hana/log    /hana/log       nfs     defaults    0 0
```

5. On the HANA Node add the following lines to /etc/fstab

```
172.30.4.4:/hana/data_es   /hana/data_es      nfs     defaults    0 0
172.30.4.4:/hana/log_es    /hana/log_es       nfs     defaults    0 0
```

On both nodes issue mount –a to mount all file systems specified in /etc/fstab

Tip: A restart of nfs-server service on both nodes in some cases may help with mount issues.

6. Please use the SAP HANA installation Guide provided by SAP for the software revision you plan to install. The program to install SAP HANA Revision 100 is hdblcm located in the directory <Installation source>/DATA_UNITS/HDB_LCM_LINUX_X86_64.

```
cd /software/SAP/SPS10/REV100/DATA_UNITS/HDB_LCM_LINUX_X86_64
./hdblcm --action=install --component_root=/software/SAP
```

```
SAP HANA Lifecycle Management - SAP HANA 1.00.100.00.1434512907
************************************************************


Scanning Software Locations...
Detected components:
    SAP HANA Database (1.00.100.00.1434512907) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA AFL (Misc) (1.00.100.00.1434529984) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA LCAPPS (1.00.100.000.454467) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HANA_LCAPPS_10_LINUX_X86_64/packages
    SAP TRD AFL FOR HANA (1.00.100.00.1434529984) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_TRD_AFL_LINUX_X86_64/packages
    SAP HANA Database Client (1.00.100.00.1434512907) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Studio (2.1.4.000000) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Smart Data Access (1.00.4.004.0) in
/mnt/SAP/SPS10/REV100/DATA_UNITS/SAP_HANA_SDA_10/packages
```

```
    SAP HANA Dynamic Tiering (16.0.0.995) in
/mnt/SAP/DT_1/SAP_HANA_DYNAMIC_TIERING/es


SAP HANA Database version '1.00.100.00.1434512907' will be installed.

Select additional components for installation:

  Index | Components | Description
  -------------------------------------------------------------------------------
--
  1     | server     | No additional components
  2     | all        | All components
  3     | client     | Install SAP HANA Database Client version
1.00.100.00.1434512907
  4     | afl        | Install SAP HANA AFL (Misc) version 1.00.100.00.1434529984
  5     | lcapps     | Install SAP HANA LCAPPS version 1.00.100.000.454467
  6     | smartda    | Install SAP HANA Smart Data Access version 1.00.4.004.0
  7     | studio     | Install SAP HANA Studio version 2.1.4.000000
  8     | trd        | Install SAP TRD AFL FOR HANA version 1.00.100.00.1434529984
  9     | es         | Install SAP HANA Dynamic Tiering version 16.0.0.995

Enter comma-separated list of the selected indices [3]: 2
Enter Installation Path [/hana/shared]:
Enter Local Host Name [t004-hana01]:
Do you want to add additional hosts to the system? (y/n): y
Enter comma-separated host names to add: t004-dt01
Enter Root User Name [root]:
Collecting information from host 't004-dt01'...
Information collected from host 't004-dt01'.

Select roles for host 't004-dt01':

  Index | Host Role                | Description
  ----------------------------------------------------------------
  1     | worker                   | Database Worker
  2     | standby                  | Database Standby
  3     | extended_storage_worker  | Dynamic Tiering Worker
  4     | extended_storage_standby | Dynamic Tiering Standby
  5     | streaming                | Smart Data Streaming
  6     | rdsync                   | Remote Data Sync
  7     | ets_worker               | Accelerator for SAP ASE Worker
  8     | ets_standby              | Accelerator for SAP ASE Standby

Enter comma-separated list of selected indices [1]: 3
Enter Host Failover Group for host 't004-dt01' [extended_storage]:
Enter Storage Partition Number for host 't004-dt01' [<<assign automatically>>]:
Enter SAP HANA System ID: TD4
Enter Instance Number [00]: 44

  Index | Database Mode       | Description
  -------------------------------------------------------------------------------
-------------
  1     | single_container    | The system contains one database
```

```
  2     | multiple_containers | The system contains one system database and 1..n
tenant databases

Select Database Mode / Enter Index [1]:

  Index | System Usage | Description
  -------------------------------------------------------------------------------
  1     | production   | System is used in a production environment
  2     | test         | System is used for testing, not production
  3     | development  | System is used for development, not production
  4     | custom       | System usage is neither production, test nor development

Select System Usage / Enter Index [4]: 1
Enter Location of Data Volumes [/hana/data/TD4]:
Enter Location of Log Volumes [/hana/log/TD4]:
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 't004-hana01' [t004-hana01]:
Enter Certificate Host Name For Host 't004-dt01' [t004-dt01]:
Enter SAP Host Agent User (sapadm) Password: ucs4sap!
Enter System Administrator (td4adm) Password: ucs4sap!
Confirm System Administrator (td4adm) Password: ucs4sap!
Enter System Administrator Home Directory [/usr/sap/TD4/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1000]:
Enter Database User (SYSTEM) Password: SAPhana10
Confirm Database User (SYSTEM) Password: SAPhana10
Restart instance after machine reboot? [n]:
Enter Location of Dynamic Tiering Data Volumes [/hana/data_es/TD4]:
Enter Location of Dynamic Tiering Log Volumes [/hana/log_es/TD4]:

Summary before execution:
=========================

SAP HANA Components Installation
   Installation Parameters
      Remote Execution: ssh
      Installation Path: /hana/shared
      Local Host Name: t004-hana01
      Root User Name: root
      SAP HANA System ID: TD4
      Instance Number: 44
      Database Mode: single_container
      System Usage: production
      Location of Data Volumes: /hana/data/TD4
      Location of Log Volumes: /hana/log/TD4
      Certificate Host Names: t004-hana01 -> t004-hana01, t004-dt01 -> t004-dt01
      System Administrator Home Directory: /usr/sap/TD4/home
      System Administrator Login Shell: /bin/sh
      System Administrator User ID: 1000
      ID of User Group (sapsys): 401
      Directory root to search for components: /mnt/SAP
      SAP HANA Database Client Installation Path: /hana/shared/TD4/hdbclient
      SAP HANA Studio Installation Path: /hana/shared/TD4/hdbstudio
      Location of Dynamic Tiering Data Volumes: /hana/data_es/TD4
      Location of Dynamic Tiering Log Volumes: /hana/log_es/TD4
```

```
   Software Components
      SAP HANA Database
         Install version 1.00.100.00.1434512907
         Location: /mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
      SAP HANA AFL (Misc)
         Install version 1.00.100.00.1434529984
         Location: /mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
      SAP HANA LCAPPS
         Install version 1.00.100.000.454467
         Location:
/mnt/SAP/SPS10/REV100/DATA_UNITS/HANA_LCAPPS_10_LINUX_X86_64/packages
      SAP TRD AFL FOR HANA
         Install version 1.00.100.00.1434529984
         Location:
/mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_TRD_AFL_LINUX_X86_64/packages
      SAP HANA Database Client
         Install version 1.00.100.00.1434512907
         Location: /mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
      SAP HANA Studio
         Install version 2.1.4.000000
         Location: /mnt/SAP/SPS10/REV100/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
      SAP HANA Smart Data Access
         Install version 1.00.4.004.0
         Location: /mnt/SAP/SPS10/REV100/DATA_UNITS/SAP_HANA_SDA_10/packages
      SAP HANA Dynamic Tiering
         Install version 16.0.0.995
         Location: /mnt/SAP/DT_1/SAP_HANA_DYNAMIC_TIERING/es
   Additional Hosts
      t004-dt01
         Role: Dynamic Tiering Worker (extended_storage_worker)
         High-Availability Group: extended_storage
         Storage Partition: <<assign automatically>>

Do you want to continue? (y/n): y


Installing components...
Installing SAP HANA Database...
  Preparing package 'Saphostagent Setup'...
  Preparing package 'Python Support'...
  Preparing package 'Python Runtime'...
  Preparing package 'Product Manifest'...
  Preparing package 'Binaries'...
  Preparing package 'Installer'...
  Preparing package 'Ini Files'...
  Preparing package 'HWCCT'...
  Preparing package 'Emergency Support Package'...
  Preparing package 'EPM'...
  Preparing package 'Documentation'...
  Preparing package 'Delivery Units'...
  Preparing package 'DAT Languages'...
  Preparing package 'DAT Configfiles'...
  Creating System...
  Extracting software...
  Installing package 'Saphostagent Setup'...
```

```
  Installing package 'Python Support'...
  Installing package 'Python Runtime'...
  Installing package 'Product Manifest'...
  Installing package 'Binaries'...
  Installing package 'Installer'...
  Installing package 'Ini Files'...
  Installing package 'HWCCT'...
  Installing package 'Emergency Support Package'...
  Installing package 'EPM'...
  Installing package 'Documentation'...
  Installing package 'Delivery Units'...
  Installing package 'DAT Languages'...
  Installing package 'DAT Configfiles'...
  Creating instance...
  Starting SAP HANA Database system...
  Starting 7 processes on host 't004-hana01':
      Starting on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbindexserver, hdbwebdispatcher,
hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbwebdispatcher
    All server processes started on host 't004-hana01'.
  Importing delivery units...
  Importing delivery unit HCO_INA_SERVICE
  Importing delivery unit HANA_DT_BASE
  Importing delivery unit HANA_IDE_CORE
  Importing delivery unit HANA_TA_CONFIG
  Importing delivery unit HANA_UI_INTEGRATION_SVC
  Importing delivery unit HANA_UI_INTEGRATION_CONTENT
  Importing delivery unit HANA_XS_BASE
  Importing delivery unit HANA_XS_DBUTILS
  Importing delivery unit HANA_XS_EDITOR
  Importing delivery unit HANA_XS_IDE
  Importing delivery unit HANA_XS_LM
  Importing delivery unit HDC_ADMIN
  Importing delivery unit HDC_IDE_CORE
  Importing delivery unit HDC_SEC_CP
  Importing delivery unit HDC_XS_BASE
  Importing delivery unit HDC_XS_LM
  Importing delivery unit SAPUI5_1
  Importing delivery unit SAP_WATT
  Importing delivery unit HANA_BACKUP
  Importing delivery unit HANA_HDBLCM
  Importing delivery unit HANA_SEC_BASE
  Importing delivery unit HANA_SEC_CP
  Importing delivery unit HANA_ADMIN
Installing Resident hdblcm...
Installing SAP HANA AFL (Misc)...
  Preparing package 'AFL'...
```

```
  Installing SAP Application Function Libraries to
/hana/shared/TD4/exe/linuxx86_64/plugins/afl_1.00.100.00.1434529984_2170235...
  Installing package 'AFL'...
  Stopping system...
  Stopping 7 processes on host 't004-hana01':
      Stopping on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor, hdbwebdispatcher, hdbxsengine
    All server processes stopped on host 't004-hana01'.
  Activating plugin...
Installing SAP HANA LCAPPS...
  Preparing package 'LCAPPS'...
  Installing SAP liveCache Applications to
/hana/shared/TD4/exe/linuxx86_64/plugins/lcapps_1.00.100.00.454467_4590229...
  Installing package 'LCAPPS'...
  Stopping system...
    All server processes stopped on host 't004-hana01'.
  Activating plugin...
Installing SAP TRD AFL FOR HANA...
  Preparing package 'TRD'...
  Installing SAP TRD AFL FOR SAP HANA to
/hana/shared/TD4/exe/linuxx86_64/plugins/trd_1.00.100.00.1434529984_2170235...
  Installing package 'TRD'...
  Stopping system...
    All server processes stopped on host 't004-hana01'.
  Activating plugin...
  Starting system...
  Starting 7 processes on host 't004-hana01':
      Starting on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbindexserver, hdbwebdispatcher,
hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbwebdispatcher, hdbxsengine
      Starting on 't004-hana01': hdbdaemon, hdbwebdispatcher
    All server processes started on host 't004-hana01'.
Installing SAP HANA Database Client...
  Preparing package 'Python Runtime'...
  Preparing package 'Product Manifest'...
  Preparing package 'SQLDBC'...
  Preparing package 'REPOTOOLS'...
  Preparing package 'Python DB API'...
  Preparing package 'ODBC'...
  Preparing package 'JDBC'...
  Preparing package 'HALM Client'...
  Preparing package 'Client Installer'...
  Installing SAP HANA Database Client to /hana/shared/TD4/hdbclient...
  Installing package 'Python Runtime'...
  Installing package 'Product Manifest'...
  Installing package 'SQLDBC'...
  Installing package 'REPOTOOLS'...
  Installing package 'Python DB API'...
  Installing package 'ODBC'...
  Installing package 'JDBC'...
  Installing package 'HALM Client'...
```

```
  Installing package 'Client Installer'...
Installing SAP HANA Studio...
  Preparing package 'Studio Director'...
  Preparing package 'Client Installer'...
  Installing SAP HANA Studio to /hana/shared/TD4/hdbstudio...
  Installing package 'Studio Director'...
  Installing package 'Client Installer'...
  Installing SAP HANA Studio Update repository...
    hdbupdrep: Importing delivery units...
    hdbupdrep: Importing delivery unit HANA_STUDIO_TD4
Installing SAP HANA Smart Data Access...
  Removing old driver files from /hana/shared/TD4/federation ...
Installing SAP HANA Dynamic Tiering...
  Installing jre7...
  Installing shared...
  Installing lang...
  Installing conn_lm...
  Installing open client...
  Installing conn_add_lm...
  Installing odbc...
  Installing client_common...
  Installing server...
  Installing complete - log files written to /hana/shared/TD4/es/log
  Importing delivery unit HANA_TIERING
  Force Remove            : 1
Adding Additional Hosts...
Adding additional host...
Adding host 't004-dt01'...
  t004-dt01:  Adding host 't004-dt01' to instance '44'...
  t004-dt01:  Starting SAP HANA Database...
  t004-dt01:  Starting 3 processes on host 't004-dt01':
  t004-dt01:      Starting on 't004-dt01': hdbdaemon, hdbesserver, hdbnameserver
  t004-dt01:      Starting on 't004-dt01': hdbdaemon, hdbesserver
  t004-dt01:    All server processes started on host 't004-dt01'.
Creating Component List...
  Registering SAP HANA Studio...
    Registering SAP HANA Database Client...
      Deploying SAP Host Agent configurations...
Updating SAP HANA instance integration on host 't004-dt01'...
SAP HANA system installed
You can send feedback to SAP with this form: https://t004-
hana01:1129/lmsl/HDBLCM/TD4/feedback/feedback.html
Log file written to '/var/tmp/hdb_TD4_hdblcm_install_2016-01-11_08.00.00/hdblcm.log'
on host 't004-hana01'.
[root@t004-hana01 HDB_LCM_LINUX_X86_64]#
```

7. Check the SAP HANA status on both nodes. Verifying thay DT service is running.

8. Log into t004-hana01 as td4adm and run the command HDB info

```
td4adm@t004-hana01:/usr/sap/TD4/HDB44> HDB info
USER        PID   PPID %CPU    VSZ   RSS COMMAND
td4adm    87431  87430  0.6 108456  1884 -sh
```

```
td4adm    87484  87431  0.0 114064  1960  \_ /bin/sh /usr/sap/TD4/HDB44/HDB info

td4adm    87511  87484  0.0 118044  1564      \_ ps fx -U td4adm -o user,pid,ppid,pcpu,vsz,rss,args

td4adm    29978      1  0.0  22448  1544 sapstart pf=/hana/shared/TD4/profile/TD4_HDB44_t004-hana01

td4adm    29987  29978  0.0 550204 289544  \_ /usr/sap/TD4/HDB44/t004-hana01/trace/hdb.sapTD4_HDB44 -d -
nw -f /usr/sap/TD4/HDB44/t004-hana01/

td4adm    30005  29987  0.9 4510716 1545212      \_ hdbnameserver

td4adm    30126  29987  0.8 4685700 1980484      \_ hdbcompileserver

td4adm    30129  29987  0.5 3244948 599276      \_ hdbpreprocessor

td4adm    30150  29987 12.0 23607596 20096392      \_ hdbindexserver

td4adm    30153  29987  1.3 5044744 1708168      \_ hdbxsengine

td4adm    30830  29987  0.4 3669916 816528      \_ hdbwebdispatcher

td4adm    13480      1  0.1 869180 74672 /usr/sap/TD4/HDB44/exe/sapstartsrv
pf=/hana/shared/TD4/profile/TD4_HDB44_t004-hana01 -D -u td4adm

td4adm@t004-hana01:/usr/sap/TD4/HDB44>
```

9. Log into t004-dt01 as td4adm and run the command HDB info

```
td4adm@t004-dt01:/usr/sap/TD4/HDB44> HDB info

USER       PID  PPID %CPU    VSZ   RSS COMMAND

td4adm   17720 17719  0.0 108456  1888 -sh

td4adm   17777 17720  0.0 114068  1984  \_ /bin/sh /usr/sap/TD4/HDB44/HDB info

td4adm   17804 17777  3.0 118044  1572      \_ ps fx -U td4adm -o user,pid,ppid,pcpu,vsz,rss,args

td4adm   10854     1  0.0  22452  1548 sapstart pf=/hana/shared/TD4/profile/TD4_HDB44_t004-dt01

td4adm   10863 10854  0.0 549940 287076  \_ /usr/sap/TD4/HDB44/t004-dt01/trace/hdb.sapTD4_HDB44 -d -nw -f
/usr/sap/TD4/HDB44/t004-dt01/daemon

td4adm   10881 10863  0.1 3344412 692788      \_ hdbnameserver

td4adm   10901 10863  0.0 22810148 70776      \_ hdbesserver -n esTD444 -x tcpip{port=34412} -hes

td4adm   10741     1  0.0 736564 61624 /hana/shared/TD4/HDB44/exe/sapstartsrv
pf=/hana/shared/TD4/profile/TD4_HDB44_t004-dt01 -D -u td4adm

td4adm@t004-dt01:/usr/sap/TD4/HDB44>
```

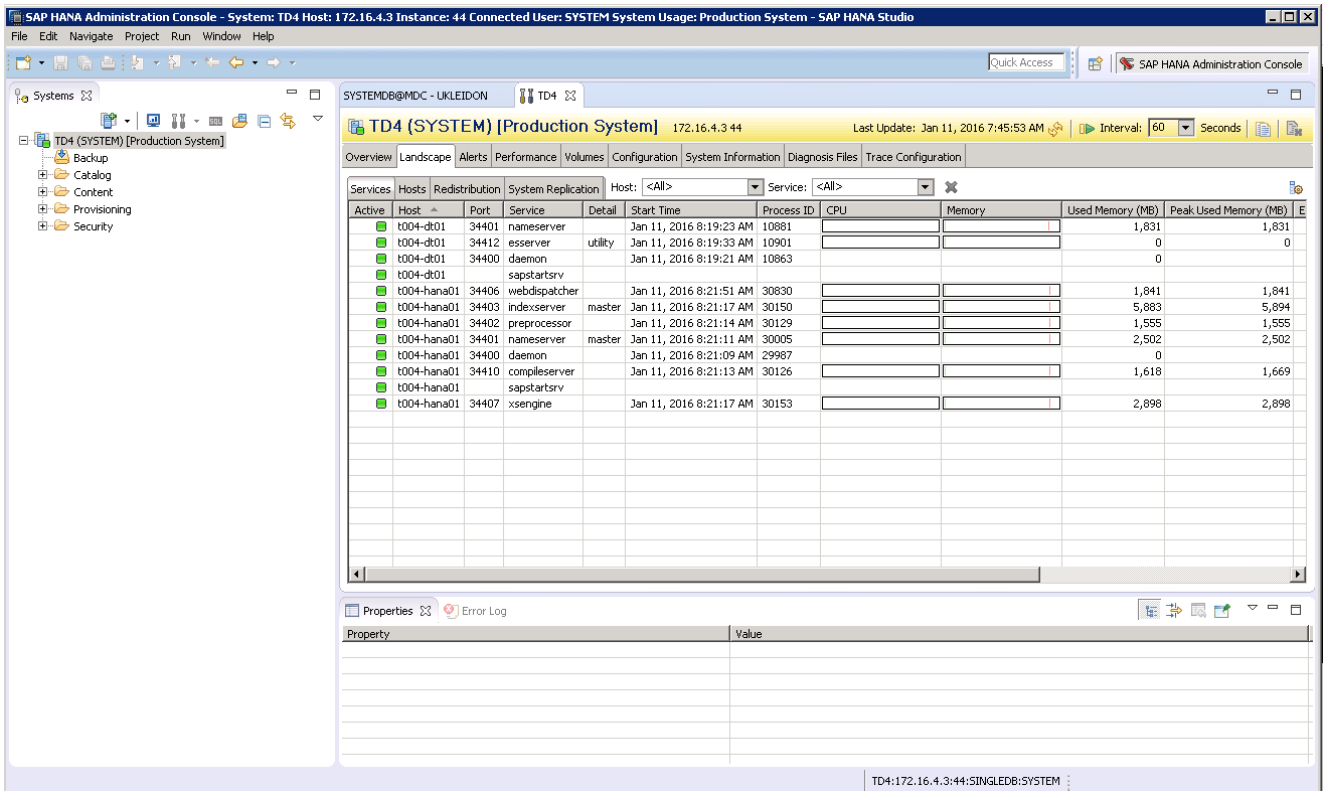


The OS process on dynamic tiering host, hdbesserver, verifies that DT service is running.

10. Connecting via HANA Studio for DT service verification and status check.

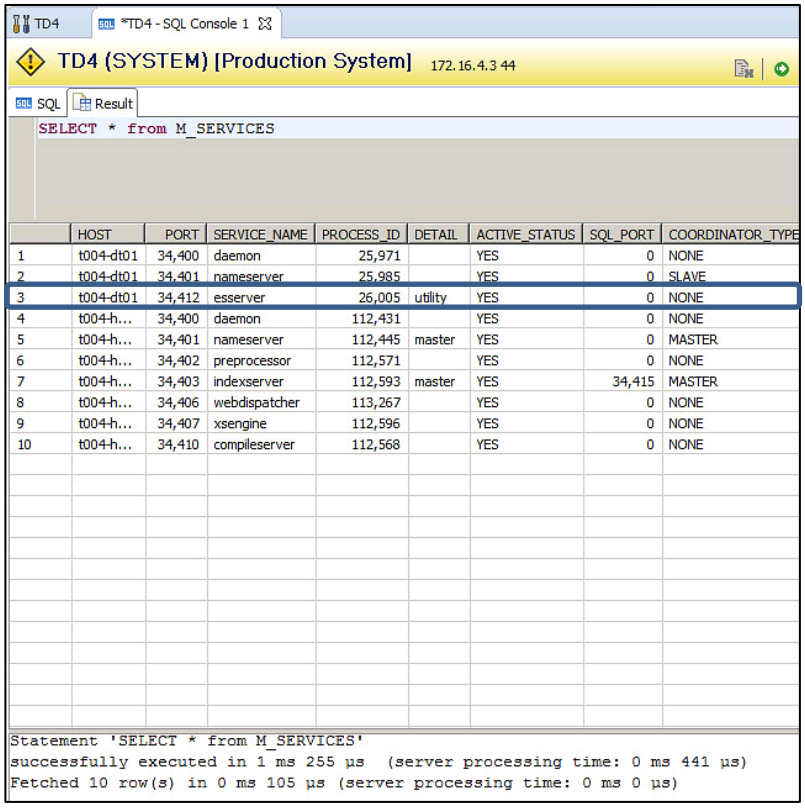
Use the SAP HANA Studio on a system with network access to the installed SAP HANA system and add the SAP HANA Database. The information you need to do so are as follows:

- Hostname or IP address <<var_t004_hana01_access_ip>>
- SAP HANA System Number <<var_t004_hana_nr>>
- SAP HANA database user (default: SYSTEM)
- SAP HANA database user password <<var_t004_hana_sys_passwd>>




You can see the esserver service listed to be running on DT host.

Use the M_SERVICES view to display the status for the dynamic tiering service on the dynamic tiering host.




On the SAP HANA dynamic tiering host, the coordinator type of the dynamic tiering service (esserver) can have one of the following statuses:

| Coordinator Type Status | Description |
|---|---|
| None | Dynamic tiering service is running, but extended storage is not created. |
| Master | Dynamic tiering service is running and extended storage is created. |
| Standby | The dynamic tiering host is configured as a standby host. |

In this example, TD4's t004-dt01 is the dynamic tiering worker. The status of NONE on the worker host indicates extended storage has not been created yet.



Once extended storage is created, the coordinator type status changes from NONE to MASTER.

# SAP HANA Scale Out System

This use case describes the setup N+1 Scale Out HANA system.

The high-level steps for this use case are as follows:

1. Create the access VLAN on Cisco Nexus 9000, and Cisco UCS.
2. Create Service Profile on Cisco UCS.
3. Define LUNs on the EMC VNX, register the server and configure the Storage-Group.
4. Install and Configure the Operating System.
5. Install SAP HANA.
6. Test the connection to the SAP HANA database.

## Workload Definition

The request to deploy this SAP HANA system has defined that the SAP HANA system must have a size of 1 TB to start with and has option to scale with requirement. This SAP HANA system is for production and has to run on SLES. The same is accomplished with a 2+1 scale-out cluster with each B260 M4 node having 512GB RAM.

## Requirements

For a SAP HANA Scale Out system the networks mandatorily required are the access network, the Inter-Node communication network and the storage network (in this case via Fibre Channel). This use case also requires a /hana/shared file system which is accessible to all nodes of the cluster. In this case a dedicated network for NFS is used. To access the installation sources for SAP HANA and other applications the access to the NFS share on the EMC VNX storage is also configured – this can be temporary only until all applications are installed. For this use case no optional network is used. This is the first system for a tenant, so no existing network definition can be used. As this is for Non-Production the relaxed storage requirements apply. The following configuration is required:

Network: 1x Access Network with >=100 Mbit/sec

1x Inter-Node Network with 10 GBit/sec

1x NFS-Network for /hana/shared >= 1 GBit/sec

1x Global-NFS Network for installation sources

SAP HANA Node

Storage: 512GB for /hana/log, 1.5TB for /hana/data, 1.5 TB for /hana/shared

## Switch Configuration

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following steps on both switches:

1. On each Nexus 9000, enter configuration mode:

```
config terminal
```

2. From the configuration mode, run the following commands:

```
vlan <<var_t005_access_vlan_id>>
name Tenant005-Access

vlan <<var_t005_internal_vlan_id>>
name Tenanat005-Internal

vlan <<var_t005_nfs_vlan_id>>
name Tenant005-NFS
```

3. Add the VLAN to the VPC Peer-Link:

```
interface po1
switchport trunk allowed vlan add
<<var_t005_access_vlan_id>>,<<var_t005_internal_vlan_id>>,<<var_t005_nfs_vlan_id>
>
```

4. Add the VLAN to the Port Channels connected to the Cisco UCS:

```
interface po13,po14
switchport trunk allowed vlan add
<<var_t005_access_vlan_id>>,<<var_t005_internal_vlan_id>>,<<var_t005_nfs_vlan_id>
>
```

5. Add the VLAN to the EMC VNX DataMovers

```
interface po33,po34
switchport trunk allowed vlan add <<var_t005_nfs_vlan_id>>
```

6. Add the VLAN to the data center uplink

```
interface po99
switchport trunk allowed vlan add <<var_t005_access_vlan_id>>
```

7. Save the running configuration to start-up:

```
copy run start
```

8. Validate the configuration:

```
#show vpc
```

```
…
vPC Peer-link status
--------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     76,177,199,2031,2034,3001-3005,3204-3205,3304-3305

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
…
13   Po13   up     success     success                    3001-3005,3
                                                          204-3205,33
                                                          04-3305
14   Po14   up     success     success                    3001-3005,3
                                                          204-3205,33
                                                          04-3305
…
33   Po33   up     success     success                    76,177,2034
                                                          ,3304,3305
34   Po34   down*  success     success                    -

…

#show vlan id 3005

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
     3005 Tenant005-Access                 active    Po1, Po13, Po14, Po99, Eth1/1
                                                     Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                           Eth1/9, Eth1/10, Eth1/15
                                                          Eth1/16, Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3005 enet         CE

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ----------------------------------------

#show vlan id 3205

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
       3205 Tenant005-Internal              active    Po1, Po13, Po14, Po33, Po34
                                                     Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                           Eth1/9, Eth1/10, Eth1/13
                                                          Eth1/14, Eth1/15, Eth1/16
                                                                   Eth1/17, Eth1/18
```

```
VLAN Type         Vlan-mode
---- -----        ----------
3205 enet         CE

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------

#show vlan id 3305

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
       3305 Tenant005-NFS                    active    Po1, Po13, Po14, Po33, Po34
                                                       Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                             Eth1/9, Eth1/10, Eth1/13
                                                           Eth1/14, Eth1/15, Eth1/16
                                                                    Eth1/17, Eth1/18

VLAN Type         Vlan-mode
---- -----        ----------
3305 enet         CE

Remote SPAN VLAN
----------------
Disabled

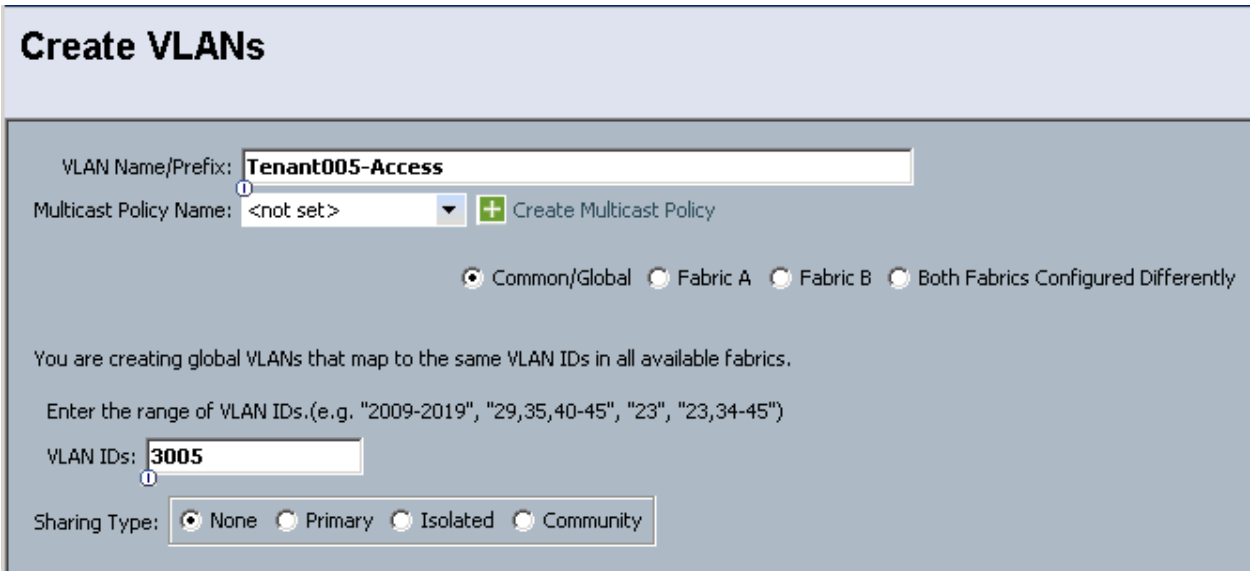
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------
---
```

## Cisco UCS Configuration

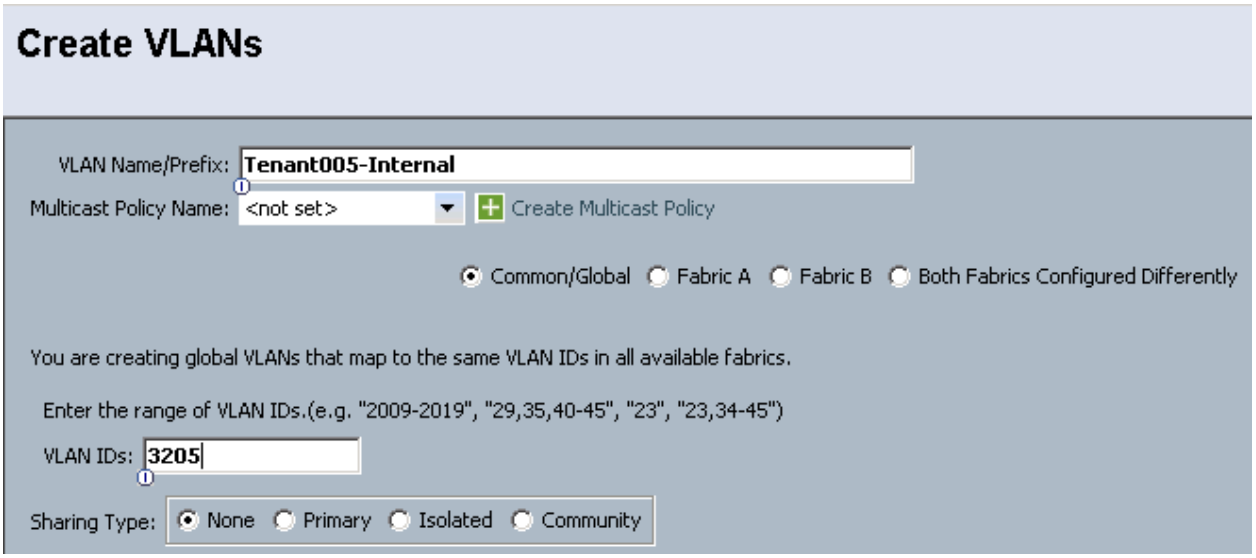
### Configure VLANs and VLAN-Group Membership

To create a VLAN, complete the following steps:

1. Log in to Cisco UCS Manager.
2. Go to LAN Tab > LAN Cloud > VLANs.
3. Right-click > Create VLANs.
4. Enter <<var_ucs_t005_access_vlan_name>> as the VLAN Name.
5. Enter <<var_t005_access_vlan_id>> as the VLAN ID.
6. Click OK.
7. Click OK.

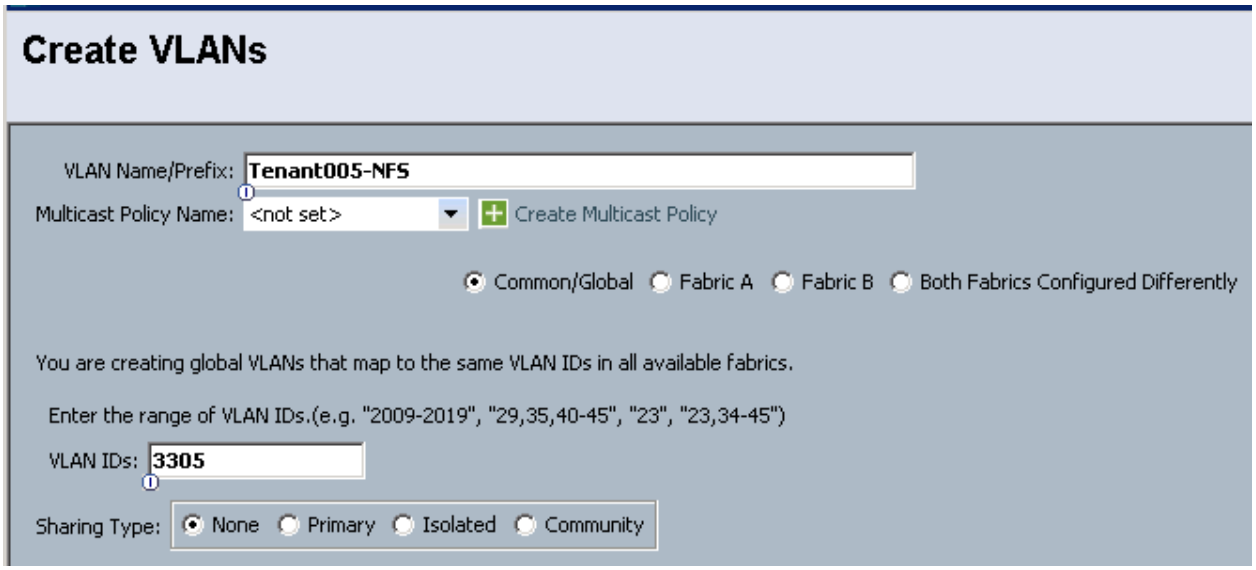



8. Right-click > Create VLANs
9. Enter <<var_ucs_t005_internal_vlan_name>> as the VLAN Name
10. Enter <<var_t005_internal_vlan_id>> as the VLAN ID
11. Click OK
12. Click OK



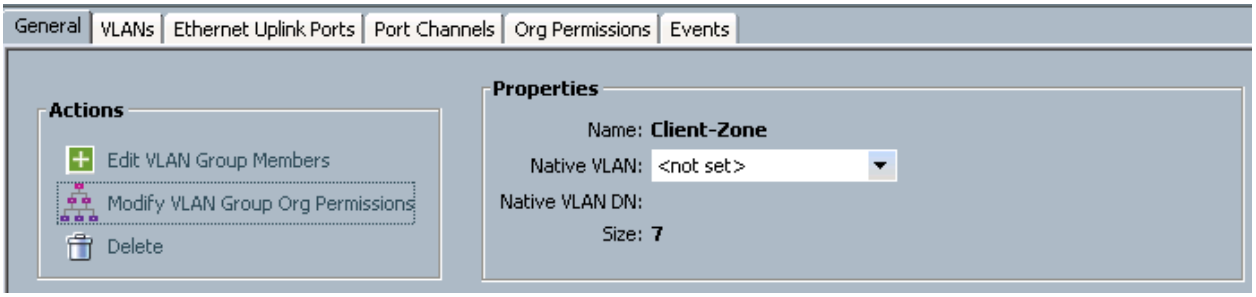

13. Right-Click > Create VLANs
14. Enter <<var_ucs_t004_nfs_vlan_name>> as the VLAN Name

15. Enter <<var_t004_nfs_vlan_id>> as the VLAN ID
16. Click OK
17. Click OK

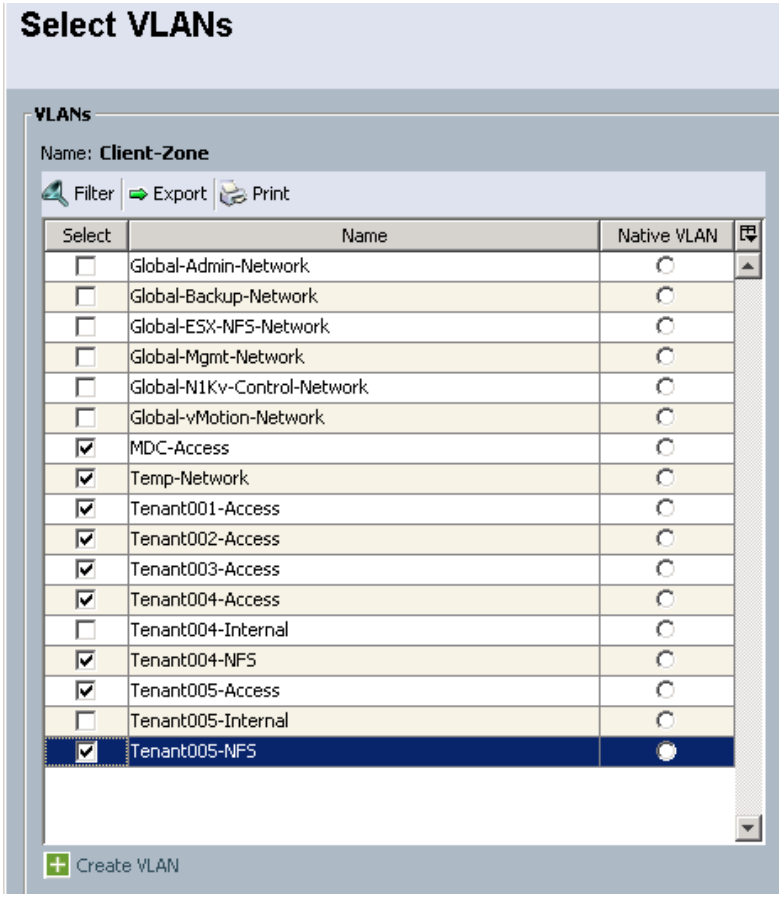



18. Go to LAN Tab > LAN Cloud > VLAN Groups.
19. Select VLAN group Client-Zone.
20. Click the Info icon 

on the right side of the list.
21. Click Edit VLAN Group Members.




22. Select <<var_ucs_t005_access_vlan_name>> and <<var_ucs_t005_nfs_vlan_name>>.
23. Click Finish.

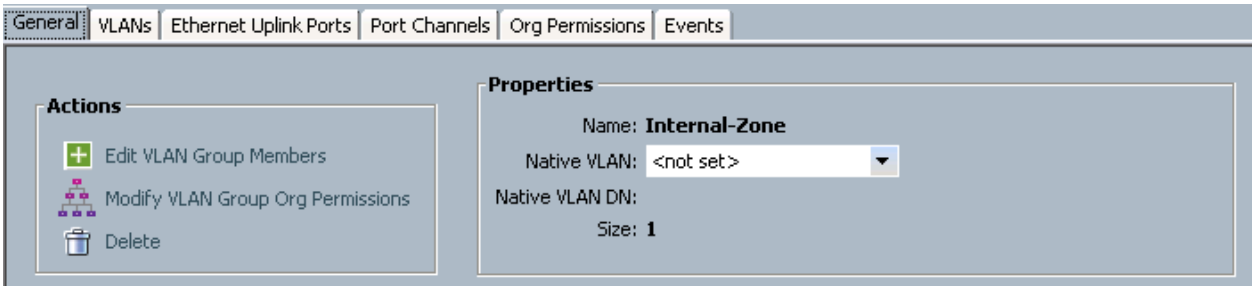



24. Click Finish.

25. Select VLAN group Internal-Zone in the right pane

26. Click the Info icon  on the right side of the list

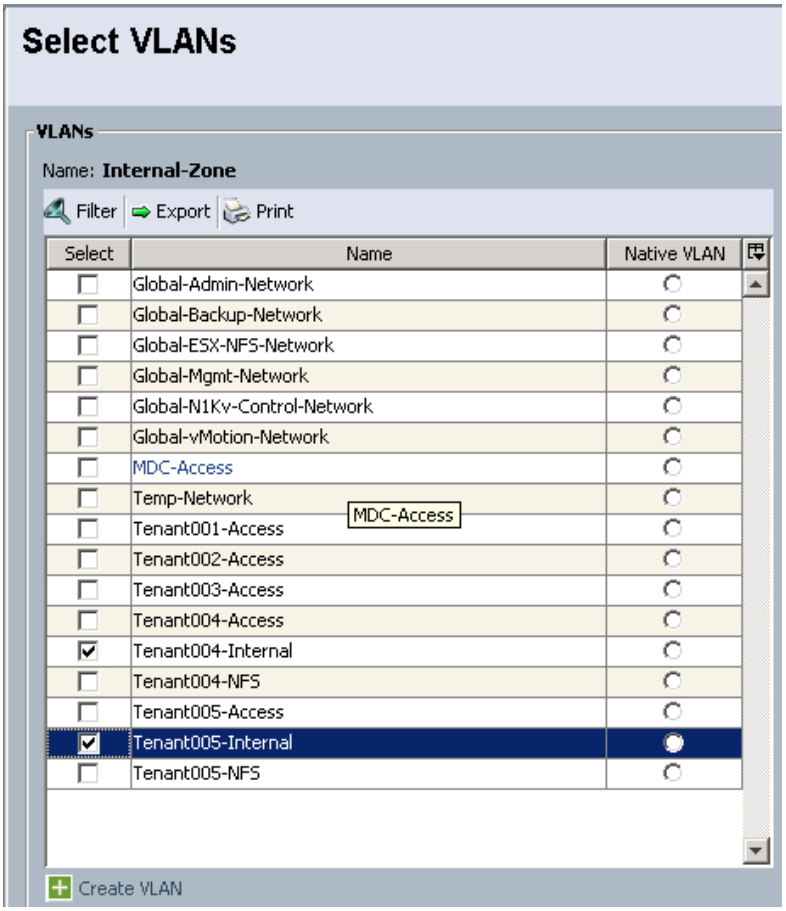

27. Click Edit VLAN Group Members




28. Select <<var_ucs_t004_internal_vlan_name>>

29. Click Finish

30. Click OK



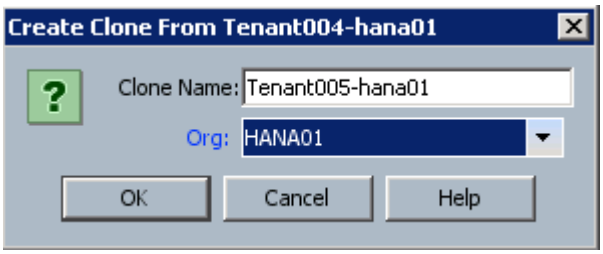

31. Click Finish

32. Click OK

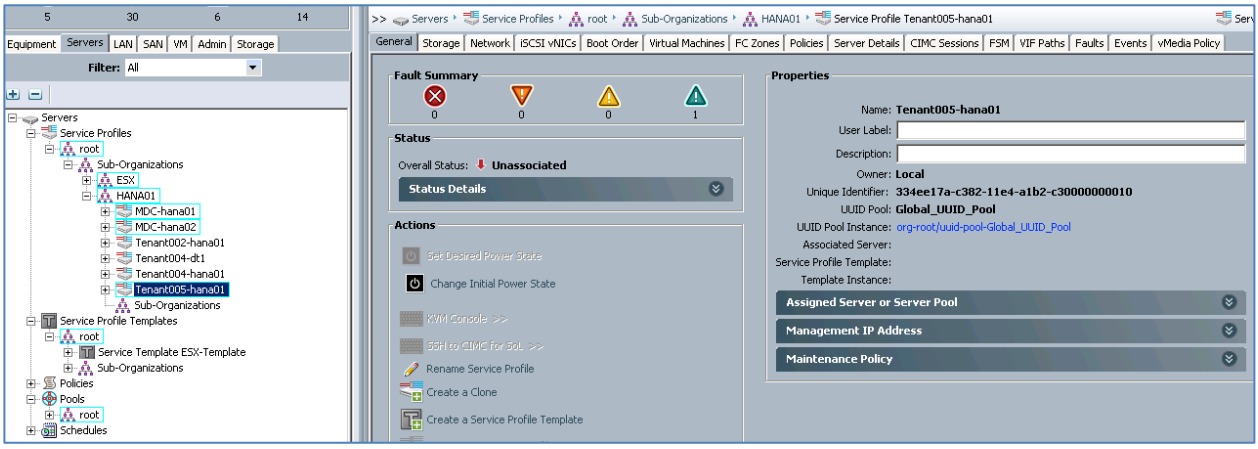
## Create Service Profile for the SAP HANA node on a Cisco UCS B460 M4 or C460 M4 Server

To create a service profile, complete the following steps:

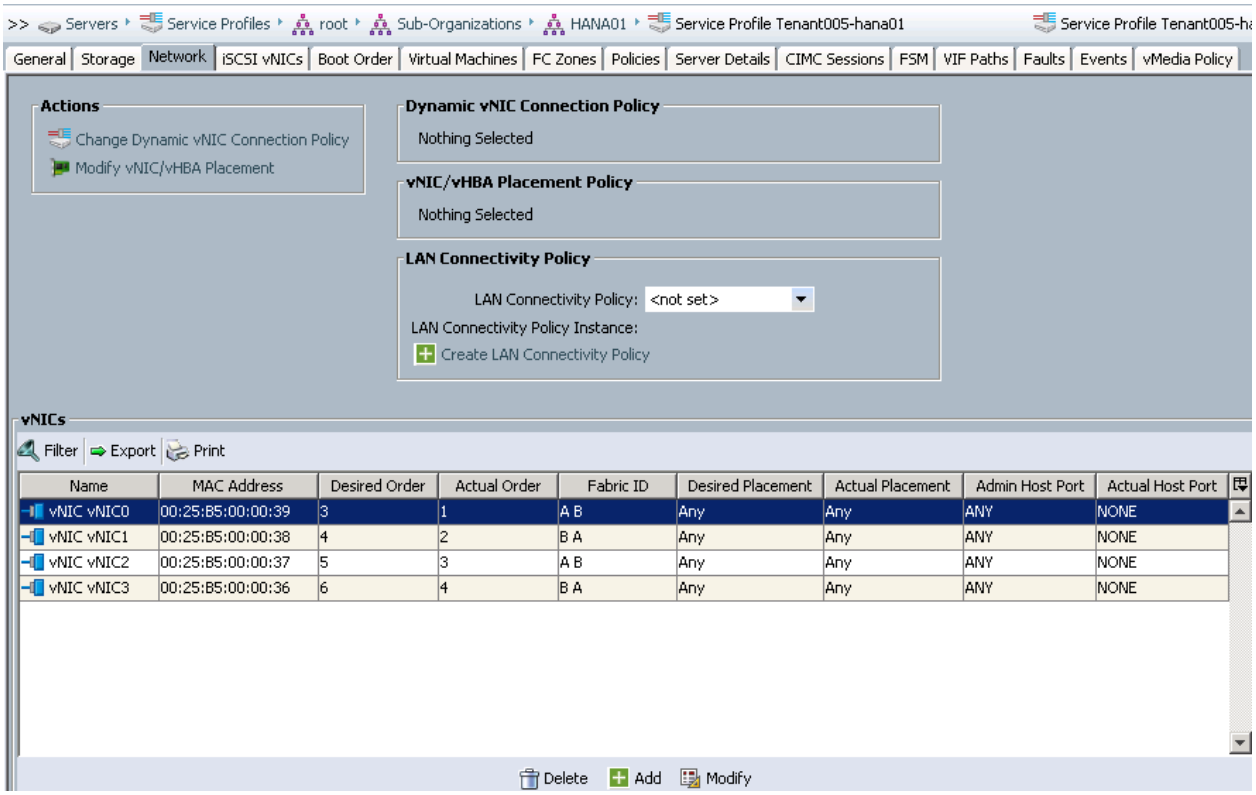
1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. Select an existing Service Profile in the Sub-Organization
3. Click Create a Clone
4. Enter <<var_ucs_t005_hana1_sp_name>> as the Name
5. Select <<var_ucs_hana01_org>> as the Org
6. Click OK




7. The Service Profile is available immediately

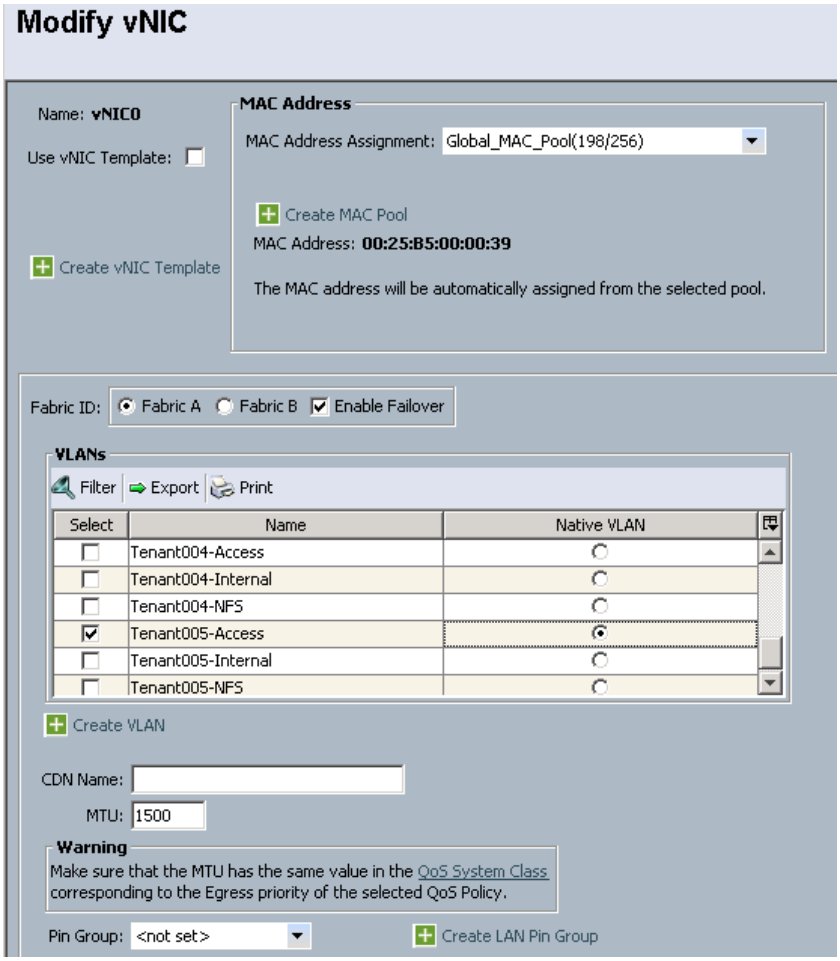



8. Click the Network tab and select vNIC0



9. Click the Modify icon.

10. Select <<var_ucs_t005_access_vlan_name>> and make it the Native VLAN.




11. Click OK.

12. Now go back to Network Tab then select vNIC1 and click Modify.

13. Select <<var_ucs_global_mac_pool_name>> from the MAC Address Assignment drop-down menu.

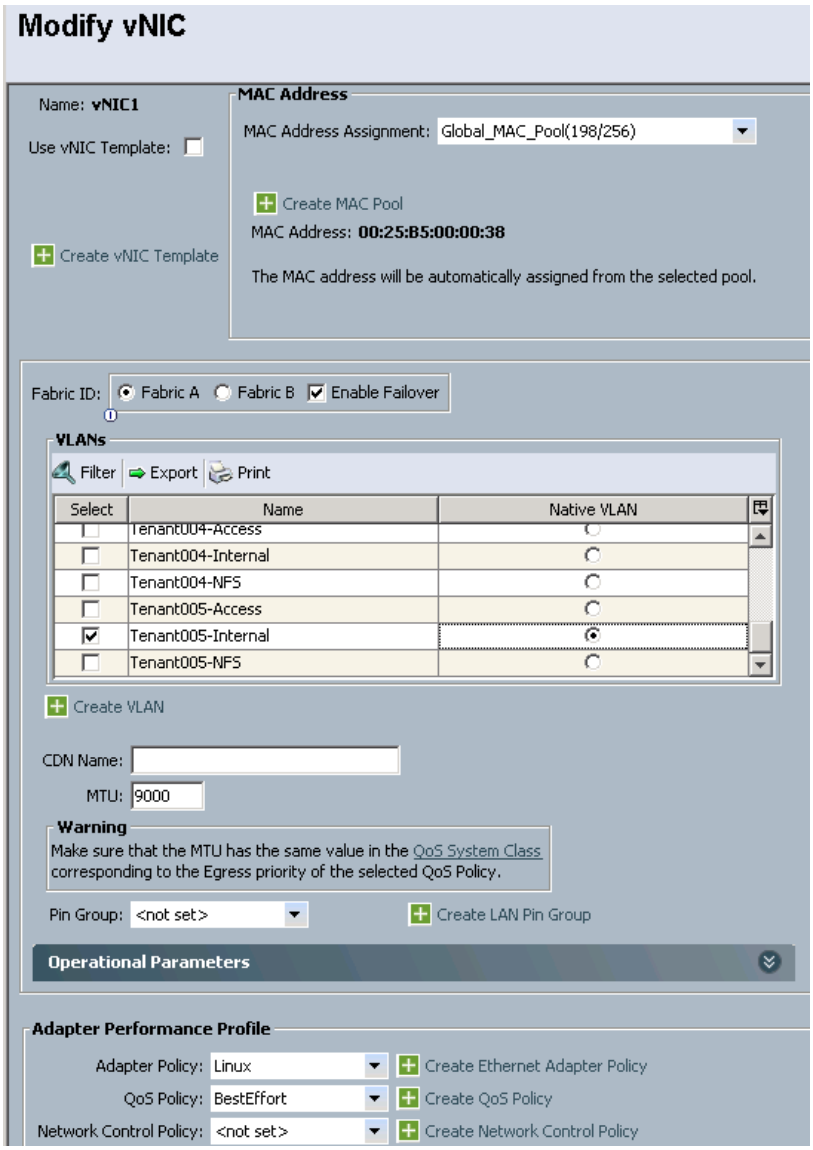
14. Select Fabric A and Enable Failover In the Fabric ID section.

15. Select <<var_ucs_t005_internal_vlan_name>> as the VLAN and make it the Native VLAN.

16. Enter 9000 as the MTU.

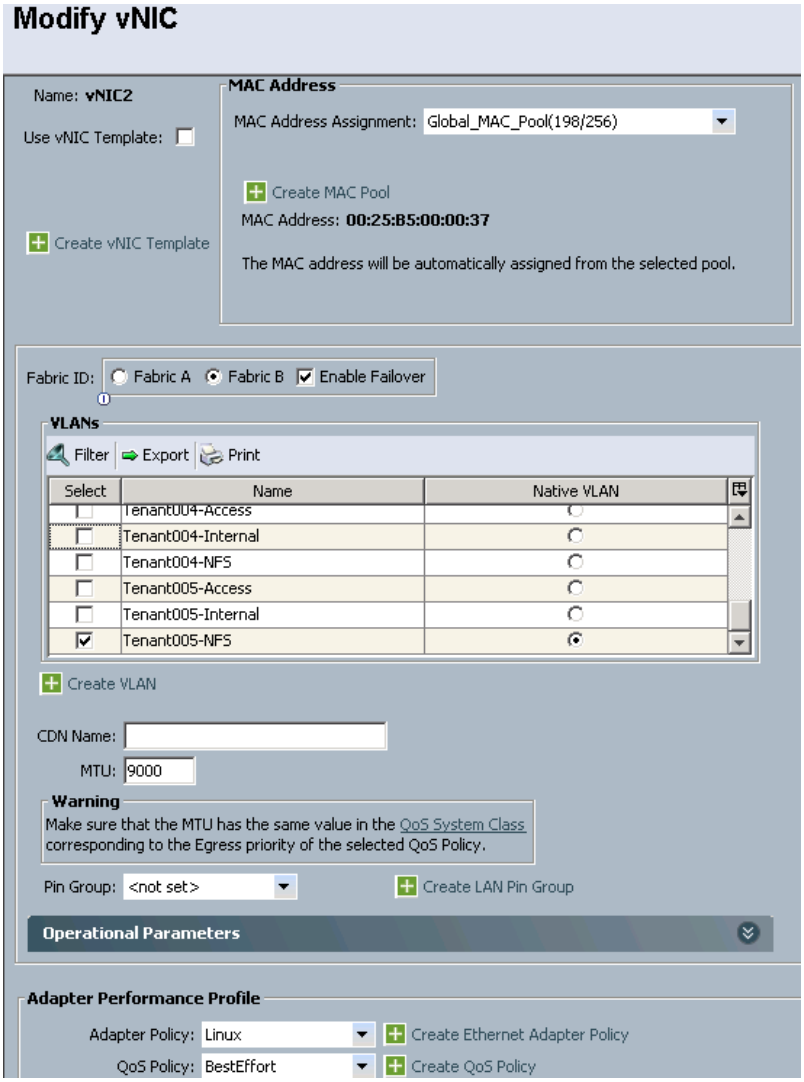
17. Select Linux as the Adapter Policy.

18. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy.




19. Click OK.
20. From the Network Tab select vNIC2 and click Modify.
21. Select <<var_ucs_global_mac_pool_name>> from the MAC Address Assignment drop-down menu
22. Select Fabric B and Enable Failover In the Fabric ID section
23. Select <<var_ucs_t005_nfs_vlan_name>> as the VLAN and make it the Native VLAN
24. Enter 9000 as the MTU
25. Select Linux as the Adapter Policy

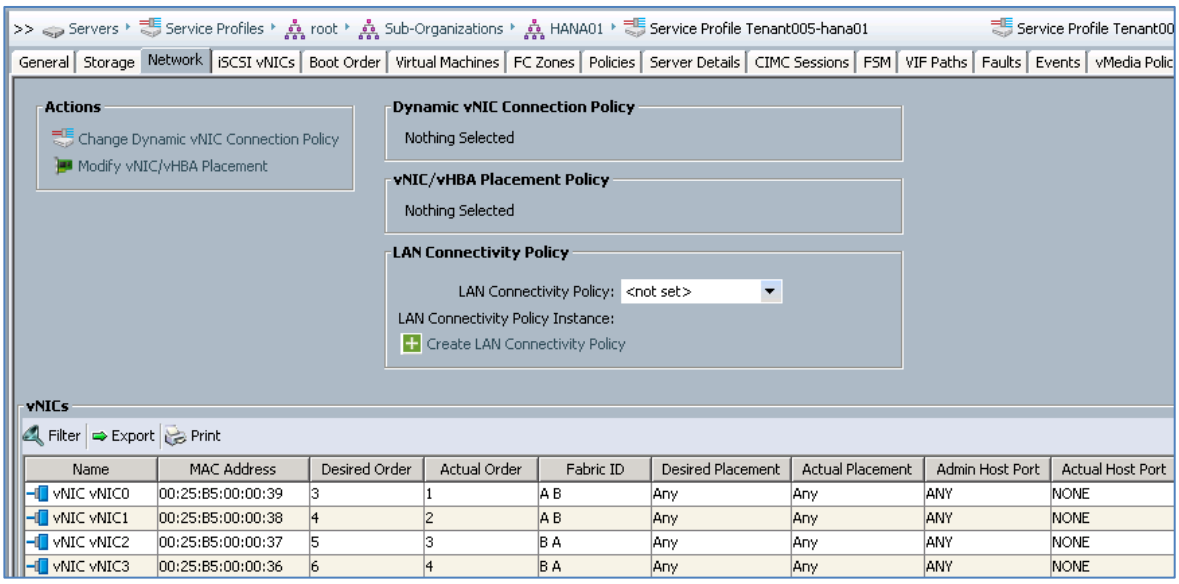
26. Select <<var_ucs_besteffort_policy_name>> as the QoS Policy



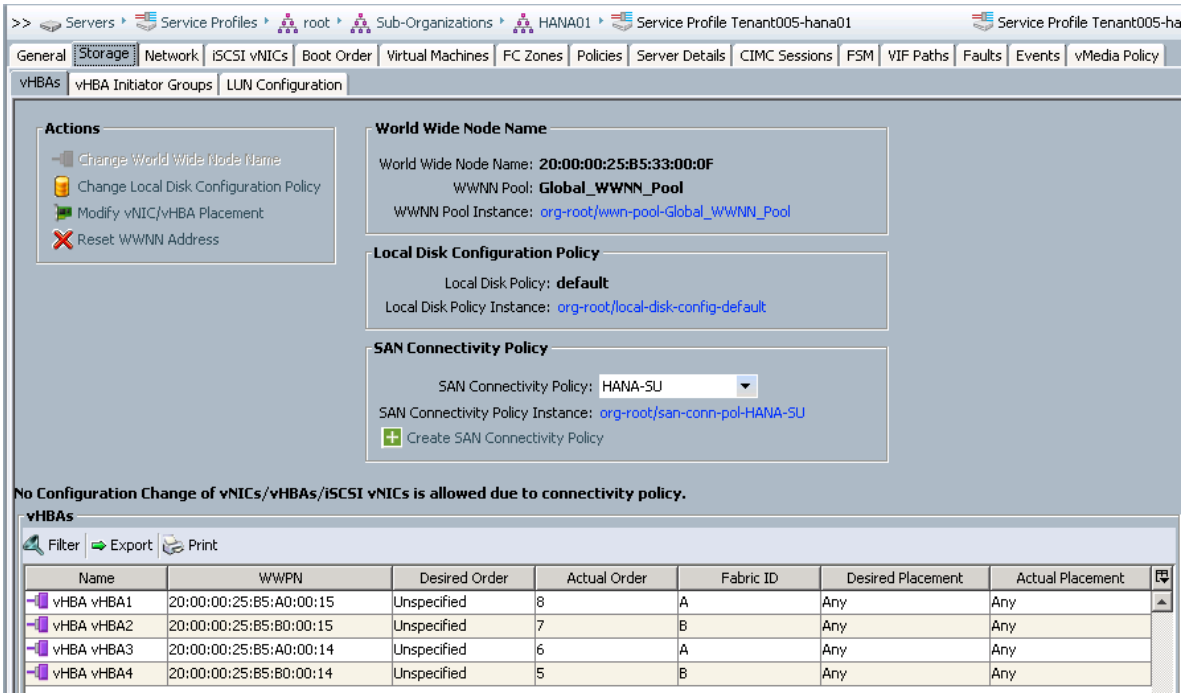

27. Click OK

28. Click Save Changes

29. Click OK




30. Click the Storage tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX



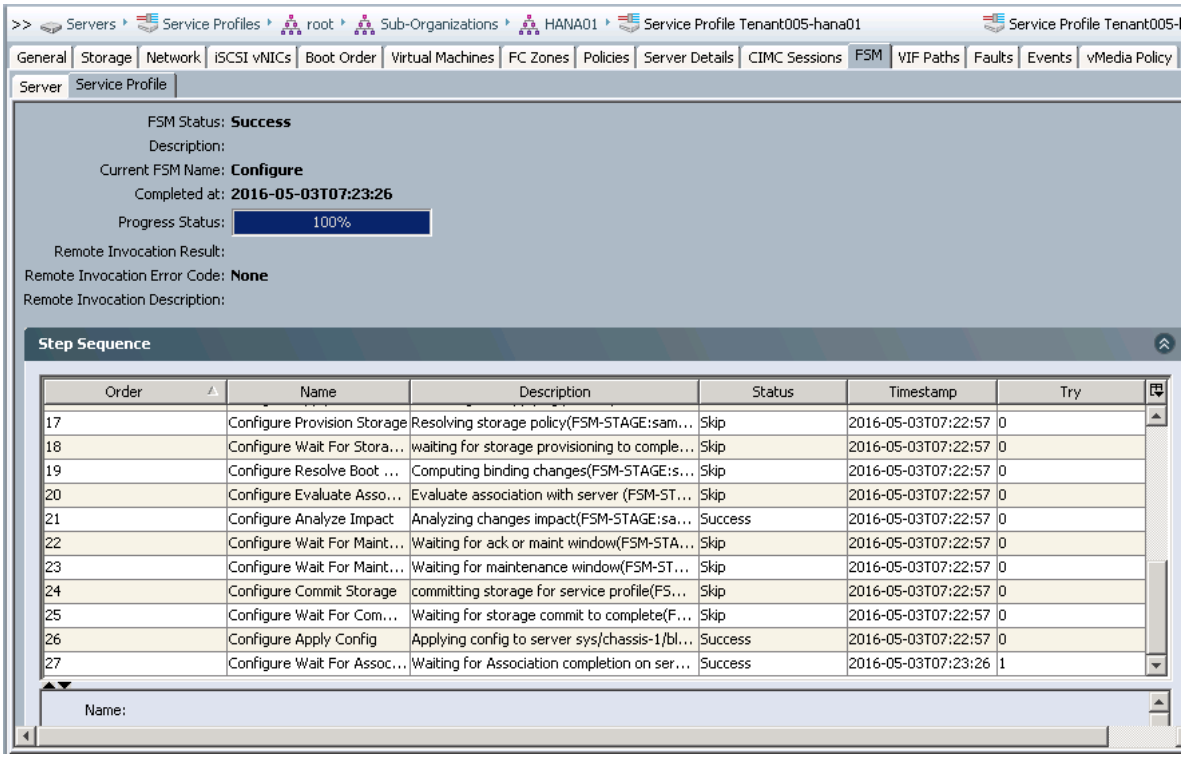

31. Select the General tab, click Change Service Profile Association

32. Select “Select existing Server” from the Server Assignment drop-down menu

33. Select a server that meets the requirements, click OK

34. Click Yes

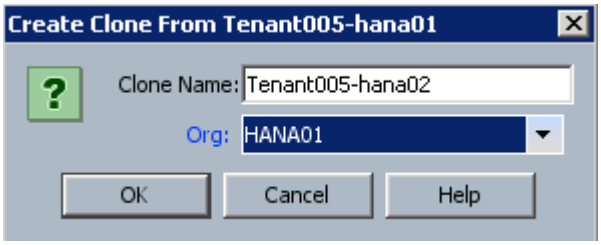
35. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.



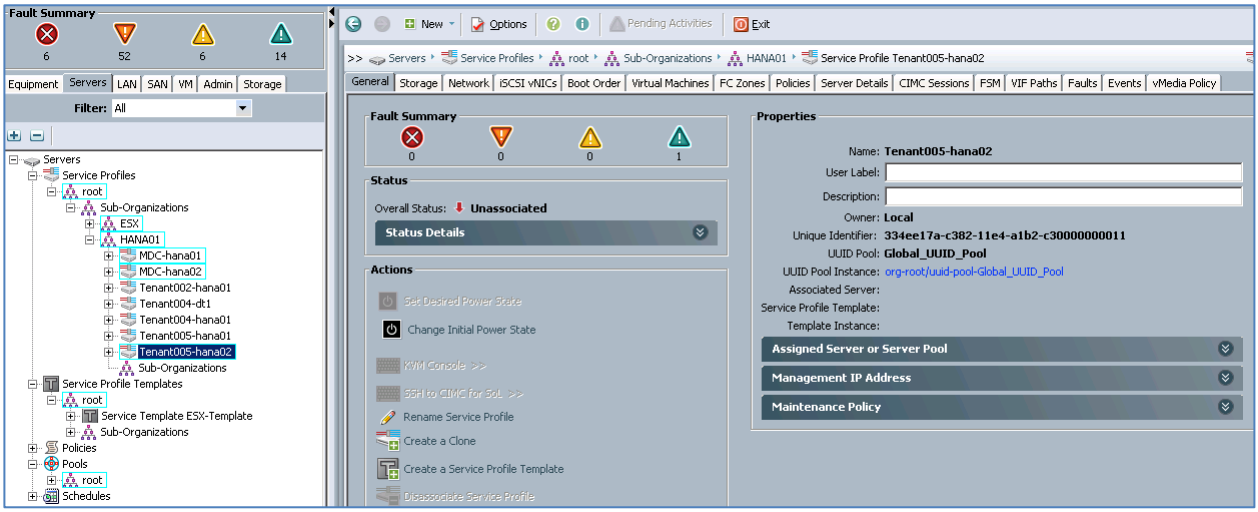

## Create Service Profile for the rest of nodes of Scale-Out cluster

The above procedure could be repeated to create required number of service profiles based on the number of nodes of the cluster. Below are steps to create two more nodes in the example.

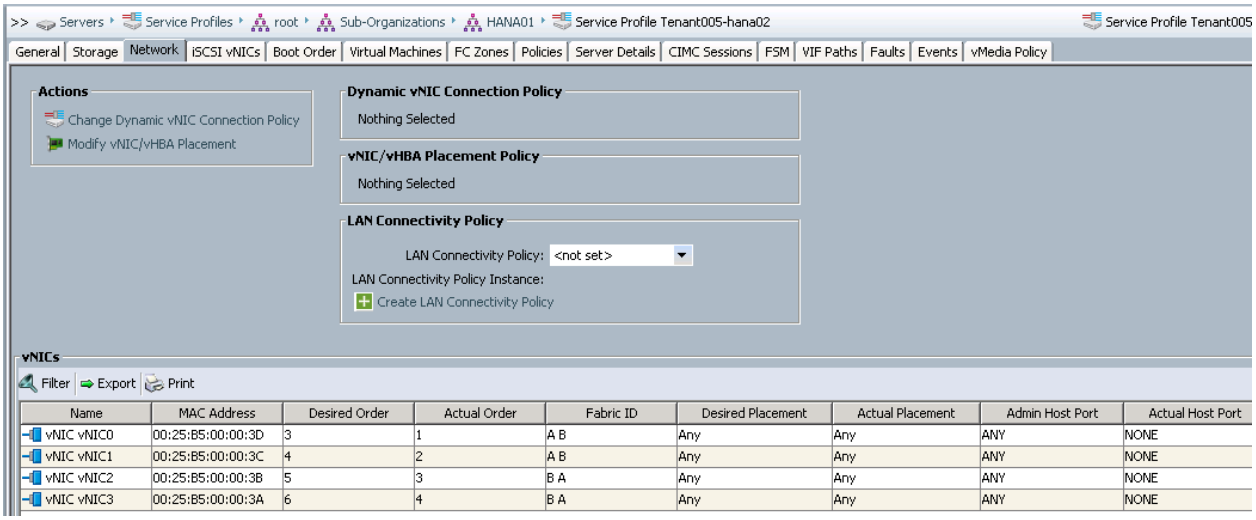
1. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
2. Select the existing Service Profile of the SAP HANA Node <<var_ucs_t005_hana1_sp_name>>
3. Click Create a Clone
4. Enter <<var_ucs_t005_hana2_sp_name>> as the Name
5. Select <<var_ucs_hana01_org>> as the Org
6. Click OK



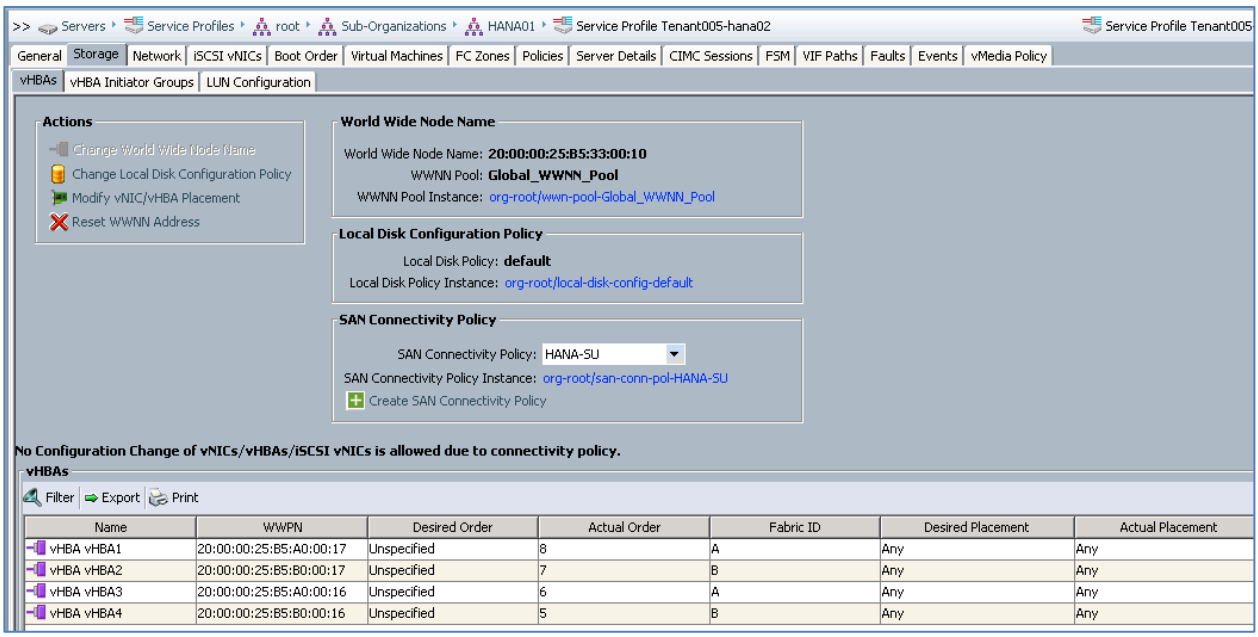
7. The Service Profile is available immediately



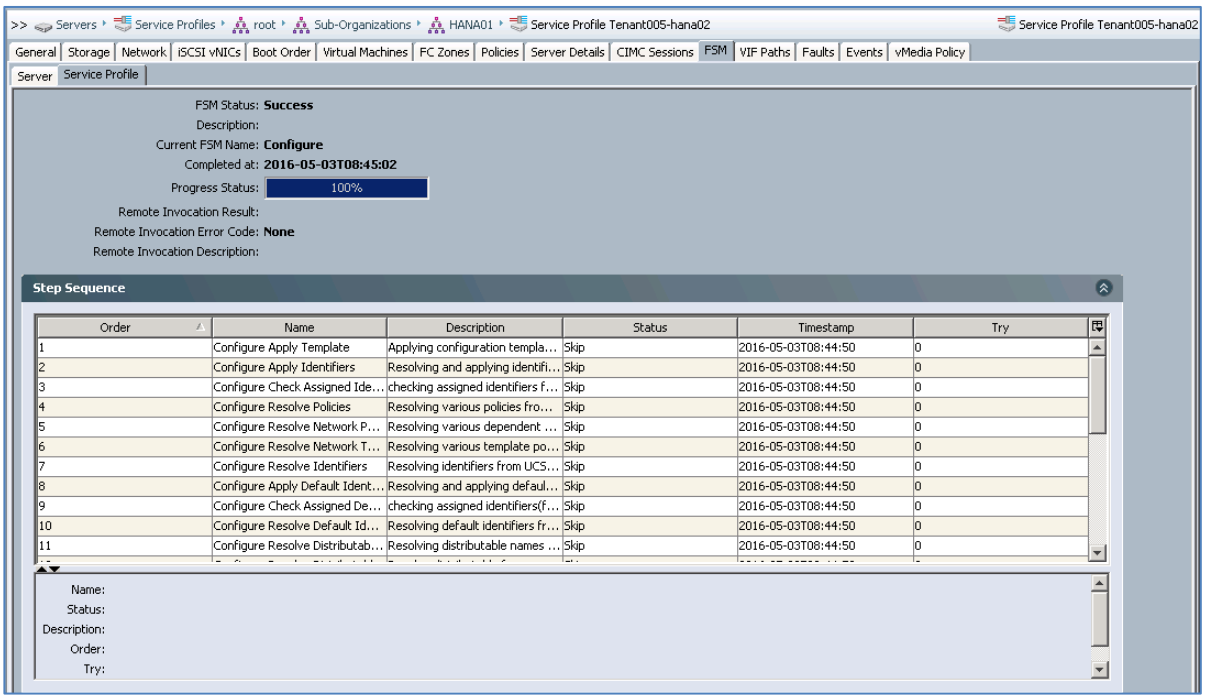

8. Click the Network tab and check the MAC addresses, those are required to configure the interfaces on the operating system later in the process



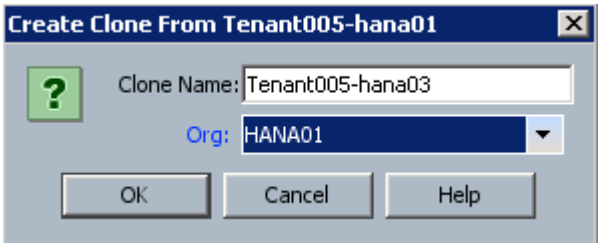

9. Click the Storage tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX



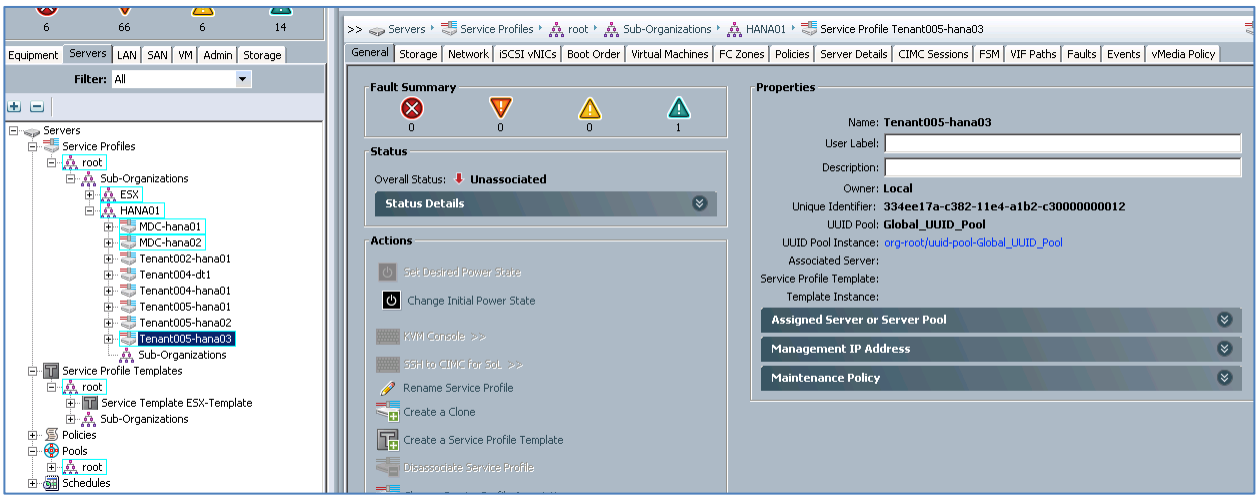

10. Select the General tab, click Change Service Profile Association
11. Select “Select existing Server” from the Server Assignment drop-down menu
12. Select a server that meets the requirements and click OK
13. Click Yes
14. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.



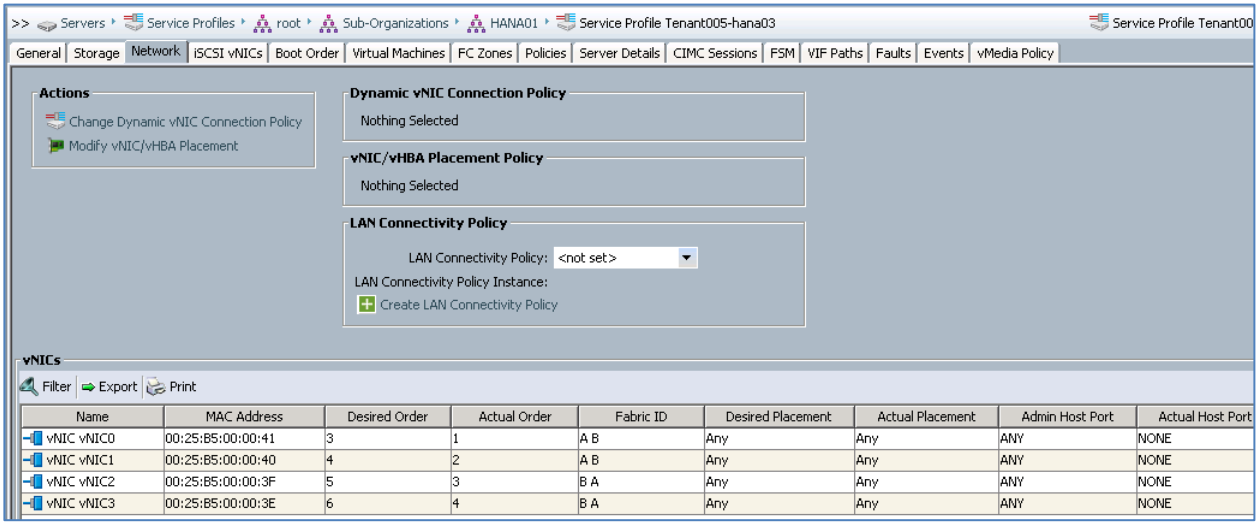

15. Repeat the steps to create the third service profile in the example.
16. Go to Server Tab > Servers > Service Profiles > root > Sub-Organizations > HANA01
17. Select the existing Service Profile of the SAP HANA Node <<var_ucs_t005_hana1_sp_name>>
18. Click Create a Clone
19. Enter <<var_ucs_t005_hana2_sp_name>> as the Name
20. Select <<var_ucs_hana01_org>> as the Org
21. Click OK




22. The Service Profile is available immediately

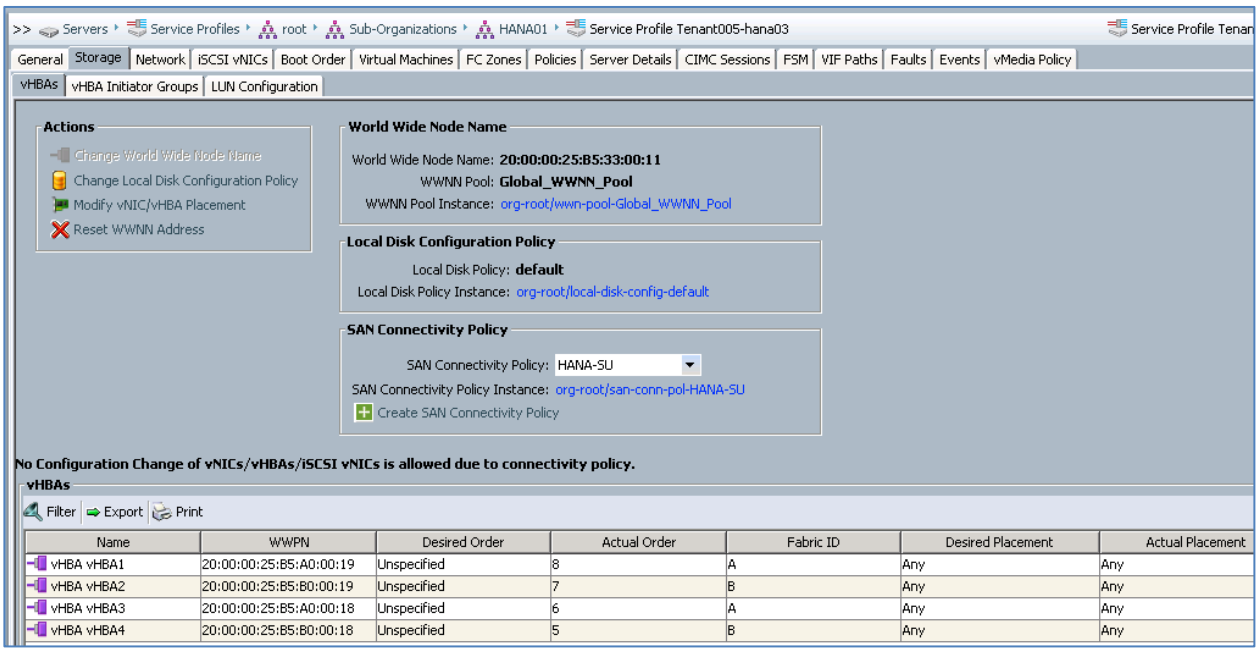



23. Click the Network tab and check the MAC addresses, those are required to configure the interfaces on the operating system later in the process

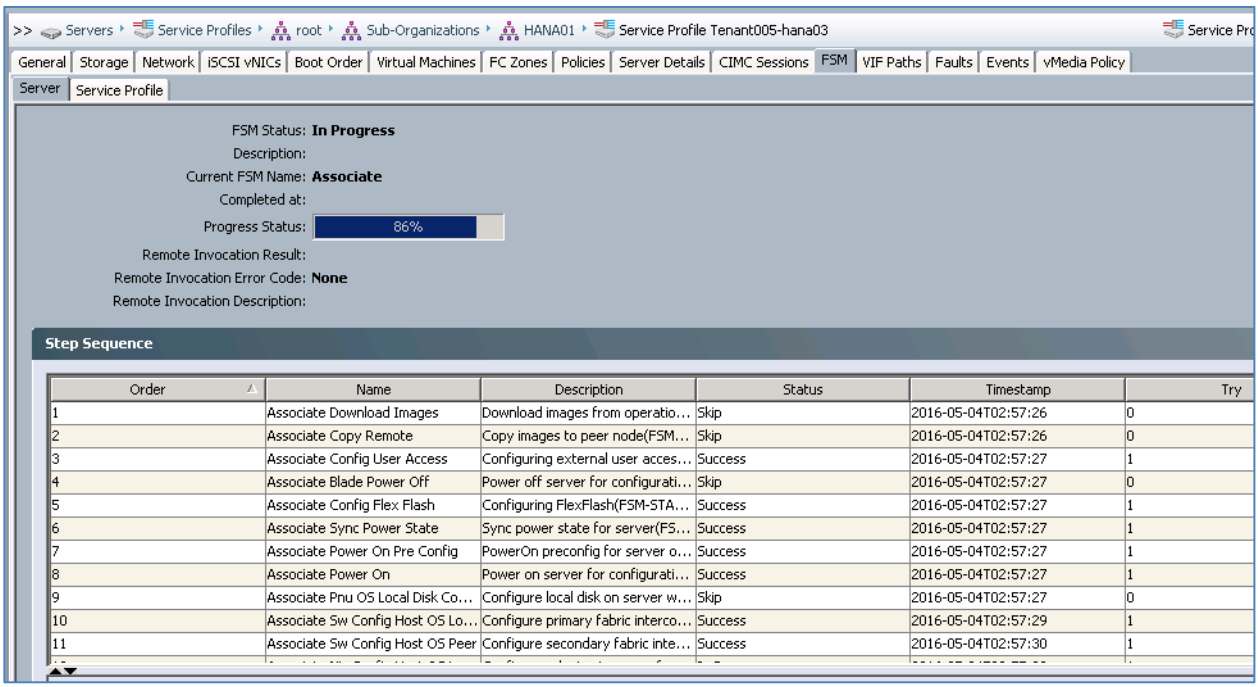



| Name | MAC Address | Desired Order | Actual Order | Fabric ID | Desired Placement | Actual Placement | Admin Host Port | Actual Host Port |
|---|---|---|---|---|---|---|---|---|
| vNIC vNIC0 | 00:25:B5:00:00:41 | 3 | 1 | A B | Any | Any | ANY | NONE |
| vNIC vNIC1 | 00:25:B5:00:00:40 | 4 | 2 | A B | Any | Any | ANY | NONE |
| vNIC vNIC2 | 00:25:B5:00:00:3F | 5 | 3 | B A | Any | Any | ANY | NONE |
| vNIC vNIC3 | 00:25:B5:00:00:3E | 6 | 4 | B A | Any | Any | ANY | NONE |

24. Click the Storage tab and check the WWPNs, those are required to configure the Zoning on the MDS switches and the Storage-Group on the EMC VNX




25. Select the General tab, click Change Service Profile Association
26. Select “Select existing Server” from the Server Assignment drop-down menu
27. Select a server that meets the requirements and click OK
28. Click Yes
29. Click OK. The Server will be configured and the progress can be monitored in the FSM tab.




## Configure Cisco MDS Switches

For every Service Profile in the Cisco UCS one or more SAN Zones are required per Cisco MDS switch.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t005-hana01>> vsan 10
zone name <<var_zone_t005-hana01>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:15
   exit
zone clone zone_temp_1path <<var_zone_t005-hana02>> vsan 10
zone name <<var_zone_t005-hana02>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:17
   exit

zone clone zone_temp_1path <<var_zone_t005-hana03>> vsan 10
zone name <<var_zone_t005-hana03>> vsan 10
```

```
   member pwwn 20:00:00:25:b5:a0:00:19
   exit

zoneset name CRA-EMC-A vsan 10
member <<var_zone_t005-hana01>>
member <<var_zone_t005-hana02>>
member <<var_zone_t005-hana03>>
exit

zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
…
zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

…
zone name zone_t005-hana01 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:15
```

```
zone name zone_t005-hana02 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:17
zone name zone_t005-hana03 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:19
CRA-EMC-A#
CRA-EMC-A# sh zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_t002-vhana1-data
  zone zone_MDC-hana01
  zone zone_t004-hana01_data
  zone zone_t004-dt01
  zone zone_t004-hana01
  zone zone_t005-hana01
  zone zone_t005-hana02
  zone zone_t005-hana03
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
copy run start
```

### Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp_1path <<var_zone_t005-hana01>> vsan 20
zone name <<var_zone_t005-hana01>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:15
   exit

zone clone zone_temp_1path <<var_zone_t005-hana02>> vsan 20
zone name <<var_zone_t005-hana02>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:17
   exit

zone clone zone_temp_1path <<var_zone_t005-hana03>> vsan 20
zone name <<var_zone_t005-hana03>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:19
   exit

zoneset name CRA-EMC-B vsan 20
member <<var_zone_t005-hana01>>
member <<var_zone_t005-hana01>>
member <<var_zone_t005-hana01>>
exit

zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_temp_1path vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_t005-hana01 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:15

zone name zone_t005-hana02 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:17

zone name zone_t005-hana03 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:19

CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host1
  zone zone_esx-host2
```

```
  zone zone_esx-host3
  zone zone_esx-host4
  zone zone_esx-host5
  zone zone_esx-host6
  zone zone_esx-host7
  zone zone_esx-host8
  zone zone_esx-host9
  zone zone_esx-host10
  zone zone_t002-vhana1
  zone zone_t002-vhana1-data
  zone zone_MDC-hana01
  zone zone_t004-hana1-data
  zone zone_t004-dt01
  zone zone_t004-hana01
  zone zone_t005-hana01
  zone zone_t005-hana02
  zone zone_t005-hana03
CRA-EMC-B#
```

4. Save the running configuration as startup configuration

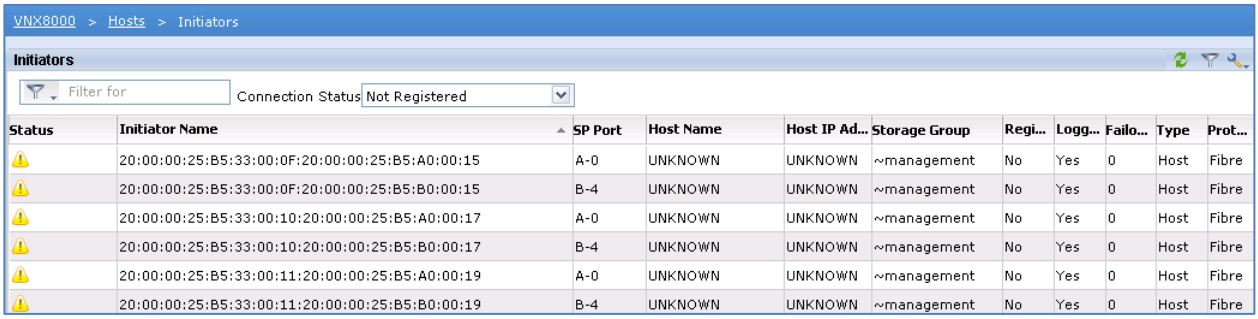
```
Copy run start
```

5. Reset the Servers' Service Profiles to ensure they are now able to see the VNX array post zoning configuration. You should then be able to see the vHBA initiators logging into VNX array.

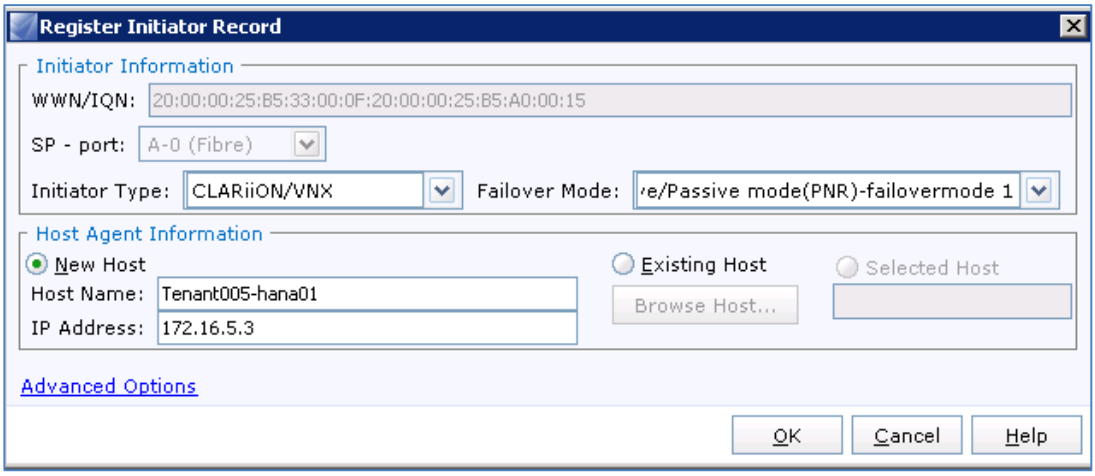
## Configure EMC VNX

### Register Host

1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators

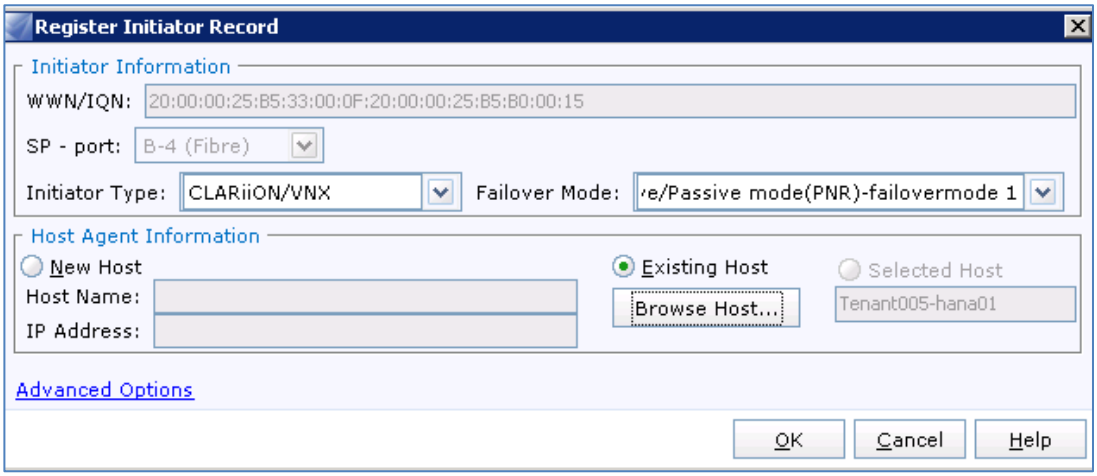



2. Select one of the unregistered entries for the host <<var_ucs_t005_hana1_name>>, Click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
5. Enter <<var_ucs_t005_hana1_name>> as the Host Name (indicates the relationship to the Service Profile)
6. Enter <<var_t005_hana1_access_ip>> as the IP Address
7. Click OK
8. Click Yes
9. Click OK
10. Click OK

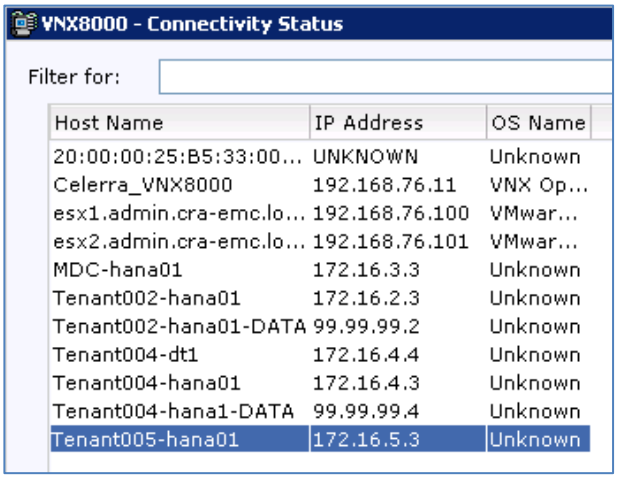



11. Select the second Entry for this host <<var_ucs_t005_hana1_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

14. Select Existing Host and click Browse Host




15. Select <<var_ucs_t005_hana1_name>> and click OK




16. Click OK

17. Click Yes

18. Click OK

19. Click OK

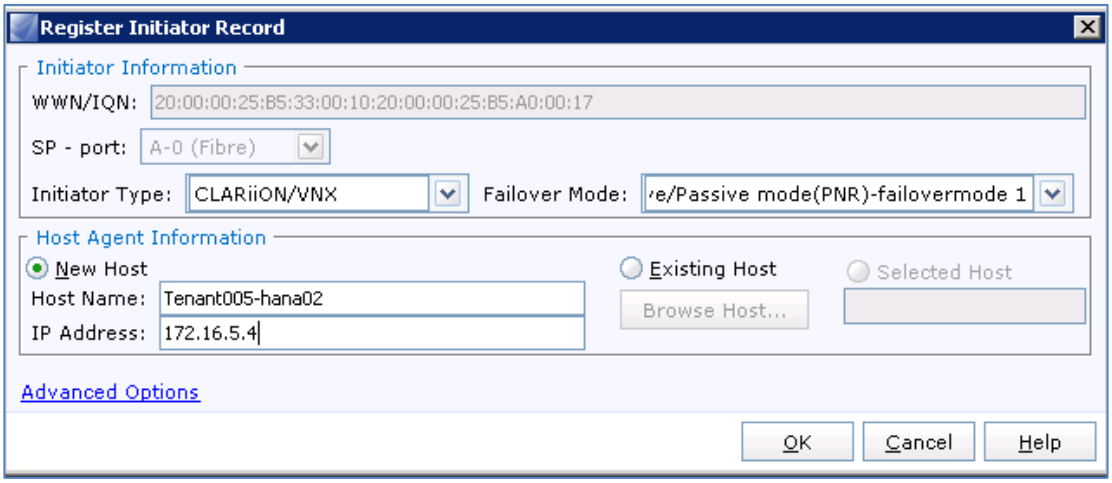
20. Select one of the unregistered entries for the host <<var_ucs_t005_hana2_name>>, click Register

21. Select CLARiiON/VNX as the Initiator Type

22. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

23. Enter <<var_ucs_t005_hana2_name>> as the Host Name (indicates the relationship to the Service Profile)

24. Enter <<var_t005_hana2_access_ip>> as the IP Address




25. Click OK

26. Click Yes

27. Click OK

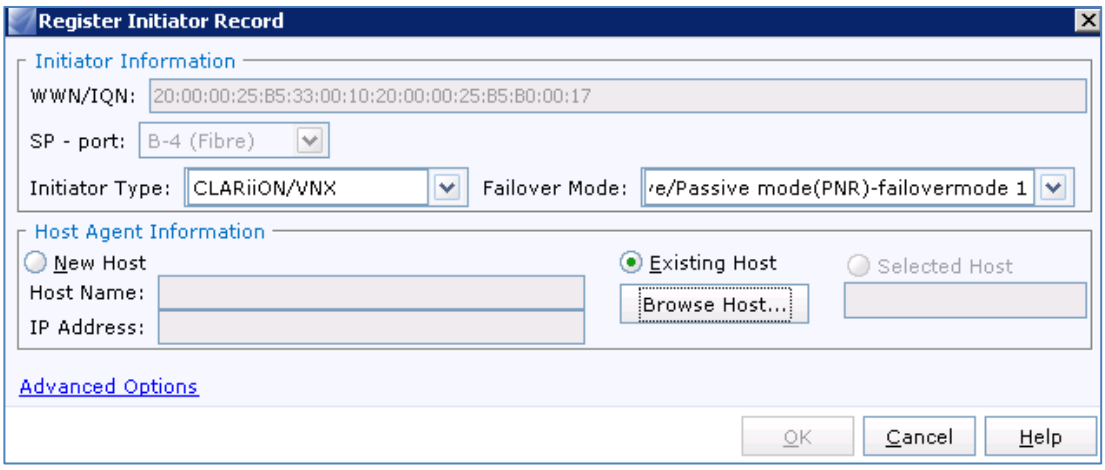
28. Click OK

29. Select the second Entry for this host <<var_ucs_t005_hana2_name>>, click Register

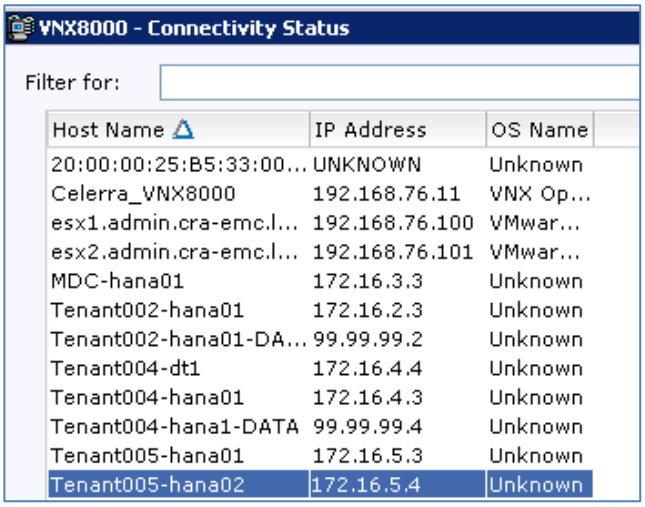
30. Select CLARiiON/VNX as the Initiator Type

31. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

32. Select Existing Host and click Browse Host




33. Select <<var_ucs_t005_hana2_name>> and click OK




34. Click OK

35. Click OK

36. Click Yes

37. Click OK

38. Click OK

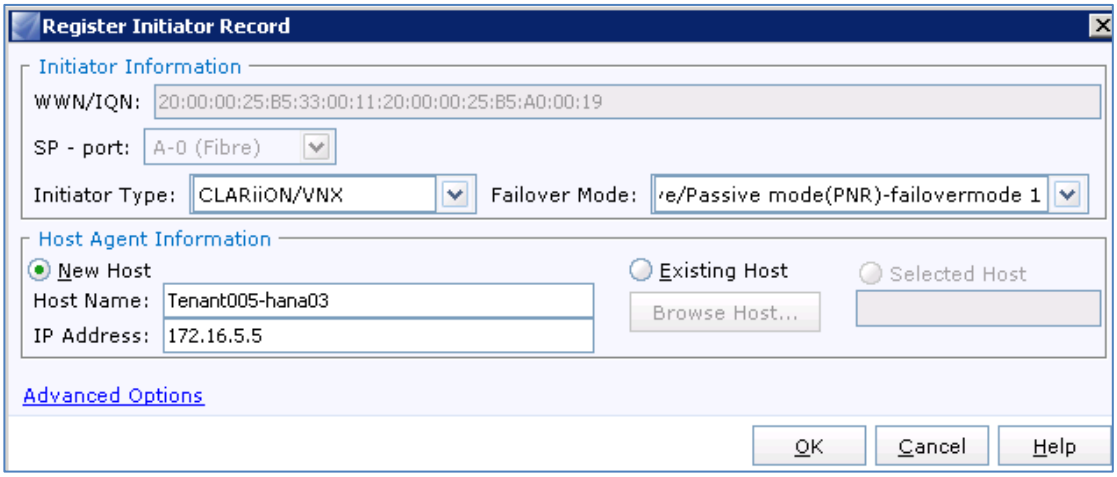
39. Select one of the unregistered entries for the host <<var_ucs_t005_hana3_name>>, click Register

40. Select CLARiiON/VNX as the Initiator Type

41. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

42. Enter <<var_ucs_t005_hana3_name>> as the Host Name (indicates the relationship to the Service Profile)

43. Enter <<var_t005_hana3_access_ip>> as the IP Address




44. Click OK

45. Click Yes

46. Click OK

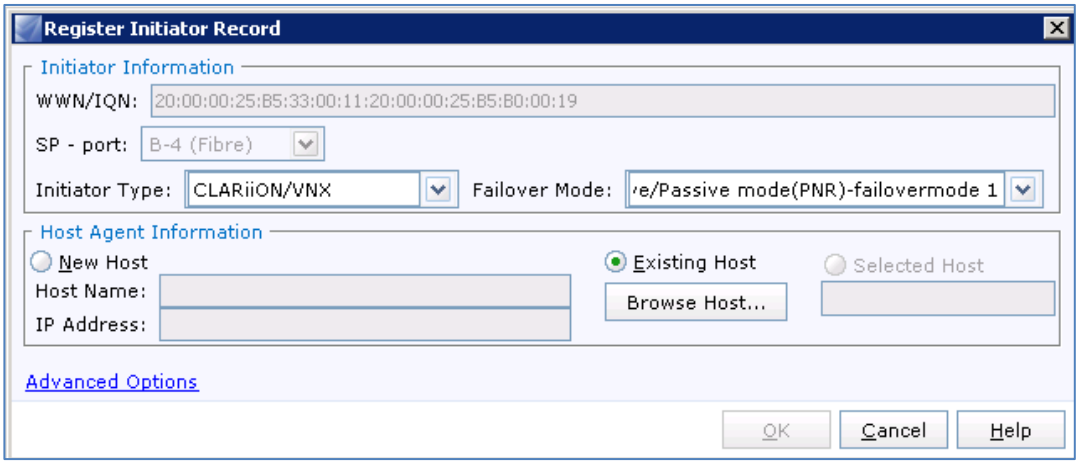
47. Click OK

48. Select the second Entry for this host <<var_ucs_t005_hana3_name>>, Click Register

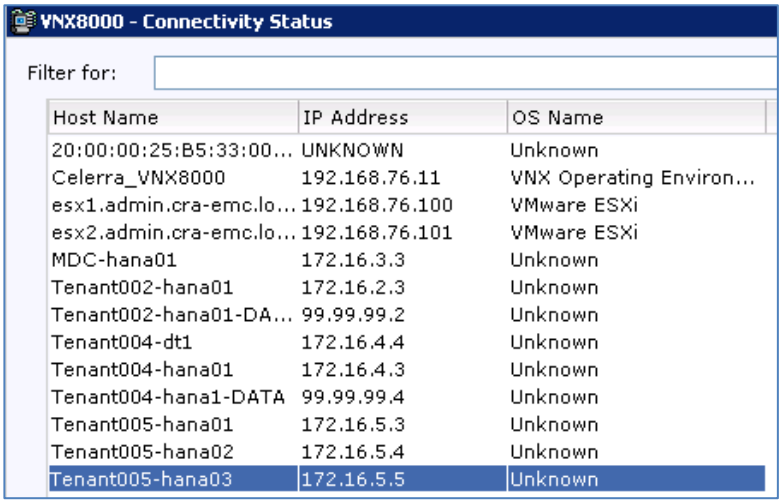
49. Select CLARiiON/VNX as the Initiator Type

50. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode

51. Select Existing Host and click Browse Host




52. Select <<var_ucs_t005_hana3_name>> and click OK




53. Click OK

54. Click OK

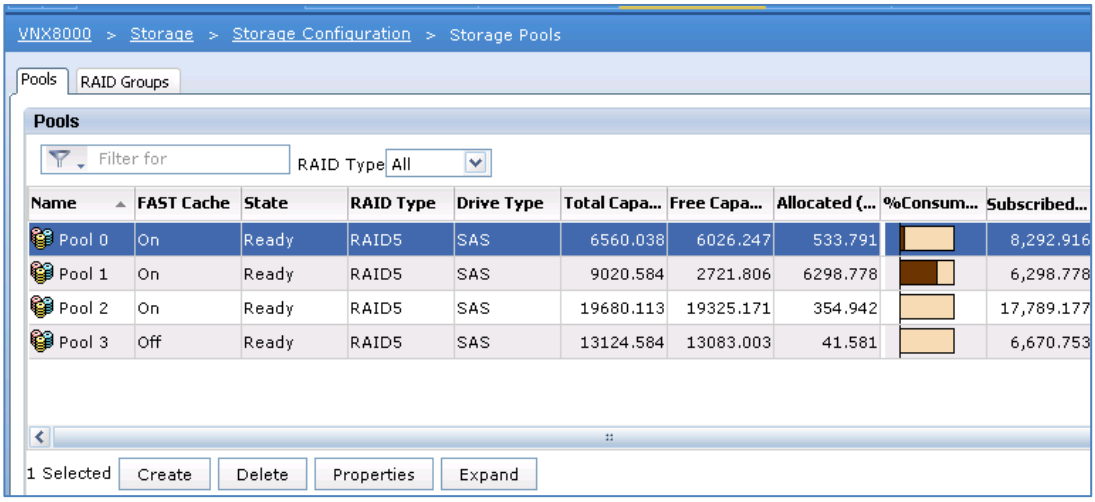
55. Click Yes

56. Click OK

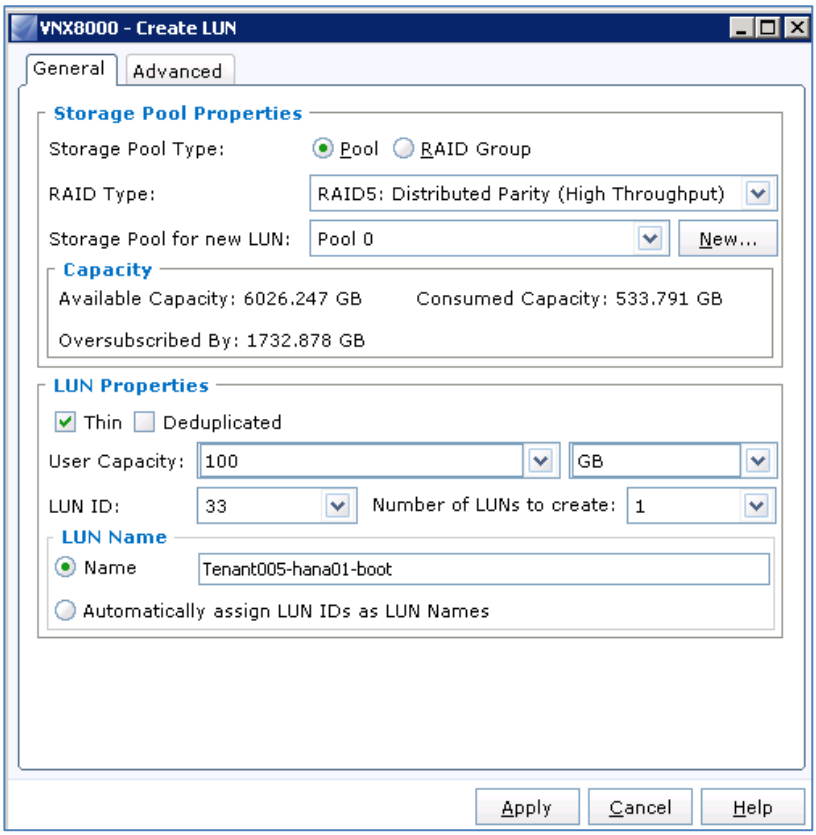
57. Click OK

## Create LUNs

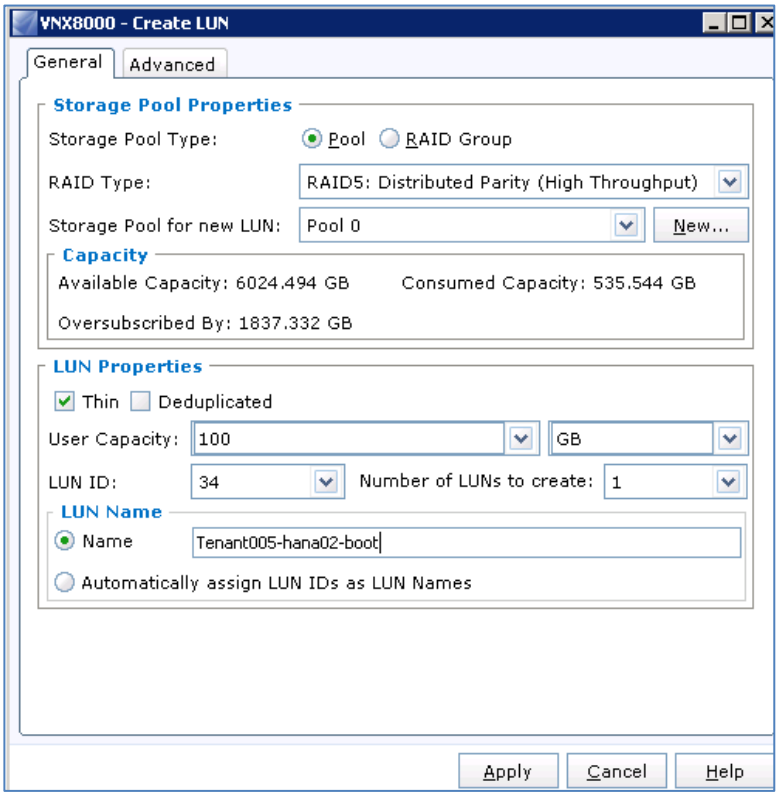
1. Navigate to Storage > Storage Pool



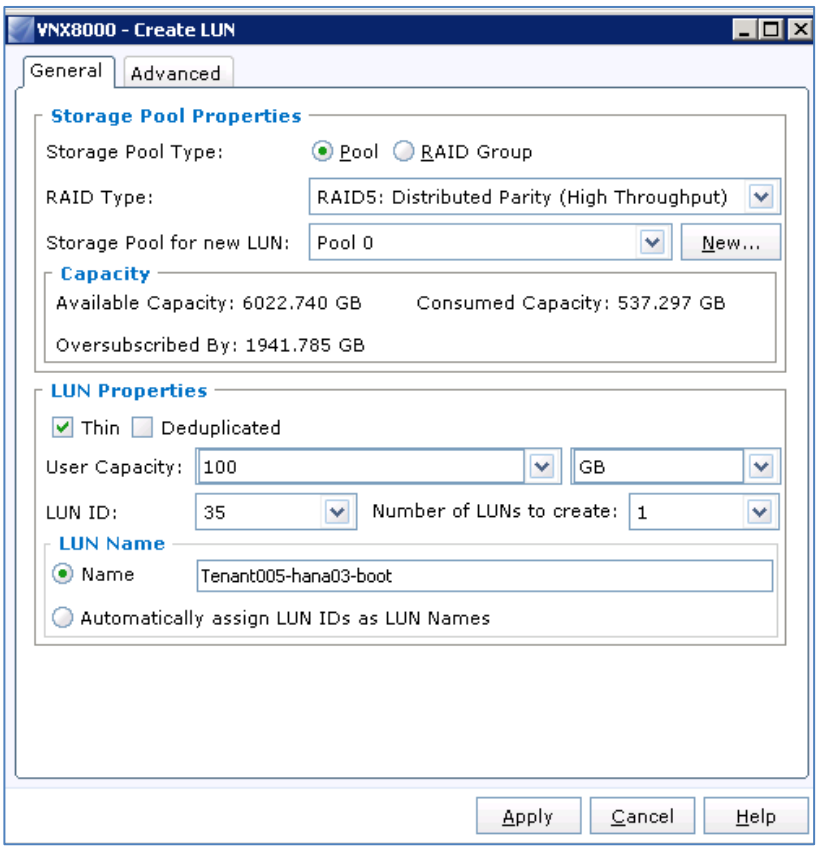

2. Right-click Pool 0
3. Select Create LUN
4. Enter 100 GB as the User Capacity
5. Click Name and enter <<var_ucs_t005_hana1_name>>-boot



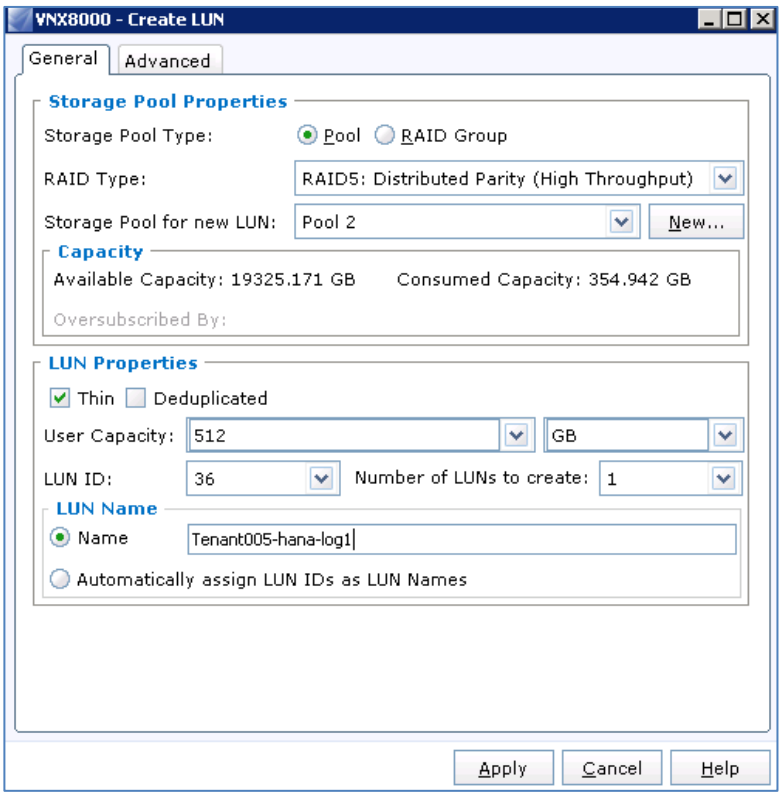
6. Click Apply
7. Click Yes
8. Click OK
9. Enter 100 GB as the User Capacity
10. Click Name and enter <<var_ucs_t005_hana2_name>>-boot



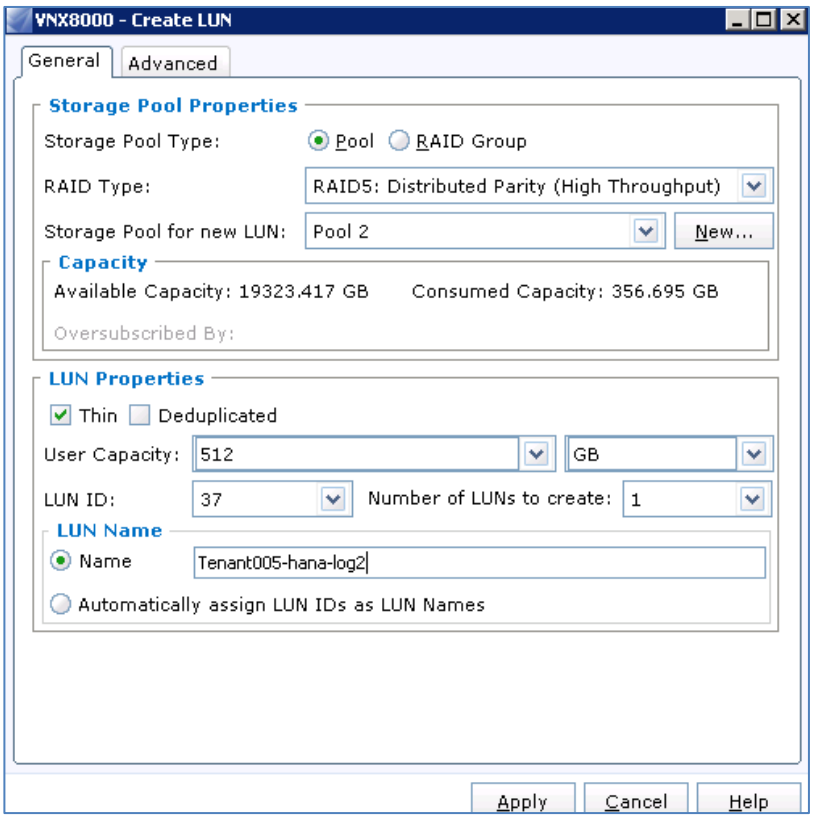

11. Click Apply
12. Click Yes
13. Click OK
14. Enter 100 GB as the User Capacity
15. Click Name and enter <<var_ucs_t005_hana3_name>>-boot




16. Click Apply
17. Click Yes
18. Click OK
19. Click Cancel
20. Right-click Pool 2
21. Select Create LUN
22. Enter 512 GB as the User Capacity
23. Click Name and enter <<var_ucs_t005-hana_sys-name>>-log1




24. Click Apply
25. Click Yes
26. Click OK
27. Enter 512 GB as the User Capacity
28. Click Name and enter <<var_ucs_t005-hana_sys-name>>-log2



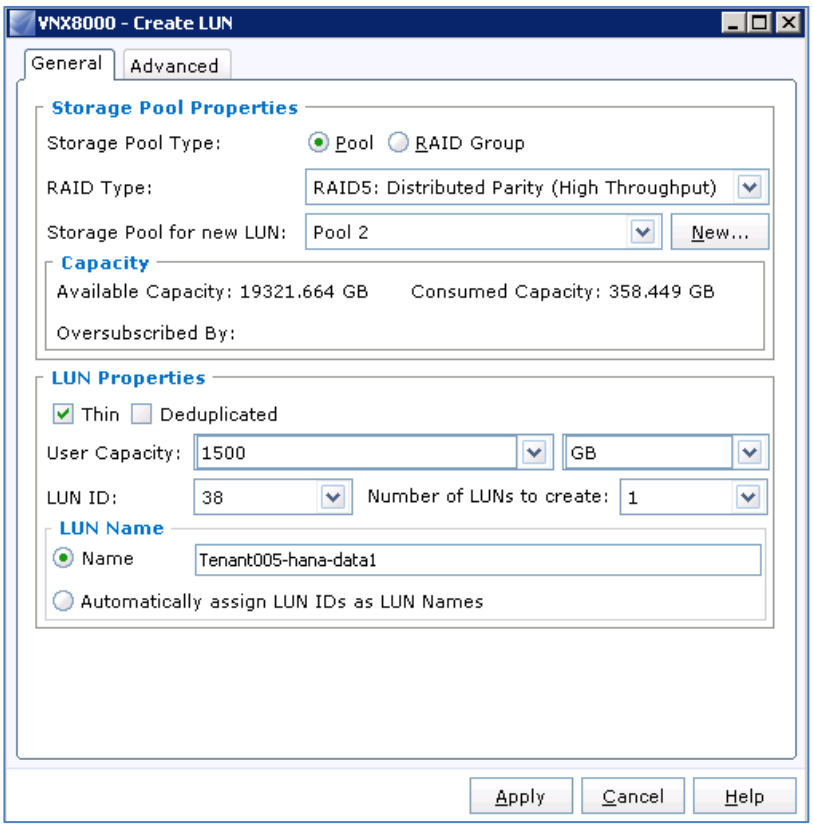

29. Click Apply

30. Click Yes

31. Click OK

32. Enter 1.5 TB as the User Capacity

33. Click Name and enter <<var_ucs_t005-hana_sys-name>>-data1



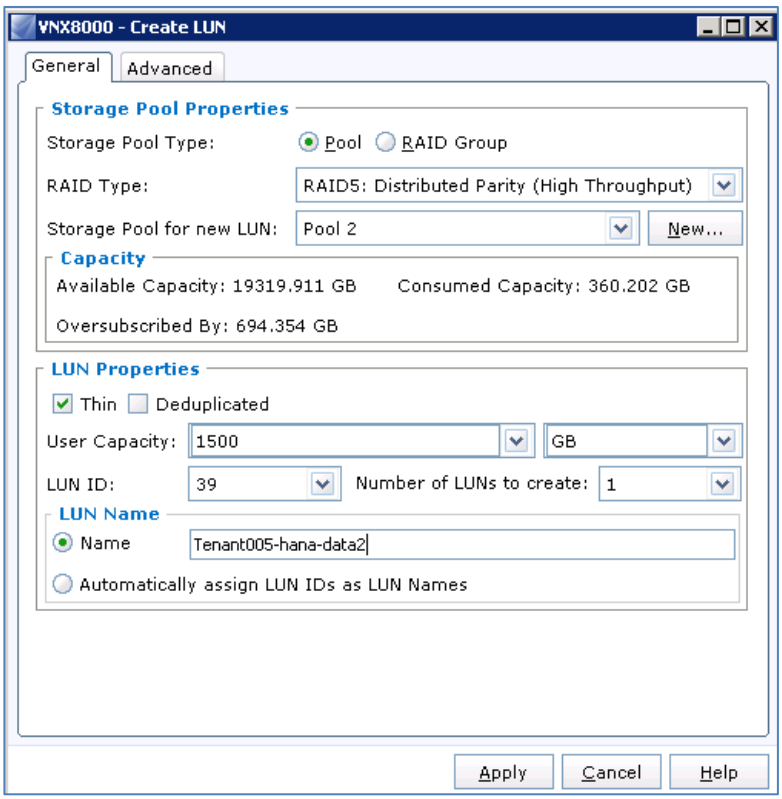

34. Click Apply

35. Click Yes

36. Click OK

37. Enter 1.5 TB as the User Capacity

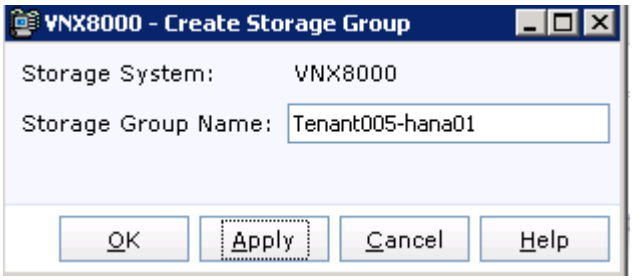
38. Click Name and enter <<var_ucs_t005-hana_sys-name>>-data2




39. Click Apply
40. Click Yes
41. Click OK
42. Click Cancel

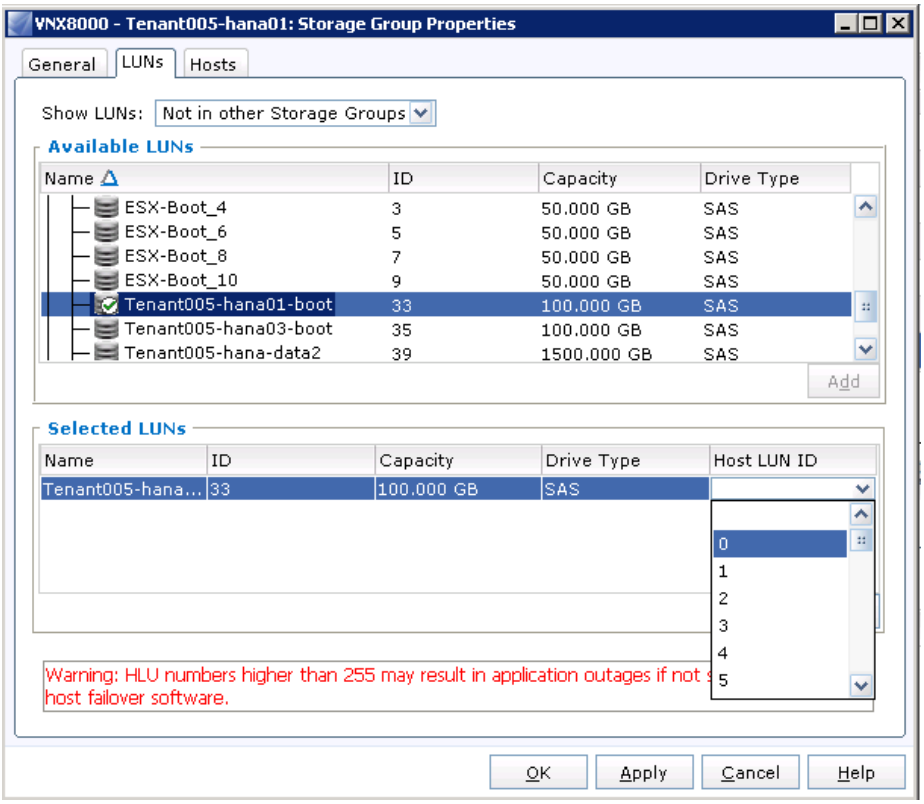
## Create Storage-Group

1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t005_hana1_sp_name>> as the Name
4. Click OK
5. Click Yes




6. Click Yes

7. Under Available LUNs expand SP A and SP B. Locate and select the host's boot LUN <<var_ucs_t005_hana1_name>>-boot and click Add. Ensure the Host LUN ID is 0.

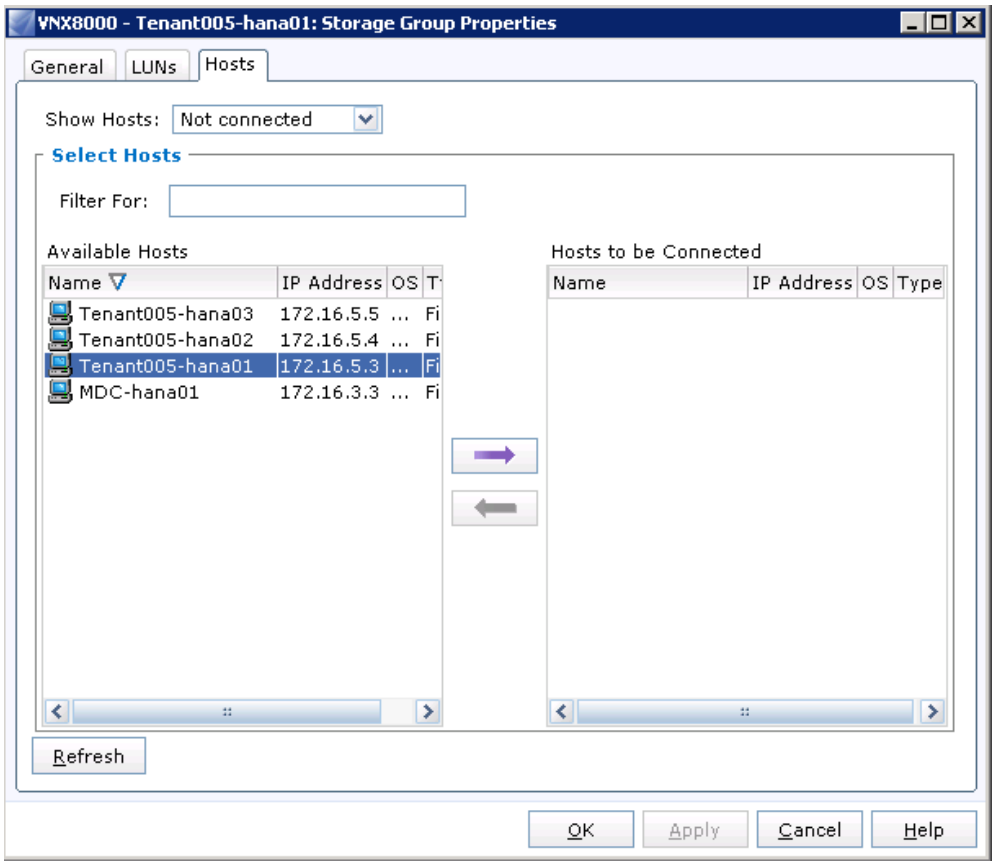



8. Click OK

9. Click Yes

10. Click the Hosts tab

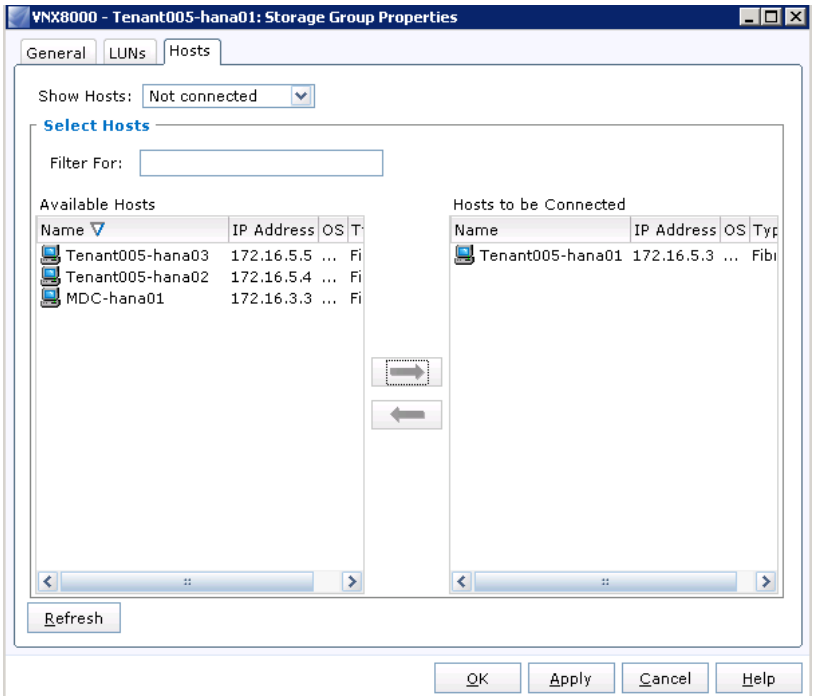
11. Select <<var_ucs_t005_hana1_name>> and click the -> icon



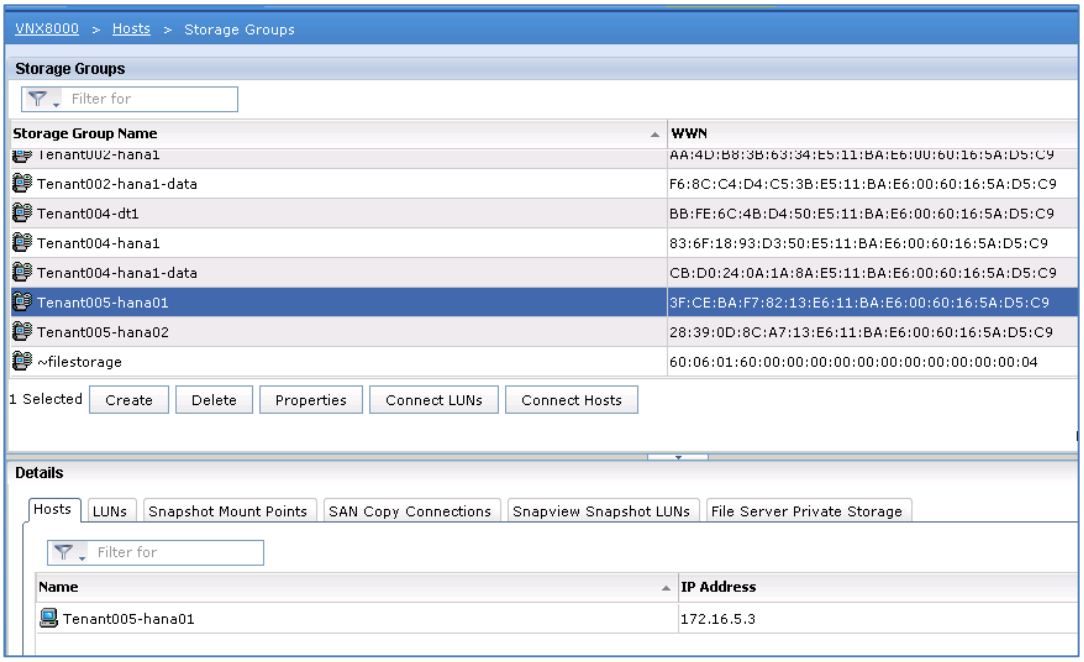

12. Click OK

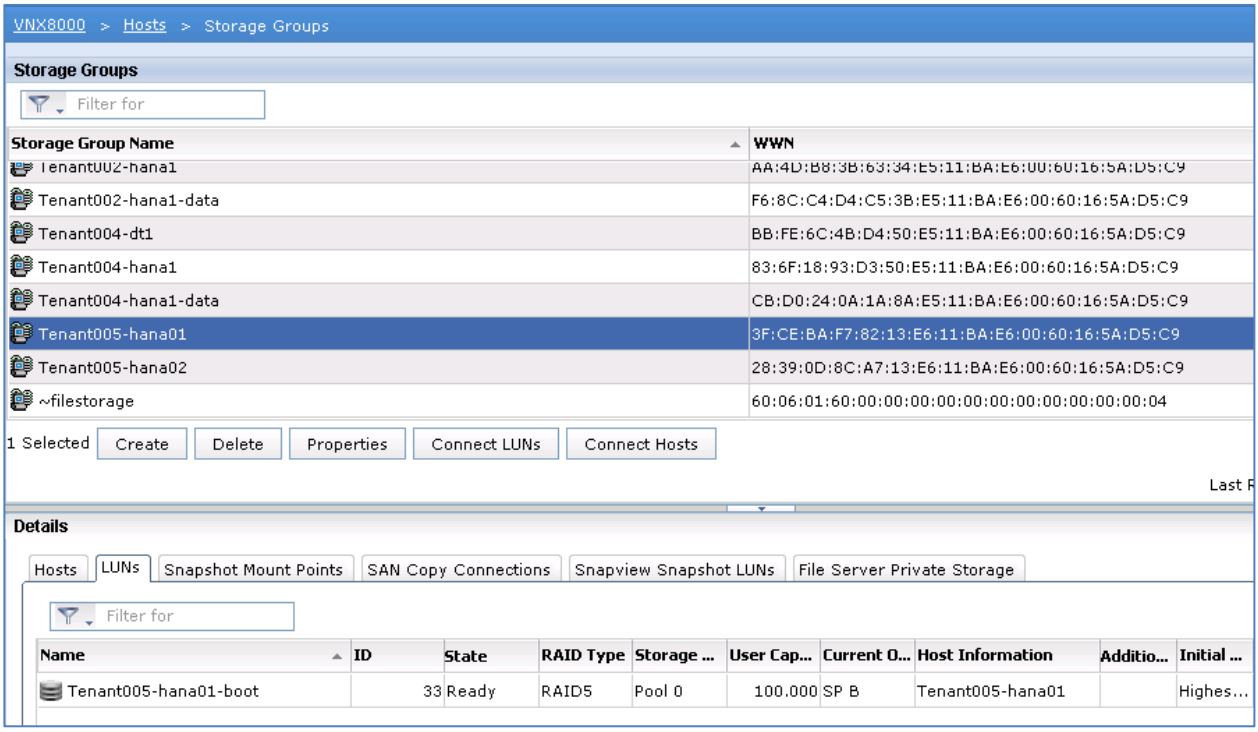
13. Click Yes

14. Click OK

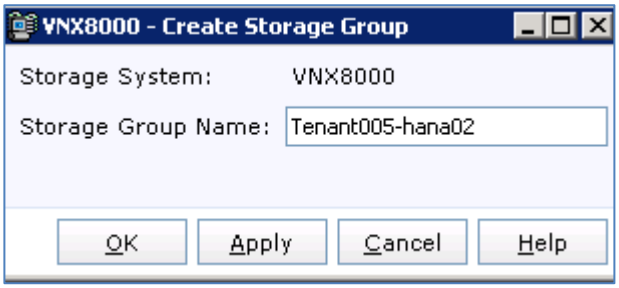



15. The result is shown below.

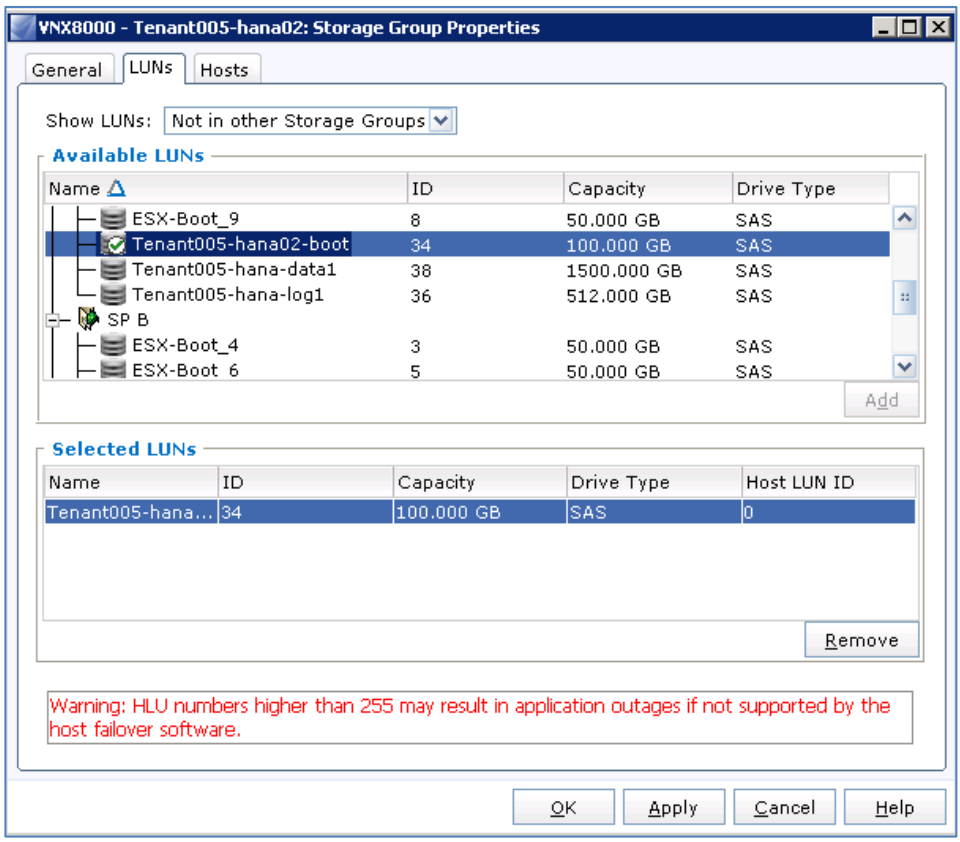





16. Click Create
17. Enter <<var_ucs_t005_hana2_sp_name>> as the Name
18. Click OK
19. Click Yes




20. Click OK
21. Click Yes
22. Click Yes for prompt for add hosts or connect hosts
23. Under Available LUNs expand SP A and SP B. Locate and select the host's boot LUN <<var_ucs_t005_hana2_name>>-boot and Click Add. Select 0 as the Host LUN ID.



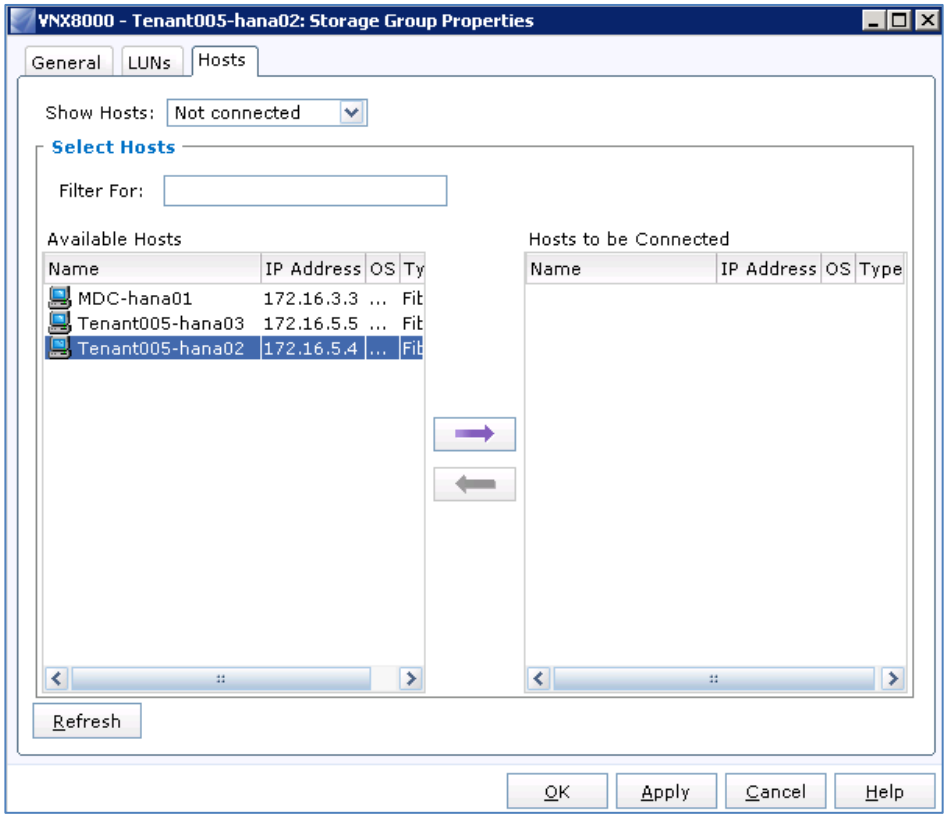

24. Click Apply

25. Click Yes

26. Click OK

27. Click the Hosts tab

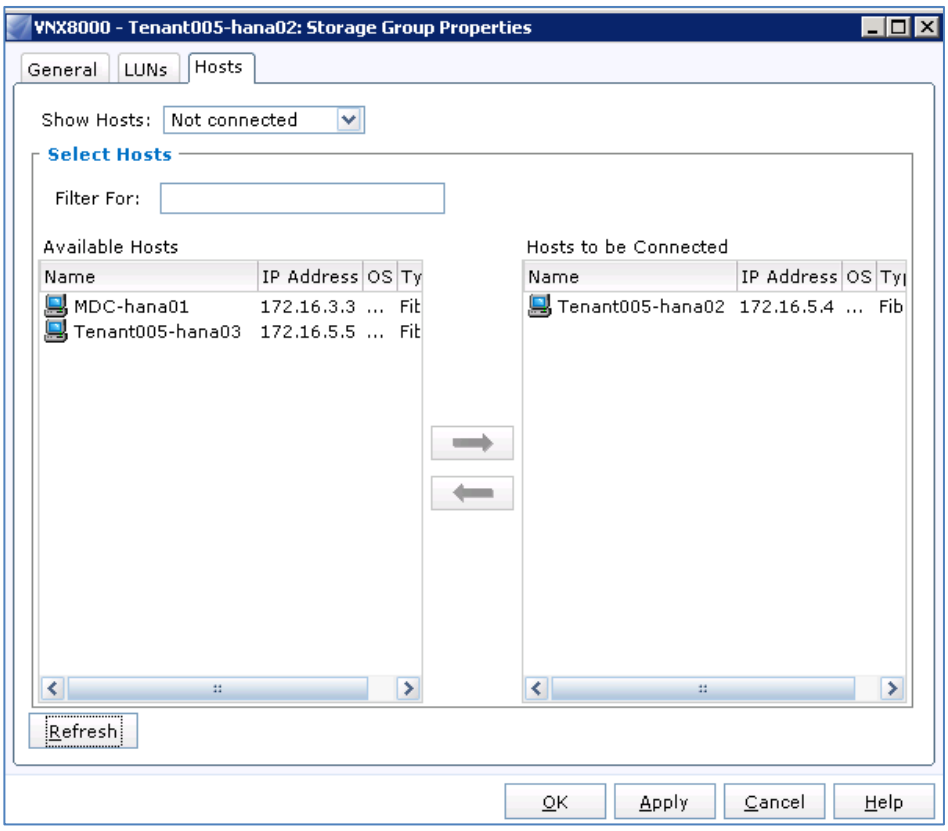
28. Select <<var_ucs_t005_hana2 _name>> and click the -> icon




29. Click OK

30. Click Yes

31. Click OK

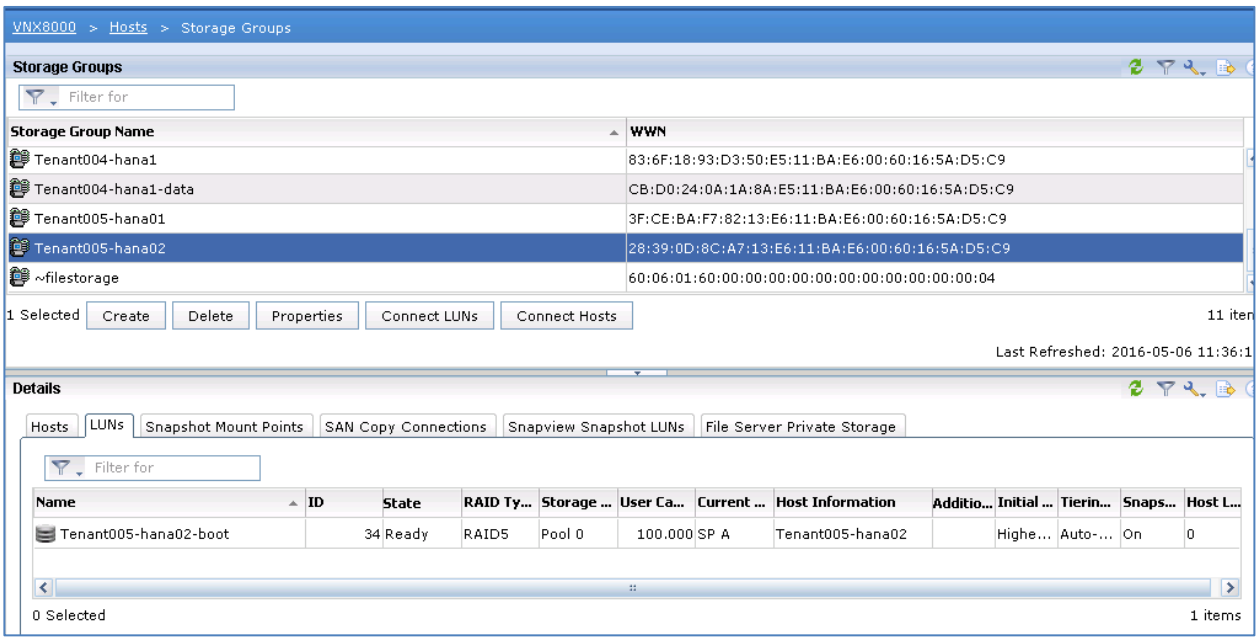



32. Click OK

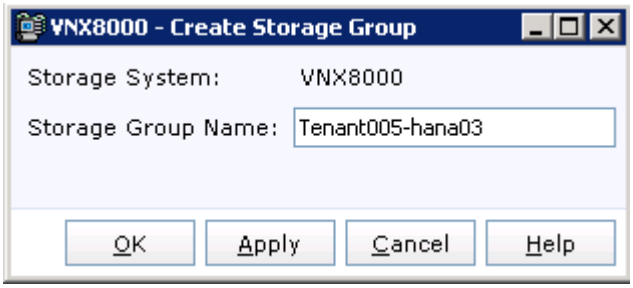
33. Click Yes

34. Click OK

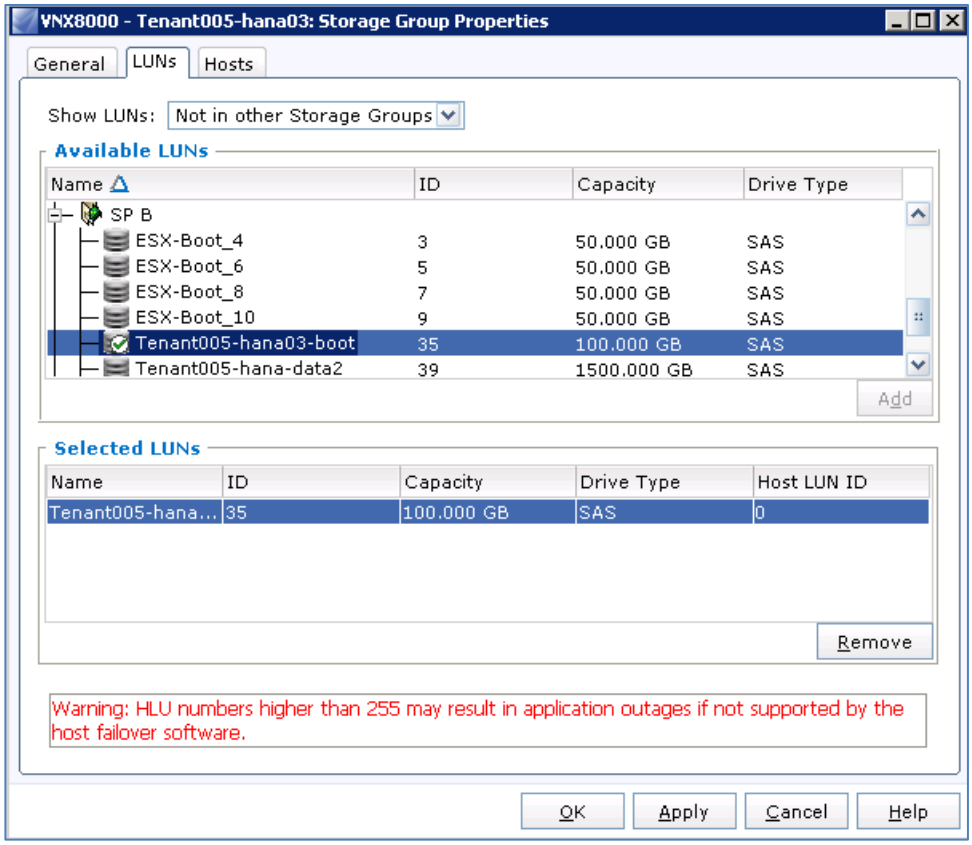
The result is shown below.




35. In the Storage Groups Page, click Create
36. Enter <<var_ucs_t005_hana3_sp_name>> as the Name
37. Click OK
38. Click Yes




39. Click OK
40. Click Yes
41. Click Yes for prompt for add hosts or connect hosts
42. Under Available LUNs expand SP A and SP B. Locate and select the host's boot LUN <<var_ucs_t005_hana3_name>>-boot and Click Add. Select 0 as the Host LUN ID.



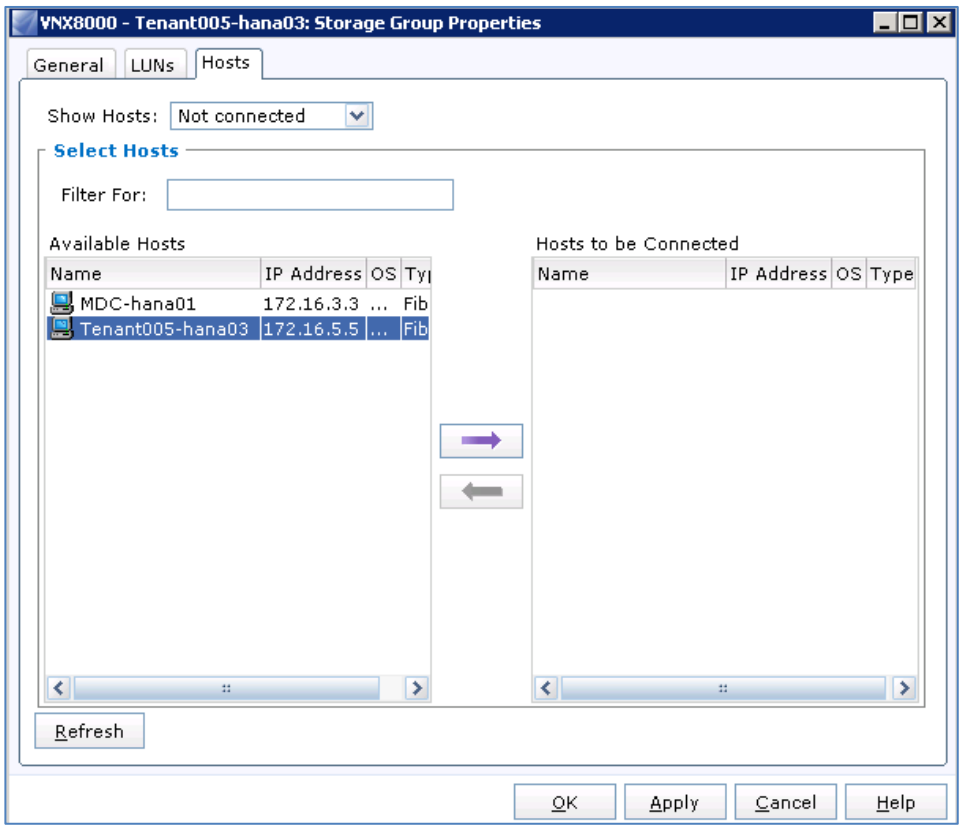

43. Click Apply

44. Click Yes

45. Click OK

46. Click the Hosts tab

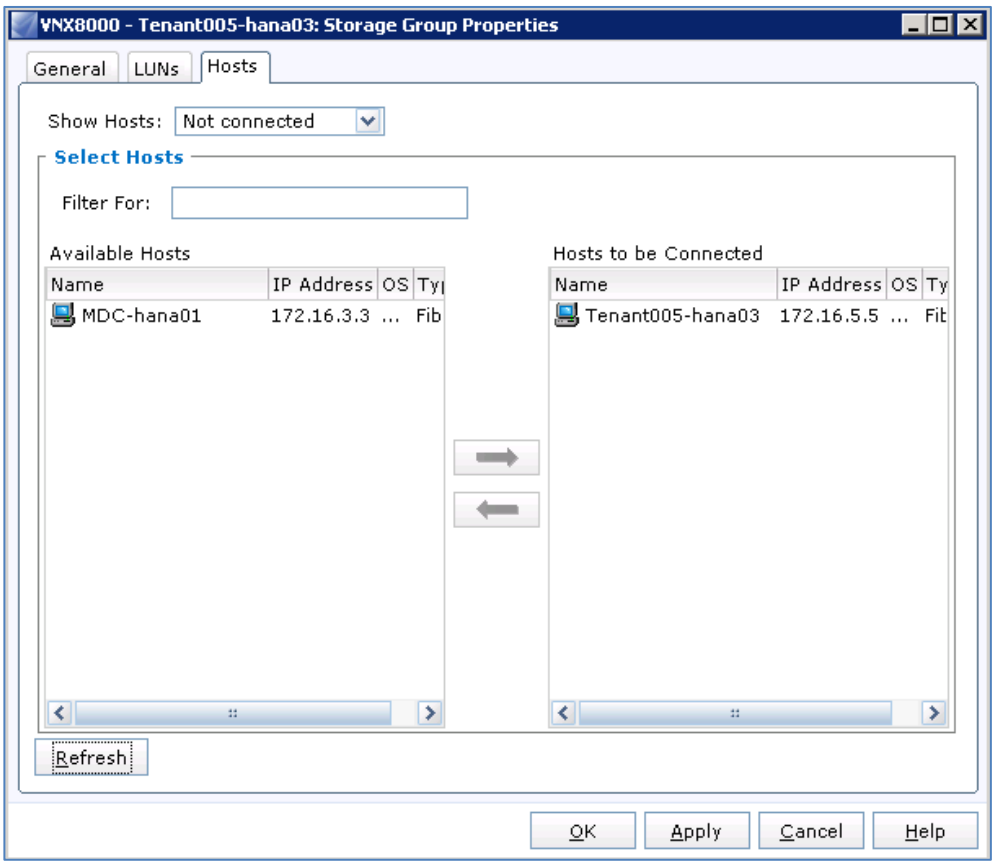
47. Select <<var_ucs_t005_hana3 _name>> and click the -> icon




48. Click OK

49. Click Yes

50. Click OK

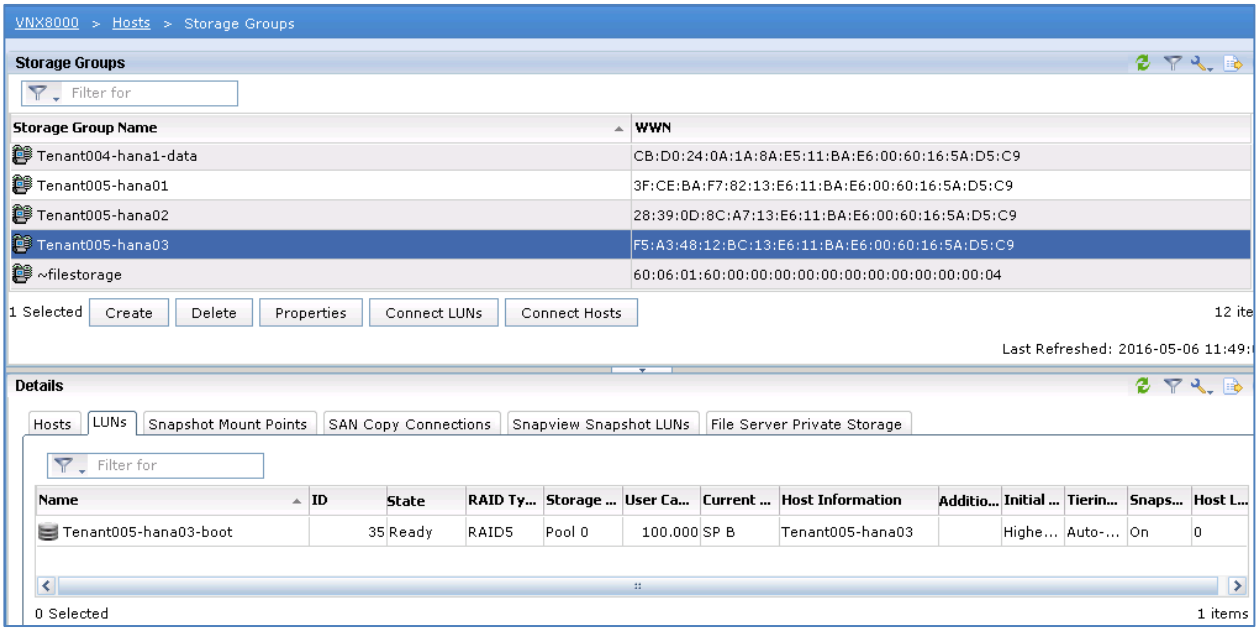



51. Click OK

52. Click Yes

53. Click OK

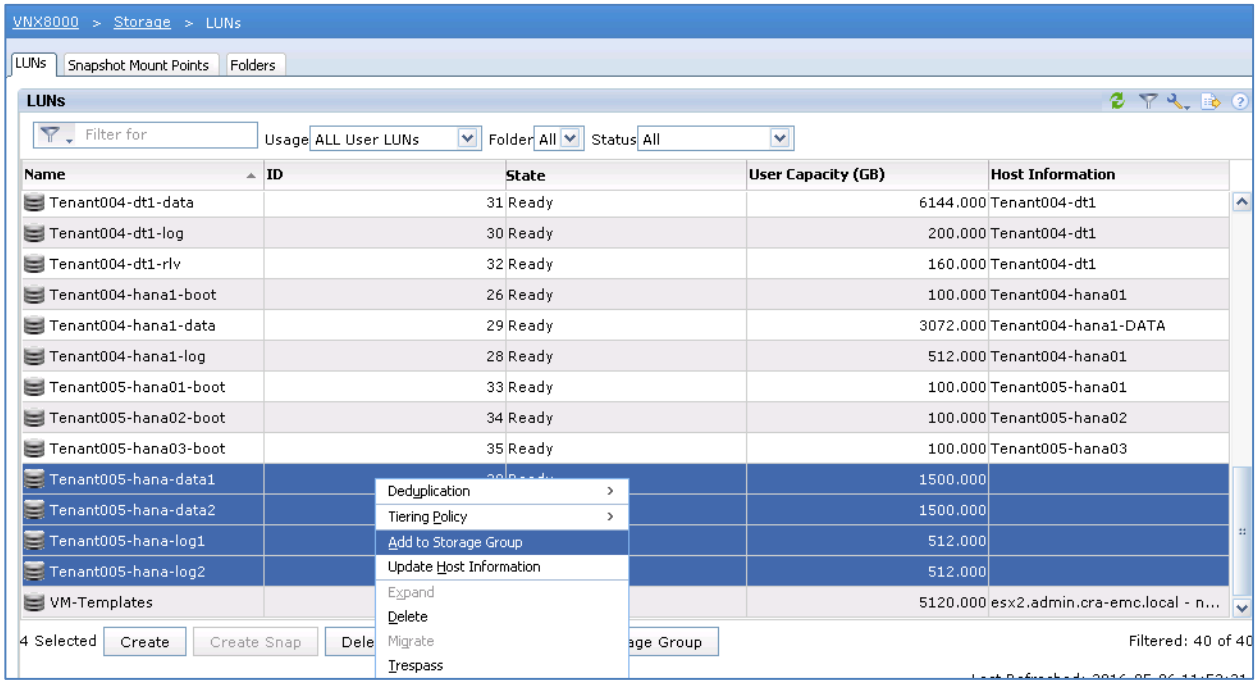
The result is shown below:



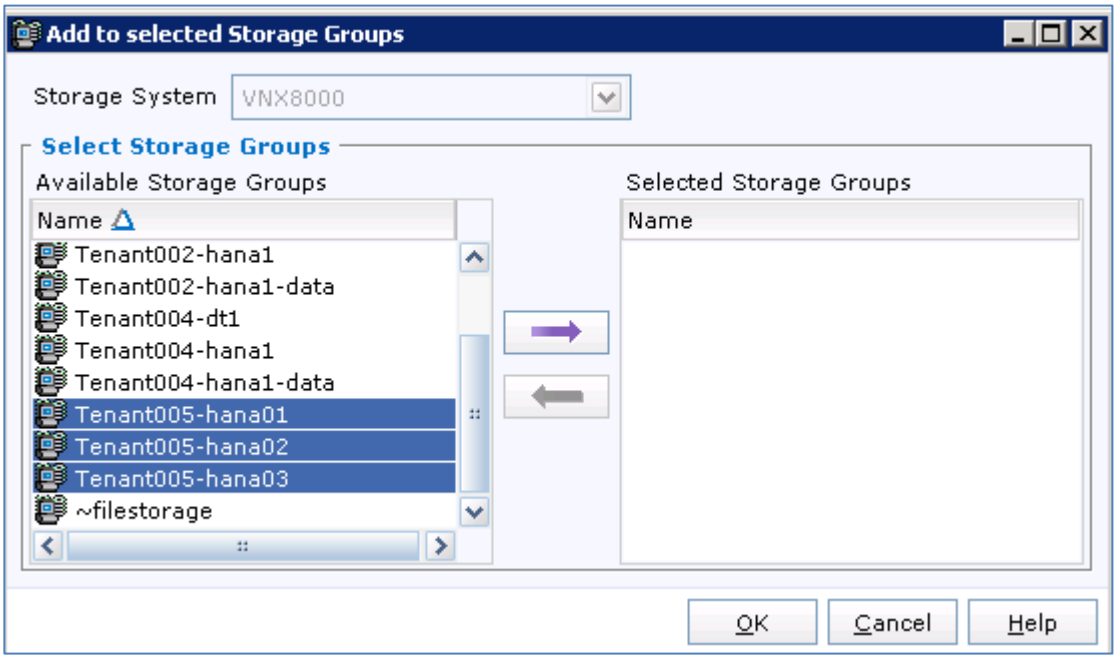

54. Add all of the DATA LUNs and LOG LUNs to all storage groups so that they are visible to all three nodes of cluster.

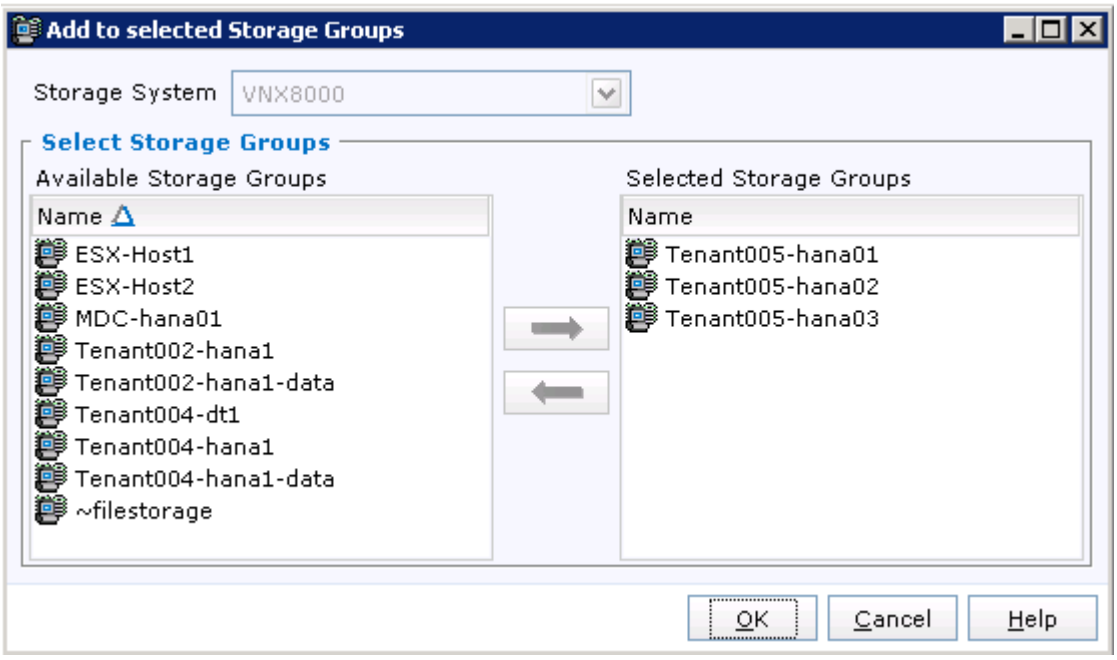
55. Go to StorageSystem -> Storage -> LUNs

56. Select LUNs <<var_ucs_t005-hana_sys-name>>-data1, <<var_ucs_t005-hana_sys-name>>-data2, <<var_ucs_t005-hana_sys-name>>-log1 and <<var_ucs_t005-hana_sys-name>>-log2 and Right click. From the list select “Add to Storage Group”



57. Under “Available Storage Groups” select <<var_ucs_t005_hana1_sp_name>>, <<var_ucs_t005_hana2_sp_name>> and <<var_ucs_t005_hana3_sp_name>> and click -> icon.



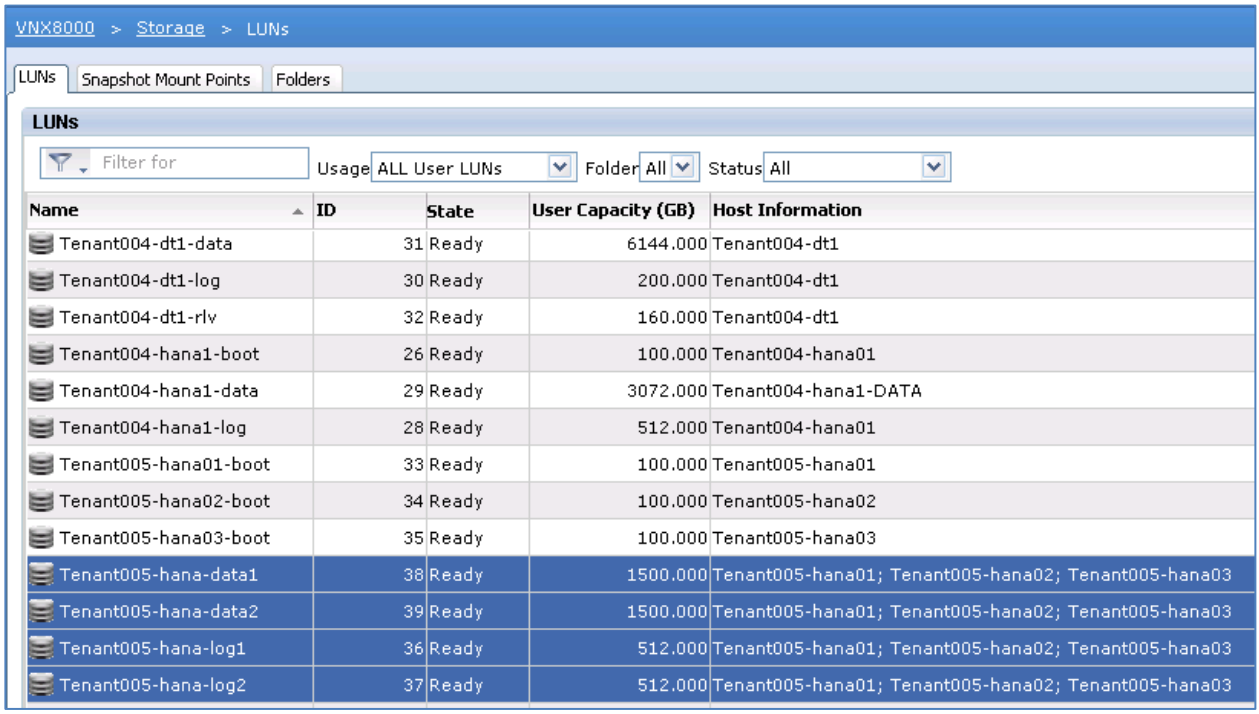

58. Click OK

59. Click Yes

60. Click Yes

61. Click OK.

62. The result is shown below:

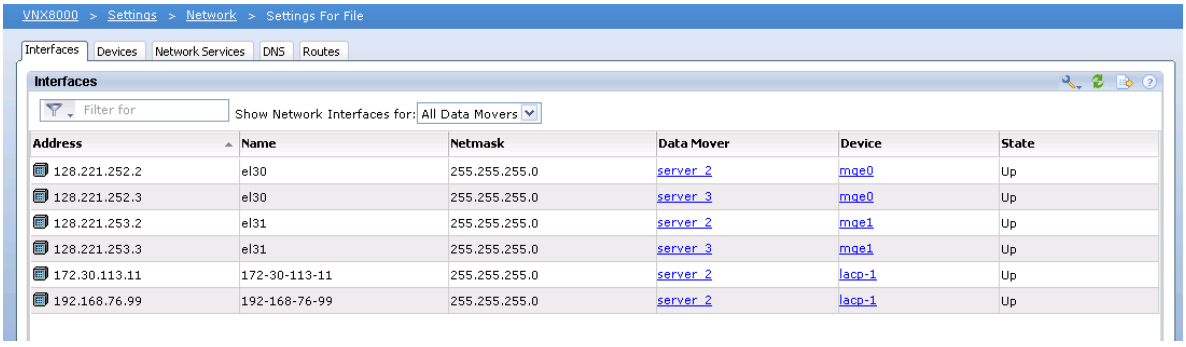



| Name | ID | State | User Capacity (GB) | Host Information |
|---|---|---|---|---|
| Tenant004-dt1-data | 31 | Ready | 6144.000 | Tenant004-dt1 |
| Tenant004-dt1-log | 30 | Ready | 200.000 | Tenant004-dt1 |
| Tenant004-dt1-rlv | 32 | Ready | 160.000 | Tenant004-dt1 |
| Tenant004-hana1-boot | 26 | Ready | 100.000 | Tenant004-hana01 |
| Tenant004-hana1-data | 29 | Ready | 3072.000 | Tenant004-hana1-DATA |
| Tenant004-hana1-log | 28 | Ready | 512.000 | Tenant004-hana01 |
| Tenant005-hana01-boot | 33 | Ready | 100.000 | Tenant005-hana01 |
| Tenant005-hana02-boot | 34 | Ready | 100.000 | Tenant005-hana02 |
| Tenant005-hana03-boot | 35 | Ready | 100.000 | Tenant005-hana03 |
| Tenant005-hana-data1 | 38 | Ready | 1500.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |
| Tenant005-hana-data2 | 39 | Ready | 1500.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |
| Tenant005-hana-log1 | 36 | Ready | 512.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |
| Tenant005-hana-log2 | 37 | Ready | 512.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |

## Configure Network Interface

1. In EMC Unisphere GUI, click Settings > Network > Settings for File

2. In the Interface tab, click Create




| Address | Name | 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 |
| 172.30.113.11 | 172-30-113-11 | 255.255.255.0 | server_2 | lacp-1 | Up |
| 192.168.76.99 | 192-168-76-99 | 255.255.255.0 | server_2 | lacp-1 | Up |

3. Enter <<var_vnx_tenant005_nfs_storage_ip>> as the Address

4. Enter <<var_vnx_tenant005_if_name>> as the Name

5. Enter <<var_tenant005_nfs_mask>> as the Netmask

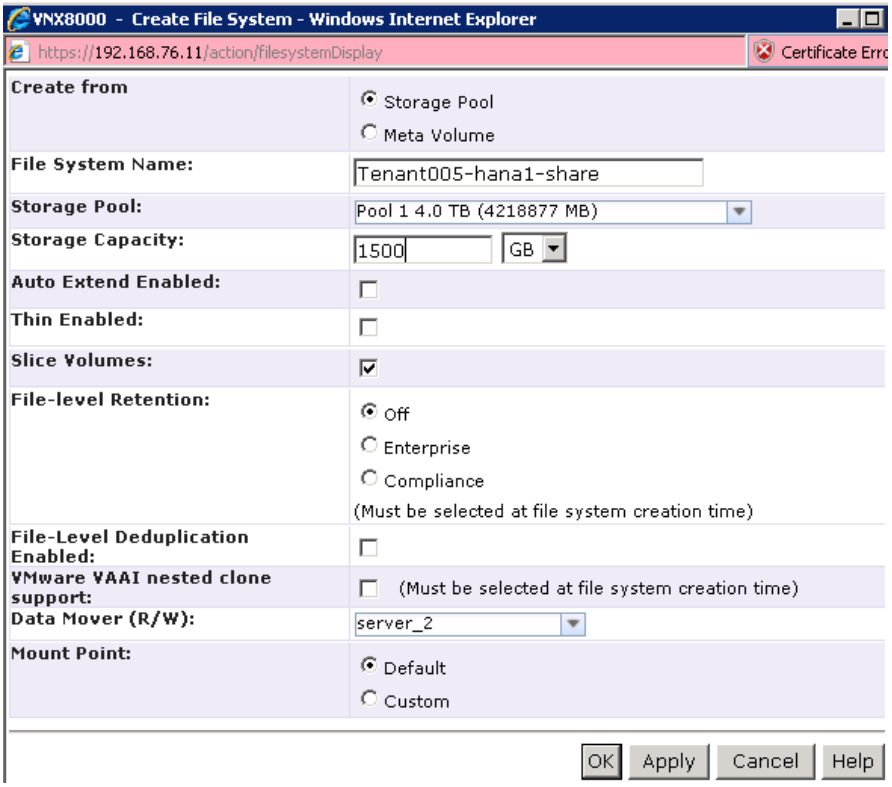
6. Enter 9000 as the MTU

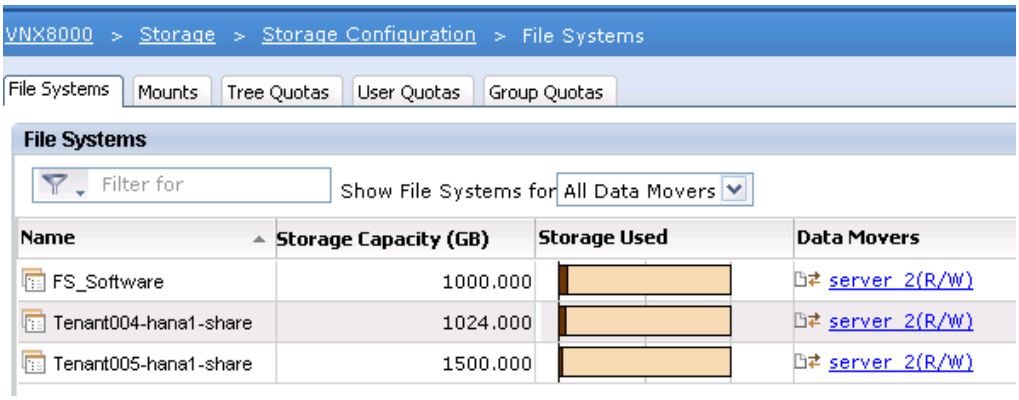
7. Enter <<var_t005_nfs_vlan_id>> as the VLAN ID
8. Click OK

### Configure Filesystem and NFS Share

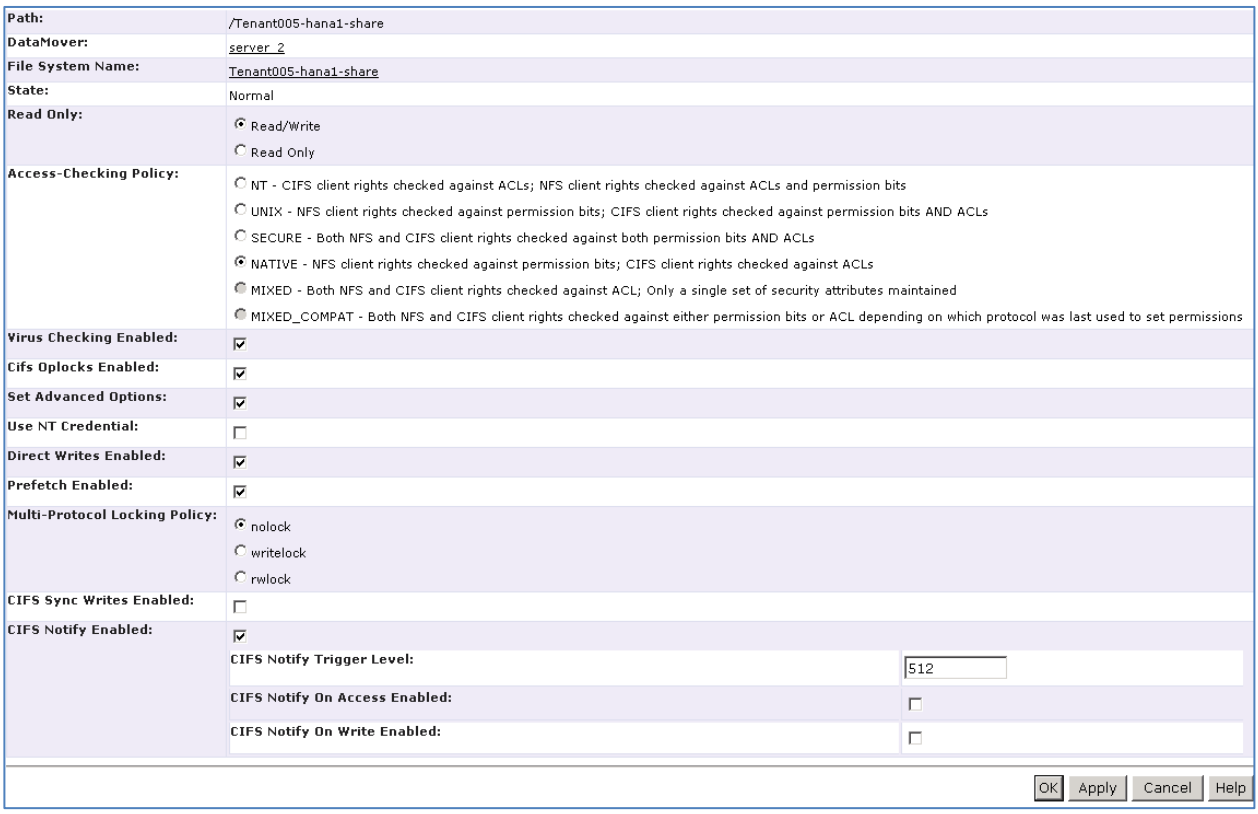
To create the Filesystem and NFS share for /hana/shared on the VNX storage, complete the following steps:

1. In EMC Unisphere GUI, Click Storage > Storage Configuration > File Systems
2. In the File Systems tab, Click Create
3. Enter <<var_vnx_t004_fs_name>> as the File System Name
4. Enter 1.5 TB as the Storage Capacity
5. Click OK



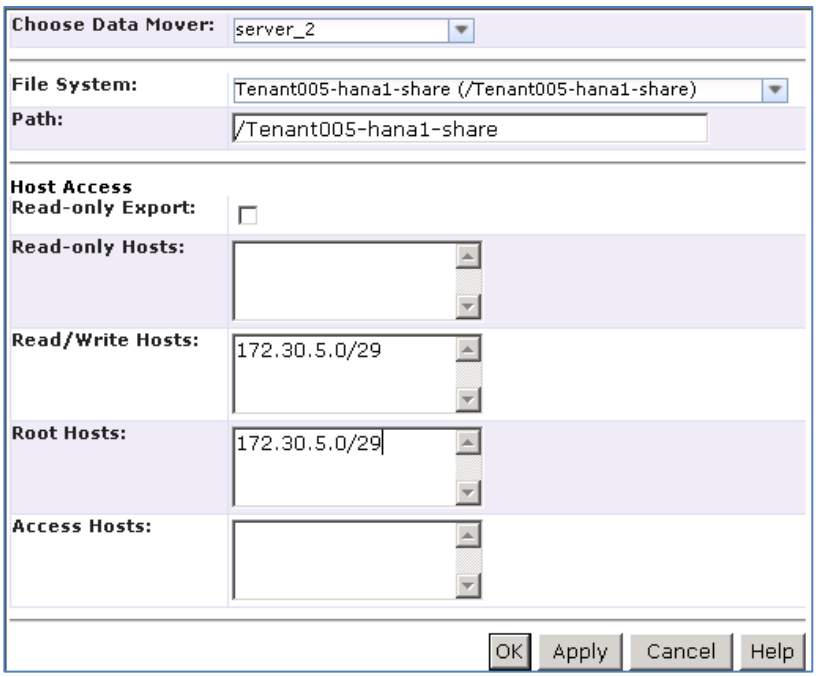



6. Click the Mounts tab
7. Select the path <<var_vnx_t005_fs_name>>
8. Click Properties
9. From the mount properties. Make sure Read/Write is selected and Native Access policy is selected.
10. Select the Set Advanced Options check box
11. Check the Direct Writes Enabled check box
12. Click OK

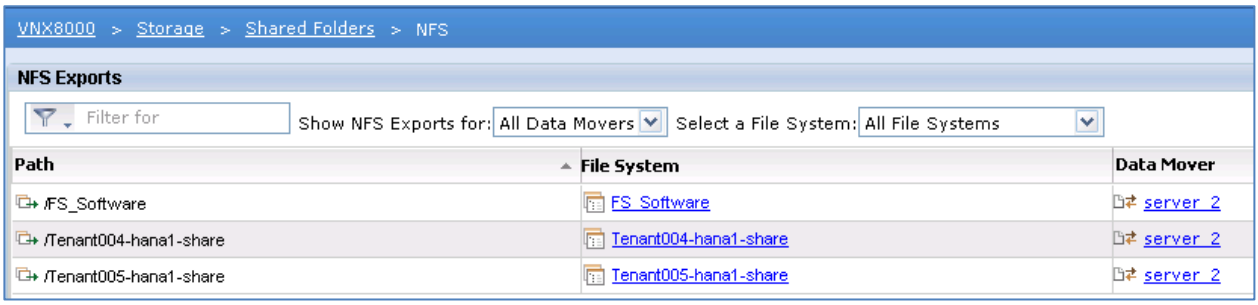



## Create NFS Share

1. Select Storage > Shared Folders > NFS
2. Click Create.
3. Select server_2 from the drop-down menu
4. Select <<var_vnx_t005_fs_name>> from drop-down menu
5. Ensure /<<var_vnx_t005_share_name>> is the selected Path
6. Enter <<var_vnx_t005_network>> with the related netmask to Read/write hosts and Root hosts
7. Click OK




8. The result looks like this




The storage configuration for this SAP HANA use case is now done and the Operating system can be installed.

## Install the Operating System

The following steps show the configuration of the Operating systems on the SAP HANA node and the SAP HANA DT node in addition to the basic OS installation.

### SAP HANA Node

1. Follow the steps documented in the Section “Operating System Installation and Configuration” to install the operating system

2. Use a SSH client to login to the newly installed system as root

3. Configure the network interfaces

4. Add or change the entries in the file(s) as shown. Do not change the UUID entry

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1

ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=172.30.113.53
PREFIX=24
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth1"

vi /etc/sysconfig/network-scripts/ifcfg-eth2

UUID=2949da7d-0782-4238-ba4a-7a88e74b6ab7
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=192.168.5.3
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth2"

vi /etc/sysconfig/network-scripts/ifcfg-eth3

ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=9000
IPADDR=172.30.5.3
PREFIX=29
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth3"
```

Perform this network configuration step for the other nodes in the scale-out system.

5. Restart the network stack

```
# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down interface eth2:                              [  OK  ]
Shutting down interface eth3:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Determining if ip address 172.16.5.3 is already in
use for device eth0...
                                                           [  OK  ]
```

```
Bringing up interface eth1:  Determining if ip address 172.30.113.53 is already
in use for device eth1...
                                                           [  OK  ]
Bringing up interface eth2:  Determining if ip address 192.168.5.3 is already in
use for device eth2...
                                                           [  OK  ]
Bringing up interface eth3:  Determining if ip address 172.30.5.3
 is already in use for device eth3...
                                                           [  OK  ]
```



Make sure the IPs are assigned correctly to the respective Ethernet interfaces in other nodes of the scale-out system.

6. List the available multi-pathed disks

```
# ls /dev/mapper/36*

/dev/mapper/3600601601c603500114592fe8113e611
/dev/mapper/3600601601c6035004c30a1de8013e611
/dev/mapper/3600601601c6035009171d2408213e611
/dev/mapper/3600601601c603500ac513a818013e611
/dev/mapper/3600601601c603500d96136b87d13e611
/dev/mapper/3600601601c603500d96136b87d13e611_part1
/dev/mapper/3600601601c603500d96136b87d13e611_part2
```

7. Check with df or pvdisplay which mapper device is used for the operating system. For all unused devices run fdisk –l <device> to verify the capacity and ascertain which are DATA and LOG LUNs.

```
# fdisk -l /dev/mapper/3600601601c603500114592fe8113e611

Disk /dev/mapper/3600601601c603500114592fe8113e611: 1610.6 GB, 1610612736000
bytes
255 heads, 63 sectors/track, 195812 cylinders, total 3145728000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/3600601601c603500114592fe8113e611 doesn't contain a valid
partition table

# fdisk -l /dev/mapper/3600601601c6035004c30a1de8013e611

Disk /dev/mapper/3600601601c6035004c30a1de8013e611: 549.8 GB, 549755813888 bytes
255 heads, 63 sectors/track, 66837 cylinders, total 1073741824 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/3600601601c6035004c30a1de8013e611 doesn't contain a valid
partition table
```

```
# fdisk -l /dev/mapper/3600601601c6035009171d2408213e611

Disk /dev/mapper/3600601601c6035009171d2408213e611: 1610.6 GB, 1610612736000
bytes
255 heads, 63 sectors/track, 195812 cylinders, total 3145728000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/3600601601c6035009171d2408213e611 doesn't contain a valid
partition table

# fdisk -l /dev/mapper/3600601601c603500ac513a818013e611

Disk /dev/mapper/3600601601c603500ac513a818013e611: 549.8 GB, 549755813888 bytes
255 heads, 63 sectors/track, 66837 cylinders, total 1073741824 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/3600601601c603500ac513a818013e611 doesn't contain a valid
partition table-l
```

8. Create the file systems for SAP HANA

Run this makefilesystem command with option to format the non-OS devices, i.e. DATA and LOG LUN devices. It is enough to perform this step from any one node.

```
# mkfs.xfs -f /dev/mapper/3600601601c603500114592fe8113e611
meta-data=/dev/mapper/3600601601c603500114592fe8113e611 isize=256    agcount=4,
agsize=98304000 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=393216000, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=192000, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0


# mkfs.xfs -f /dev/mapper/3600601601c6035004c30a1de8013e611
meta-data=/dev/mapper/3600601601c6035004c30a1de8013e611 isize=256    agcount=4,
agsize=33554432 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=134217728, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=65536, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

```
# mkfs.xfs -f /dev/mapper/3600601601c6035009171d2408213e611
meta-data=/dev/mapper/3600601601c6035009171d2408213e611 isize=256    agcount=4,
agsize=98304000 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=393216000, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=192000, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0

# mkfs.xfs -f /dev/mapper/3600601601c603500ac513a818013e611
meta-data=/dev/mapper/3600601601c603500ac513a818013e611 isize=256    agcount=4,
agsize=33554432 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=134217728, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=65536, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

9. Mount /hana/shared

The /hana/shared file system is a shared filesystem and must be mounted on all nodes of the SAP HANA scale-out system. For this purpose, the file system /Tenant005-hana1-share NFS share was created on the VNX storage.

10. Add the following line at the end of /etc/fstab file

```
172.30.5.6:/Tenant005-hana1-share   /hana/shared      nfs   defaults    0 0
```

11. Create the mount point /hana/shared

```
mkdir –p /hana/shared
```

12. Mount the File System

```
mount /hana/shared

chgrp sapsys /hana/shared

chmod 775 /hana/shared
```

13. Enter the required information into the hosts file

14. Update the /etc/hosts file of all nodes with the IP addresses of different networks assigned to the hosts' interfaces.

```
vi /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
# Access Network
#
172.16.5.3      t005-hana01.cra-emc.local  t005-hana01
172.16.5.4      t005-hana02.cra-emc.local  t005-hana02
172.16.5.5      t005-hana03.cra-emc.local  t005-hana03
#
# Global NFS
#
172.30.113.53   t005-hana01-nfs
172.30.113.54   t005-hana02-nfs
172.30.113.55   t005-hana03-nfs
#
# Storage Network
#
172.30.5.3      t005-hana01-st
172.30.5.4      t005-hana02-st
172.30.5.5      t005-hana03-st
#
# Internal Network
#
192.168.5.3     t005-hana01-int
192.168.5.4     t005-hana02-int
192.168.5.5     t005-hana02-int
```

15. Exchange the ssh key between all hosts for the SAP HANA system. This is required for remote login without a password.

16. Generate the rsa key and then copy it to all nodes including itself. Repeat these steps for all nodes.

```
t005-hana01:~ # ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
7f:61:41:af:b4:77:2d:ad:24:16:32:2b:bf:4b:51:a5 [MD5] root@t005-hana01
The key's randomart image is:
+--[ RSA 2048]----+
|             . .  |
|            . +   |
|           o E .  |
|            * = ..|
|         S o B + +|
|          + + = + |
|           + . .  |
|          . o     |
|           o.     |
+--[MD5]----------+
```

```
t005-hana01:~ # ssh-copy-id -i /root/.ssh/id_rsa t005-hana01
The authenticity of host 't005-hana01 (172.16.5.3)' can't be established.
ECDSA key fingerprint is a:19:7c:d6:ab:58:db:7d:71:ae:4c:94:c0:d0:55:d1 [MD5].
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 't005-hana01'"
and check to make sure that only the key(s) you wanted were added.

t005-hana01:~ # ssh-copy-id -i /root/.ssh/id_rsa t005-hana02
The authenticity of host 't005-hana02 (172.16.5.4)' can't be established.
ECDSA key fingerprint is 0:07:d6:c4:58:15:27:df:59:36:21:31:16:84:b1:0c [MD5].
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 't005-hana02'"
and check to make sure that only the key(s) you wanted were added.

t005-hana01:~ # ssh-copy-id -i /root/.ssh/id_rsa t005-hana03
The authenticity of host 't005-hana03 (172.16.5.5)' can't be established.
ECDSA key fingerprint is 0:07:d6:c4:58:15:27:df:59:36:21:31:16:84:b1:0c [MD5].
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 't005-hana03'"
and check to make sure that only the key(s) you wanted were added.
```

17. Reboot the system:

```
Reboot
```

### SAP HANA Nodes access to DATA and LOG LUNs

The SAP HANA Storage Connector API for Block is responsible for mounting and I/O fencing of the HANA persistent layer. It must be used in a HANA scale-out installation where the persistence resides on block-attached storage devices.

The API will be implemented by enabling the appropriate entry in the HANA global.ini file. This file resides in the /hana/shared/>SID>/global/hdb/custom/config directory.

The figure below shows an example of a global.ini file for this 2+1 nodes scale out system.

The values for DATA and LOG partitions are its scsi-id which can be derived by doing a check on `ls /dev/mapper/36*` and a look at their capacity with `fdisk –l` on each of the device helps categorizing DATA and LOG partitions.

```
[communication]
listeninterface = .global

[persistence]
use_mountpoints = yes
basepath_datavolumes = /hana/data/ <<var_t005_hana_sid>>
basepath_logvolumes = /hana/log/ <<var_t005_hana_sid>>
basepath_shared=yes

[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prType = 5
partition_1_data__wwid = 3600601601c603500114592fe8113e611
partition_1_log__wwid  = 3600601601c6035004c30a1de8013e611
partition_2_data__wwid = 3600601601c6035009171d2408213e611
partition_2_log__wwid  = 3600601601c603500ac513a818013e611
```

The EMC based Scale-Out solution employs Linux Native Multipathing (DM-MPIO) on the HANA nodes to improve performance and provide high availability for the access paths to the storage devices.

DM-MPIO requires a configuration file /etc/multipath.conf

The configuration shown below is specific to the current example with VNX backend array and Active-Passive PNR mode1 method of storage Host registration.

```
defaults {
user_friendly_names     no
}
devices {
        device {
               vendor                  "DGC"
               product                 ".*"
               product_blacklist       "LUNZ"
               features                "0"
               hardware_handler        "1 emc"
               path_selector           "round-robin 0"
               path_grouping_policy    group_by_prio
               failback                immediate
               rr_weight               uniform
               no_path_retry           5
               rr_min_io               1000
               path_checker            emc_clariion
               prio                    emc
               flush_on_last_del       yes
               fast_io_fail_tmo        off
               dev_loss_tmo            120
       }
}
```

## Enabling Data Traffic on vHBA3 and vHBA4 (SAP HANA Node)

Now that the Cisco FNIC driver is loaded in the operating system, vHBA3 and vHBA4 are also logged into the MDS switches. To enable them to access the storage, we now create zones with the pwwn of vHBA3 and vHBA4 here which we will, going forward, use exclusively for DATA traffic, done with an objective that for best performance of a SAP HANA system it is recommended to move the paths for the data volume from the single storage path zoning into the multi paths zoning.

### Cisco MDS 9148 A

1. On MDS 9148 A enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones for each of the scale-out system nodes exclusively for DATA traffic with the following commands:

```
zone clone zone_temp <<var_zone_t005-hana01-data>> vsan 10
zone name <<var_zone_t005-hana01-data>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:14
   exit
zone clone zone_temp <<var_zone_t005-hana02-data>> vsan 10
zone name <<var_zone_t005-hana01-data>> vsan 10
```

```
   member pwwn 20:00:00:25:b5:a0:00:16
   exit
zone clone zone_temp <<var_zone_t005-hana03-data>> vsan 10
zone name <<var_zone_t005-hana01-data>> vsan 10
   member pwwn 20:00:00:25:b5:a0:00:18
   exit

zoneset name CRA-EMC-A vsan 10
member <<var_zone_t005-hana01-data>>
member <<var_zone_t005-hana02-data>>
member <<var_zone_t005-hana03-data>>
exit
zoneset activate name CRA-EMC-A vsan 10
```

3. Verify the configuration with the following commands

```
CRA-EMC-A# show zone
zone name zone_temp vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68

zone name zone_temp_1path vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68

…
zone name zone_t005-hana01 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
```

```
  pwwn 20:00:00:25:b5:a0:00:15

zone name zone_t005-hana02 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:17

zone name zone_t005-hana03 vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:19
…
zone name zone_t005-hana01-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:14

zone name zone_t005-hana02-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:16
```

```
zone name zone_t005-hana03-data vsan 10
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:68
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:68
  pwwn 20:00:00:25:b5:a0:00:18

CRA-EMC-A#
CRA-EMC-A# show zoneset brief
zoneset name CRA-EMC-A vsan 10
  zone zone_esx-host1
  zone zone_esx-host2
  ...
  zone zone_esx-host10
  zone zone_t004-hana01
  zone zone_t004-hana01-data
  zone zone_t005-hana01
  zone zone_t005-hana02
  zone zone_t005-hana03
  zone zone_t005-hana01-data
  zone zone_t005-hana02-data
  zone zone_t005-hana03-data
CRA-EMC-A#
```

4. Save the running configuration as startup configuration

```
Copy run start
```

## Cisco MDS 9148 B

1. On MDS 9148 B enter configuration mode:

```
config terminal
```

2. Use the zone template to create the required zones with the following commands:

```
zone clone zone_temp <<var_zone_t004-hana1-data>> vsan 20
zone name <<var_zone_t005-hana01-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:14
   exit
zone name <<var_zone_t005-hana02-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:16
   exit
zone name <<var_zone_t005-hana03-data>> vsan 20
   member pwwn 20:00:00:25:b5:b0:00:18
   exit
zoneset name CRA-EMC-B vsan 20
member <<var_zone_t005-hana01-data>>
member <<var_zone_t005-hana02-data>>
member <<var_zone_t005-hana03-data>>
exit
zoneset activate name CRA-EMC-B vsan 20
```

3. Use the following commands to verify the configuration:

```
CRA-EMC-B# show zone
zone name zone_temp vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
```

```
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
zone name zone_temp_1path vsan 10
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
…
zone name zone_t005-hana01 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:15
zone name zone_t005-hana02 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:17
zone name zone_t005-hana03 vsan 20
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:19
…
zone name zone_t005-hana01-data vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:14
zone name zone_t005-hana02-data vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
```

```
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:16
zone name zone_t005-hana03-data vsan 20
  interface fc1/25 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/26 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/27 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/28 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/29 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/30 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/31 swwn 20:00:00:05:9b:2c:1a:78
  interface fc1/32 swwn 20:00:00:05:9b:2c:1a:78
  pwwn 20:00:00:25:b5:b0:00:18

CRA-EMC-B#
CRA-EMC-B# show zoneset brief
zoneset name CRA-EMC-B vsan 20
  zone zone_esx-host1
  zone zone_esx-host2
  ...
  zone zone_esx-host10
  zone zone_t004-hana01
  zone zone_t004-hana01-data
  zone zone_t005-hana01
  zone zone_t005-hana02
  zone zone_t005-hana03
  zone zone_t005-hana01-data
  zone zone_t005-hana02-data
  zone zone_t005-hana03-data
CRA-EMC-B#
```

4. Save the running configuration as startup configuration:

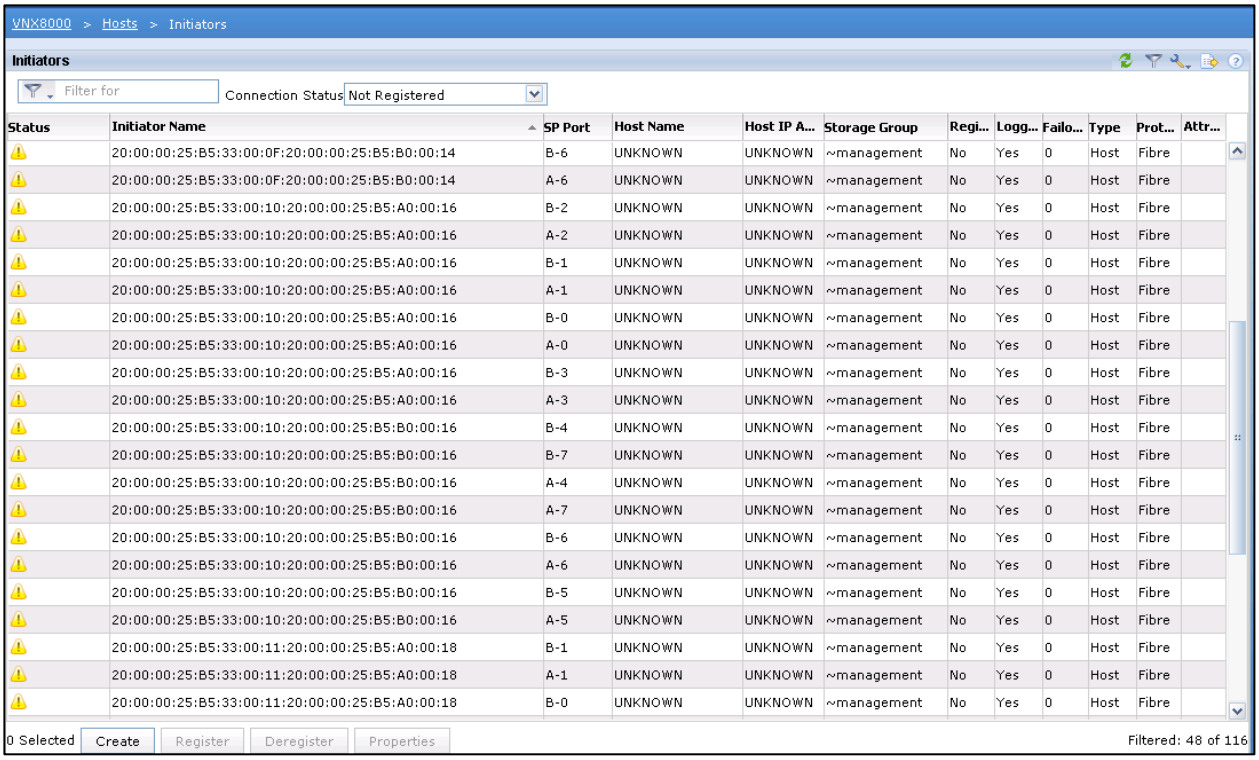
```
copy run start
```

## Configure EMC VNX

### Register Host

To register a host, complete the following steps:

1. Log in to the EMC Unisphere Manager and navigate to the <<var_vnx1_name>> > Hosts > Initiators

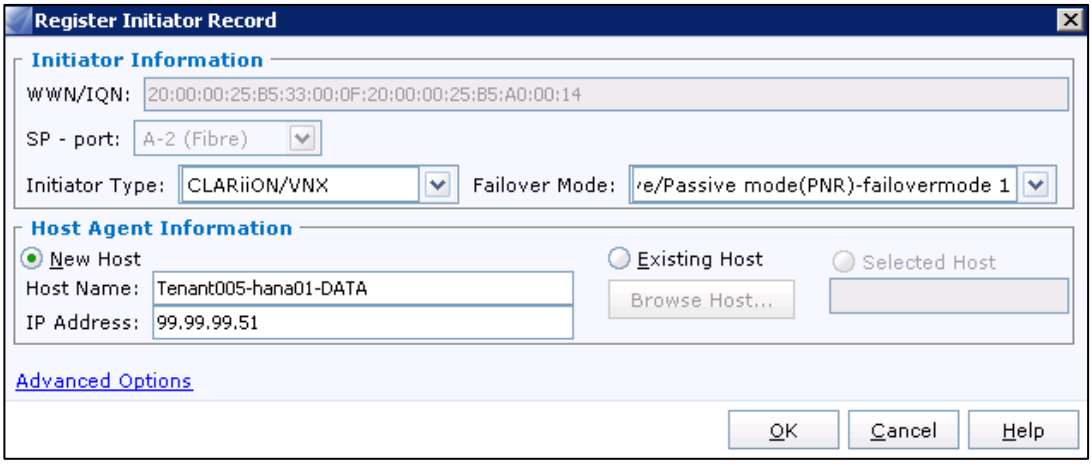




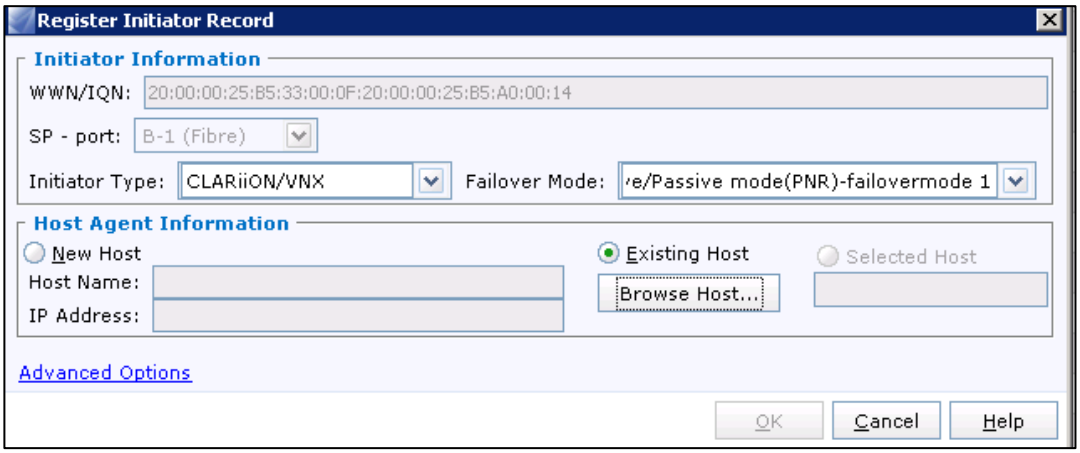

Now there are 48 new initiators logging into the array – 16 paths, 8 each for vHB3and vHBA4 pwwns since 8 ports are used in the zone for each node.

2. Select one of the unregistered entries for the host Tenant005-hana01, click Register
3. Select CLARiiON/VNX as the Initiator Type
4. Select Active/Passive PNR - failovermode 1 as the Failover Mode
5. Enter <<var_ucs_t005_hana1_sp_name>>-DATA as the Host Name (indicates the relationship to the Service Profile)
6. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
7. Click OK

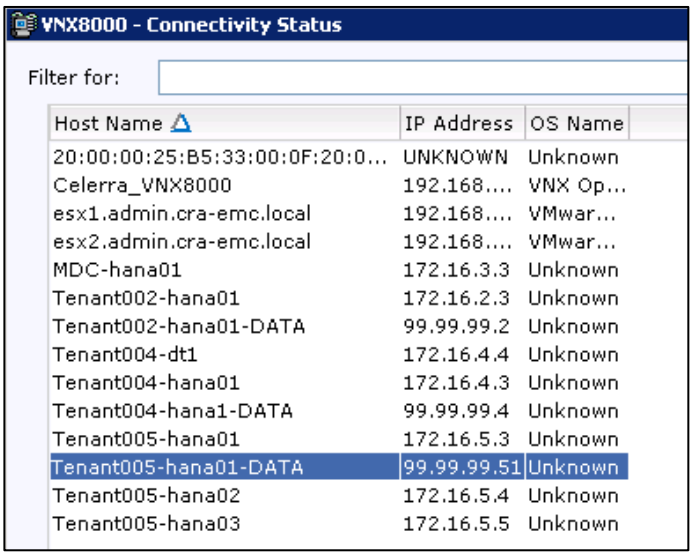
8. Click Yes
9. Click OK
10. Click OK




11. Select the next un-registered Entry for this host <<var_ucs_t005_hana1_sp_name>>, click Register
12. Select CLARiiON/VNX as the Initiator Type
13. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
14. Select Existing Host and click Browse Host




15. Select <<var_ucs_t005_hana1_sp_name>>-DATA and click OK

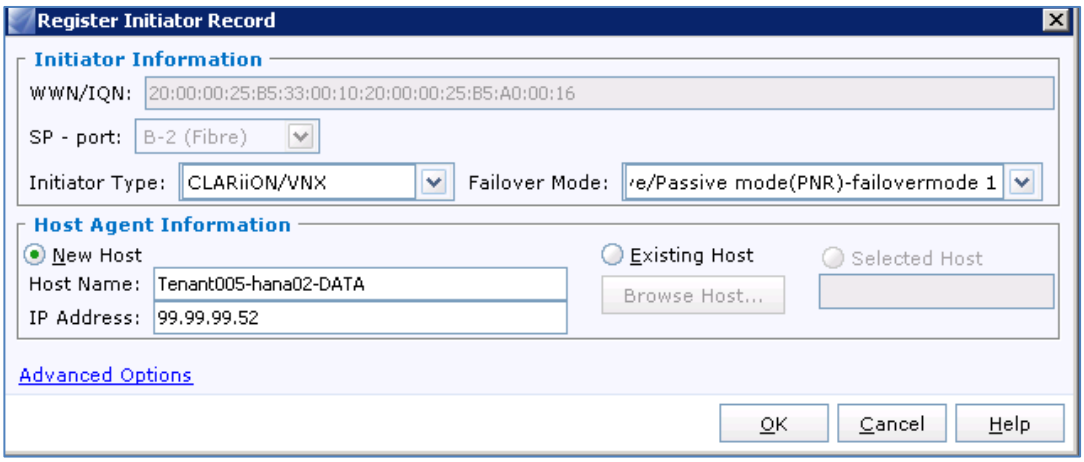



16. Click OK
17. Click Yes
18. Click OK
19. Click OK

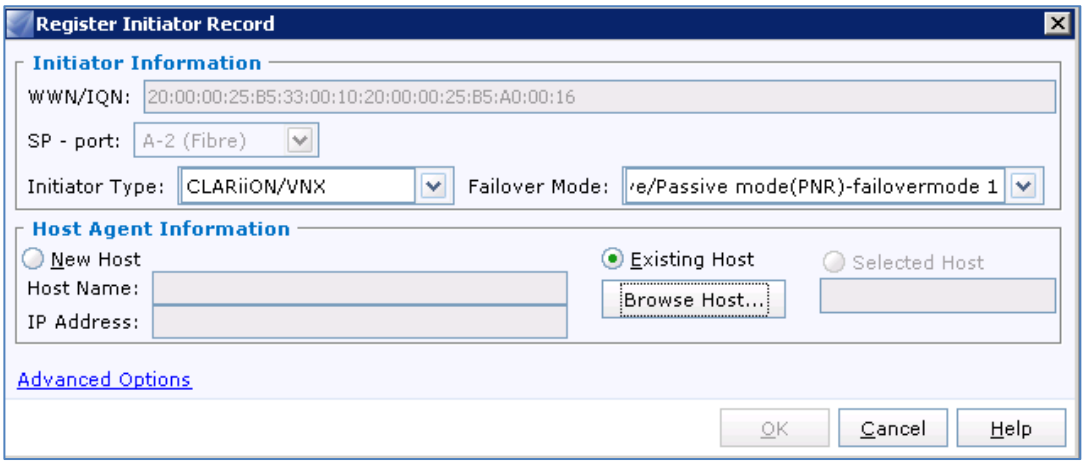


Repeat Step 10 to 18 for all remaining paths of this server in the list.

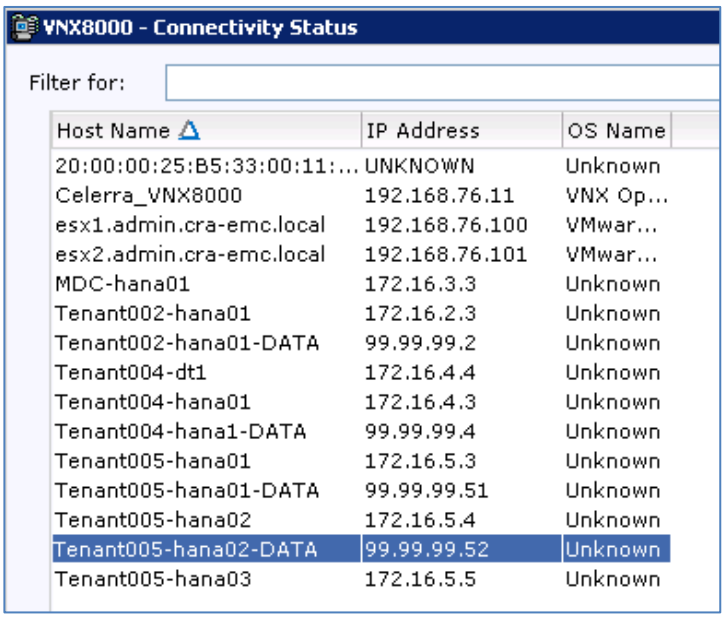
20. Select one of the unregistered entries for the host Tenant005-hana02, click Register
21. Select CLARiiON/VNX as the Initiator Type
22. Select Active/Passive PNR - failovermode 1 as the Failover Mode
23. Enter <<var_ucs_t005_hana2_sp_name>>-DATA as the Host Name (indicates the relationship to the Service Profile)
24. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
25. Click OK
26. Click Yes
27. Click OK
28. Click OK




29. Select the next un-registered Entry for this host <<var_ucs_t005_hana2_sp_name>>, click Register
30. Select CLARiiON/VNX as the Initiator Type
31. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
32. Select Existing Host and click Browse Host




33. Select <<var_ucs_t005_hana2_sp_name>>-DATA and click OK

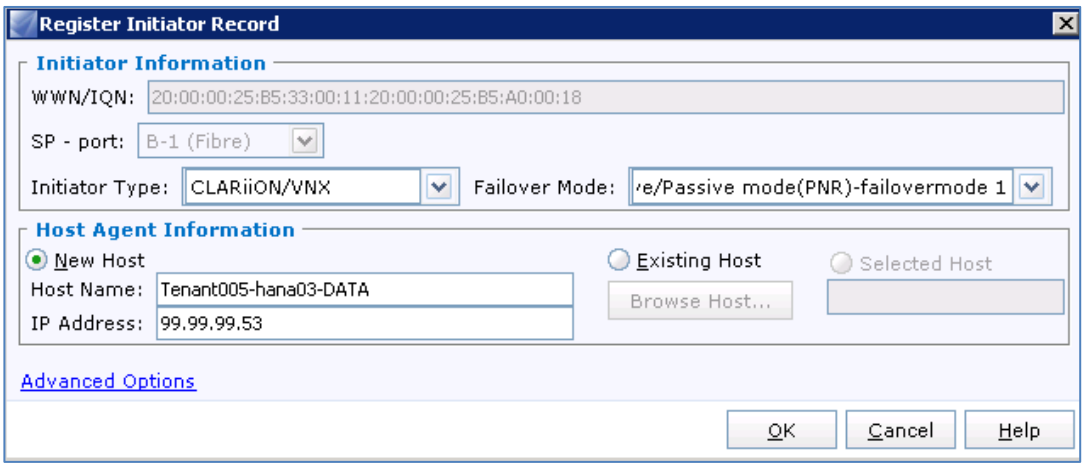



34. Click OK
35. Click Yes
36. Click OK
37. Click OK

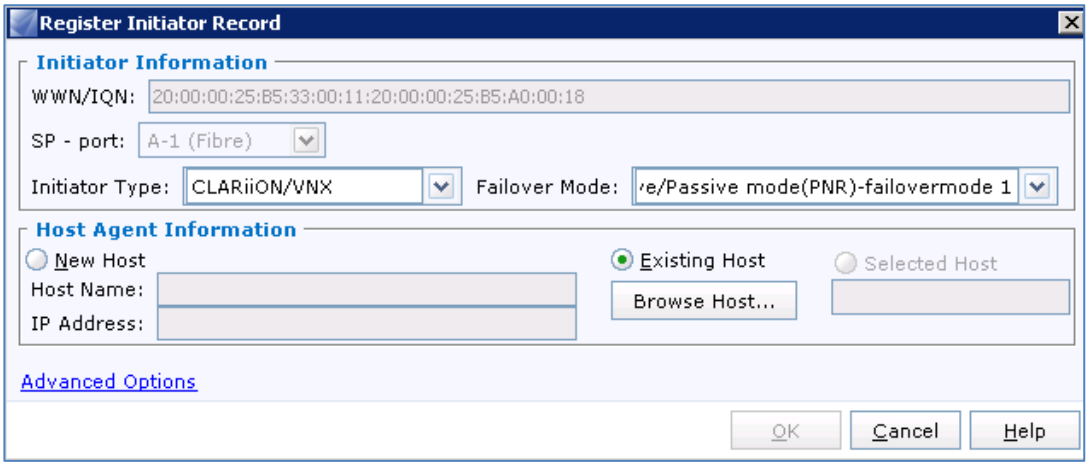


Repeat Step 28 to 36 for all remaining paths of this server in the list.

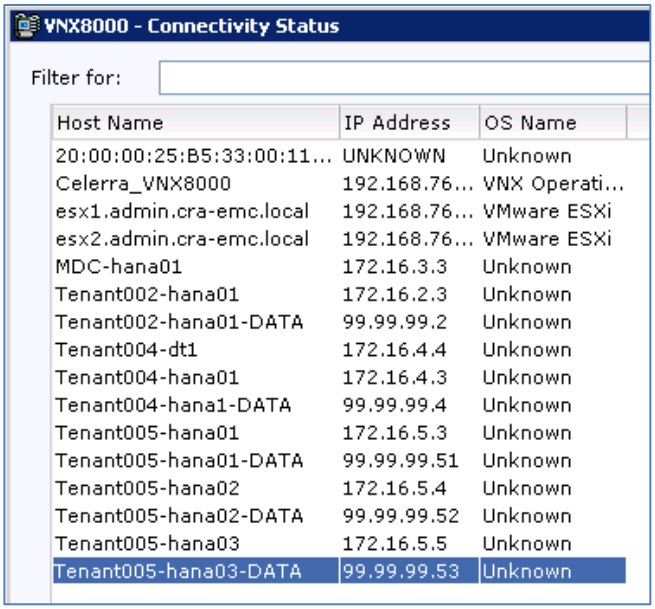
38. Select one of the unregistered entries for the host Tenant005-hana03, click Register
39. Select CLARiiON/VNX as the Initiator Type
40. Select Active/Passive PNR - failovermode 1 as the Failover Mode
41. Enter <<var_ucs_t005_hana3_sp_name>>-DATA as the Host Name (indicates the relationship to the Service Profile)
42. Enter a fictive IP Address as the IP Address – the IP address must be unique on the EMC VNX
43. Click OK
44. Click Yes
45. Click OK
46. Click OK




47. Select the next un-registered Entry for this host <<var_ucs_t005_hana3_sp_name>>, click Register
48. Select CLARiiON/VNX as the Initiator Type
49. Select Active/Passive mode(PNR)-failovermode 1 as the Failover Mode
50. Select Existing Host and click Browse Host




51. Select <<var_ucs_t005_hana3_sp_name>>-DATA and click OK



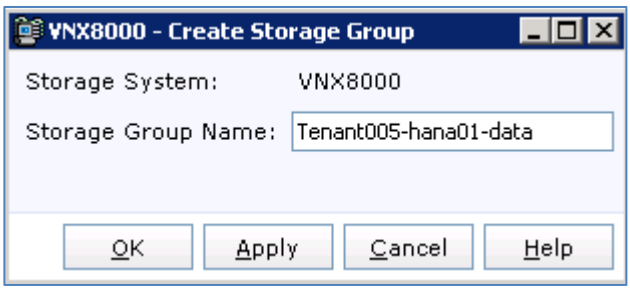

52. Click OK
53. Click Yes
54. Click OK
55. Click OK



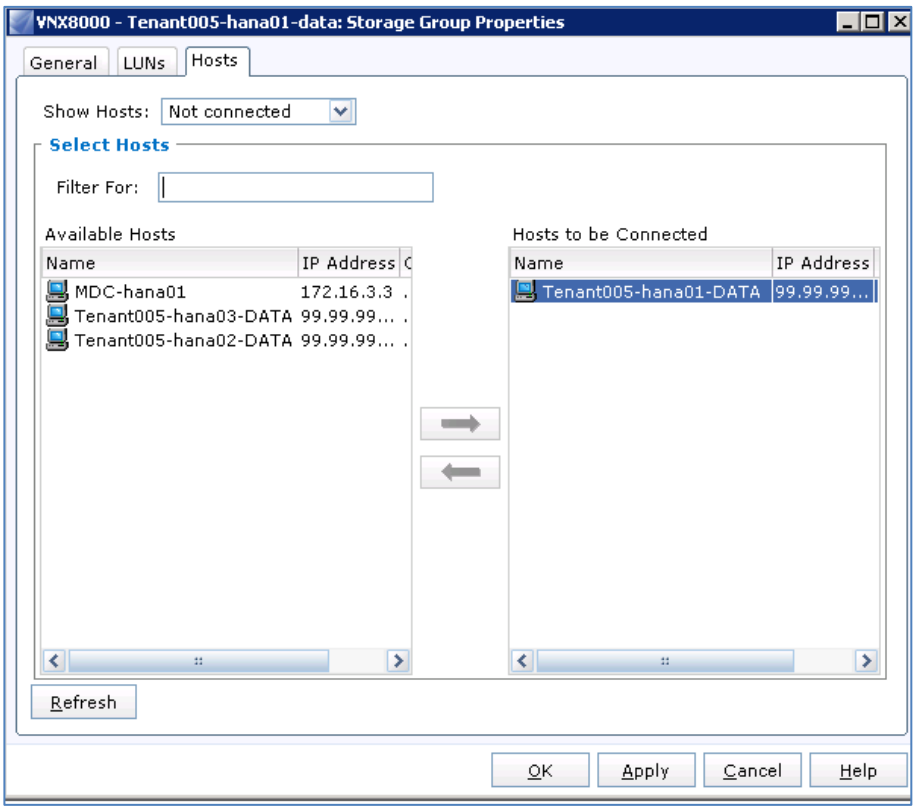
Repeat Step 46 to 55 for all remaining paths of this server in the list.

## Create Storage-Group

1. Navigate to Hosts > Storage Groups
2. Click Create
3. Enter <<var_ucs_t005_hana1_sp_name>>-data as the Name
4. Click OK
5. Click Yes

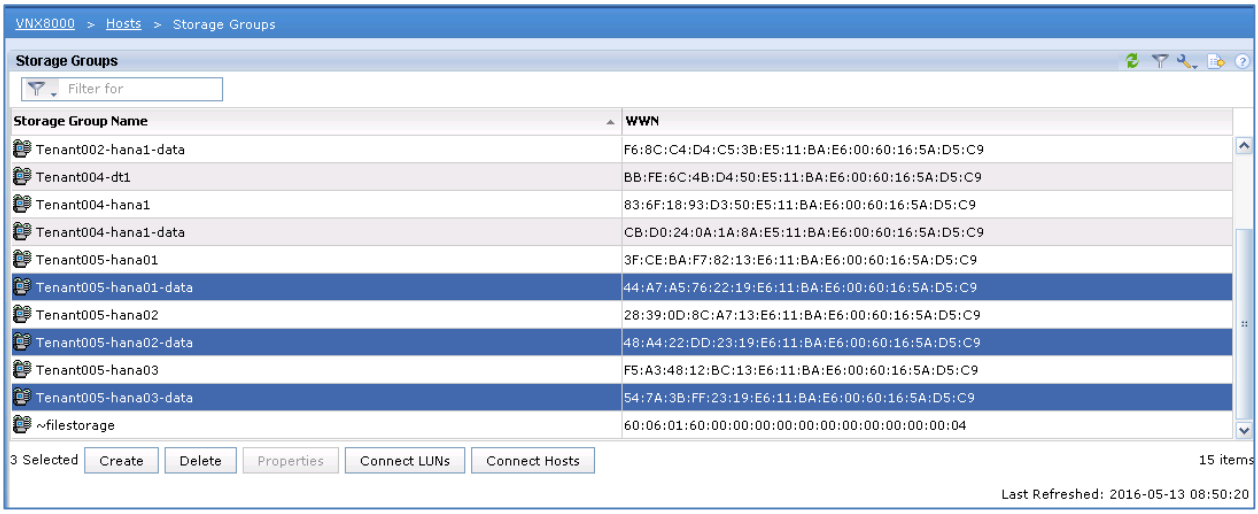



6. Click Yes
7. Click the Hosts tab
8. Select <<var_ucs_t005_hana1_sp_name>>-DATA and click the -> icon
9. Click OK
10. Click Yes
11. Click OK



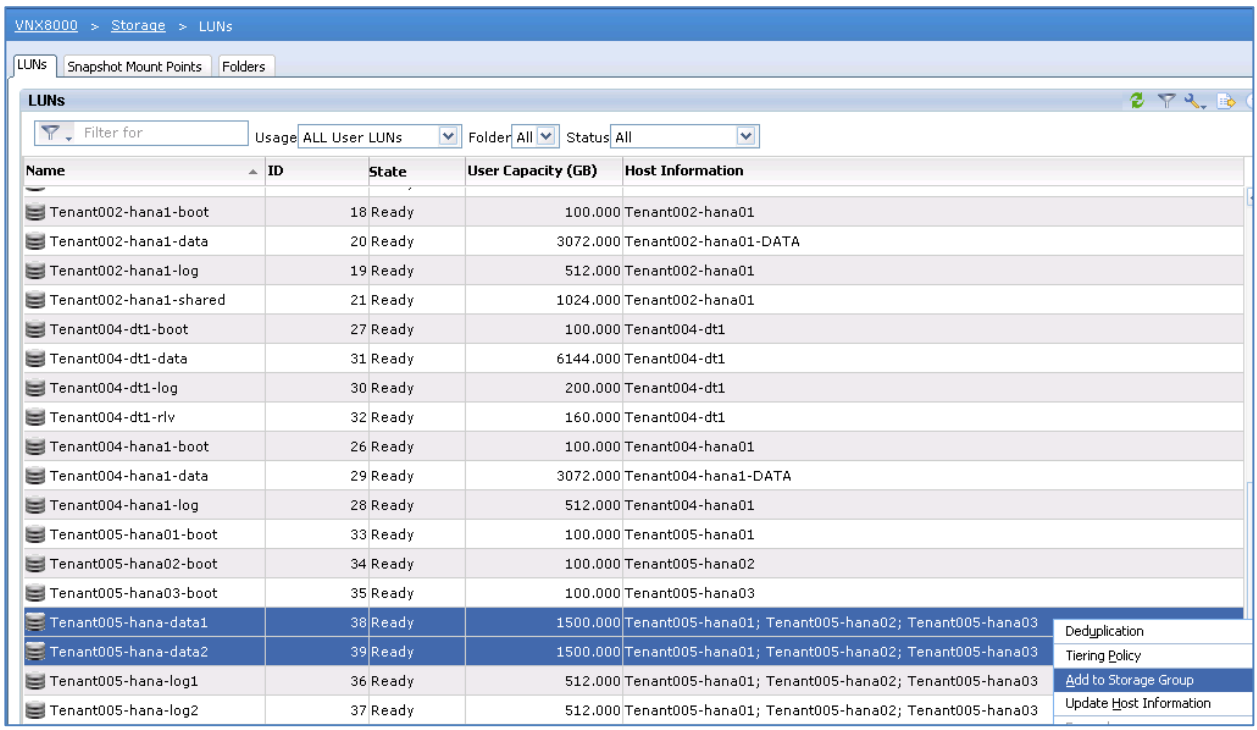

12. Create Storage Groups Tenant005-hana02-data and Tenant005-hana03-data and assign the Hosts Tenant005-hana02-DATA & Tenant005-hana03-DATA created in the previous step.

The storage hosts list is shown below:

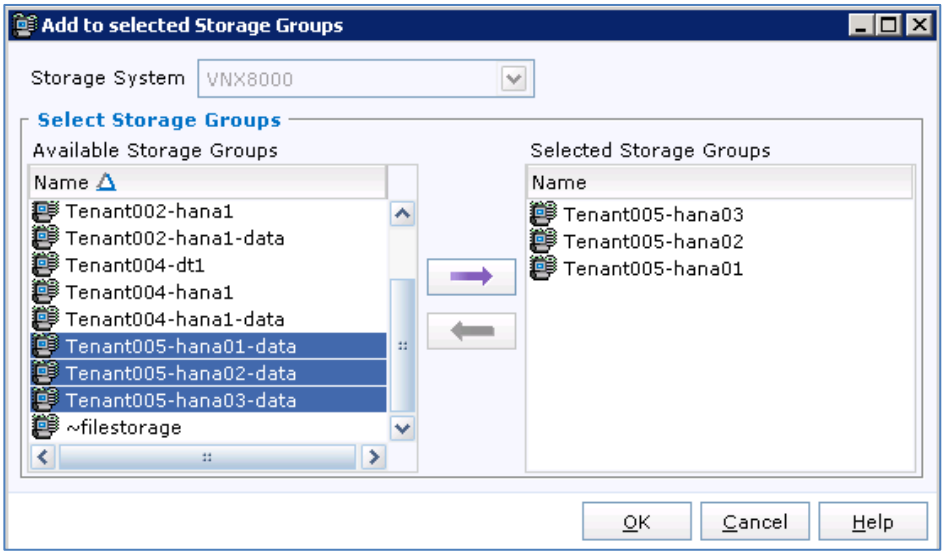


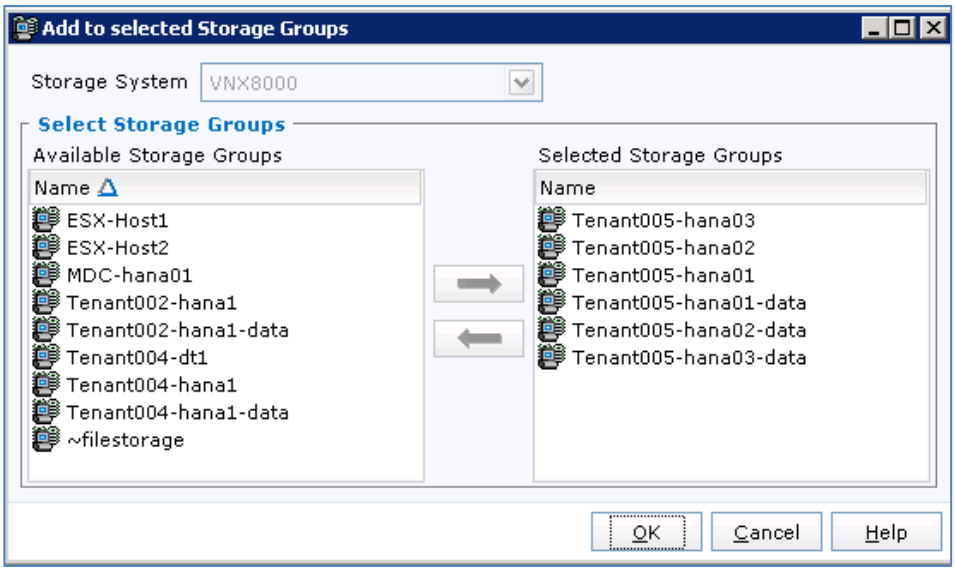

13. Go to StorageSystem -> Storage -> LUNs

14. Select LUNs <<var_ucs_t005-hana_sys-name>>-data1 and <<var_ucs_t005-hana_sys-name>>-data2 and Right click. From the list select “Add to Storage Group”

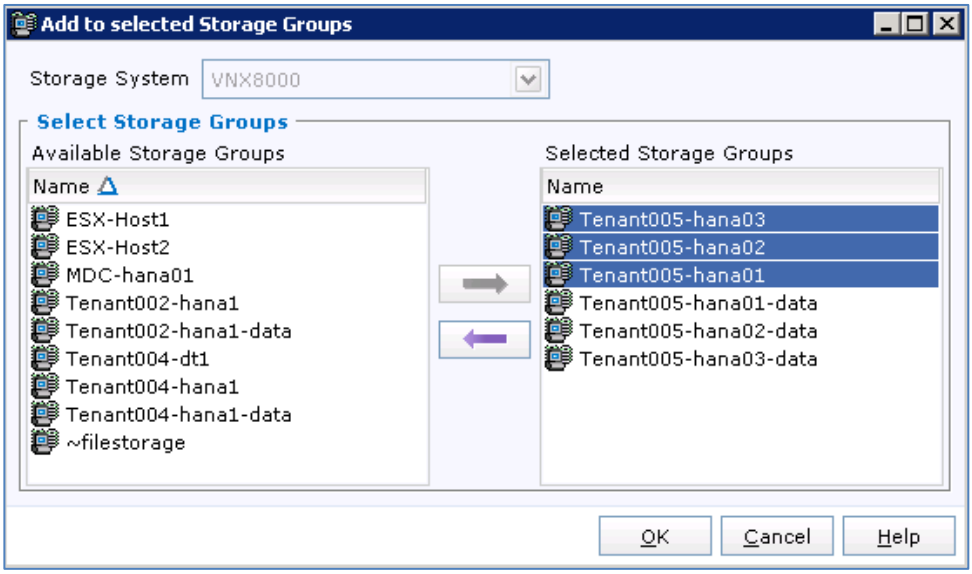


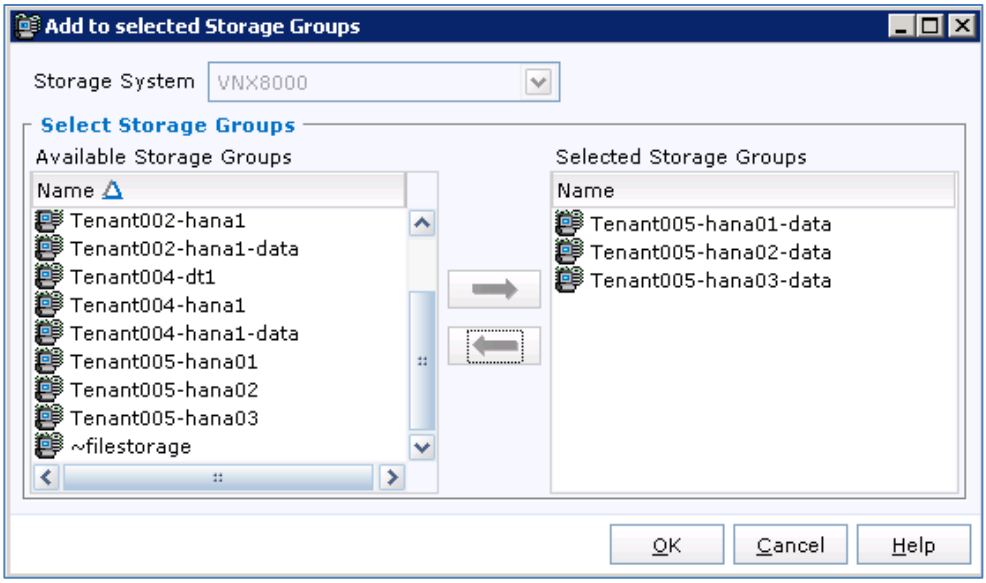

15. Under “Available Storage Groups” select <<var_ucs_t005_hana1_sp_name>>-data, <<var_ucs_t005_hana2_sp_name>>-data and <<var_ucs_t005_hana3_sp_name>>-data and Click -> Icon.



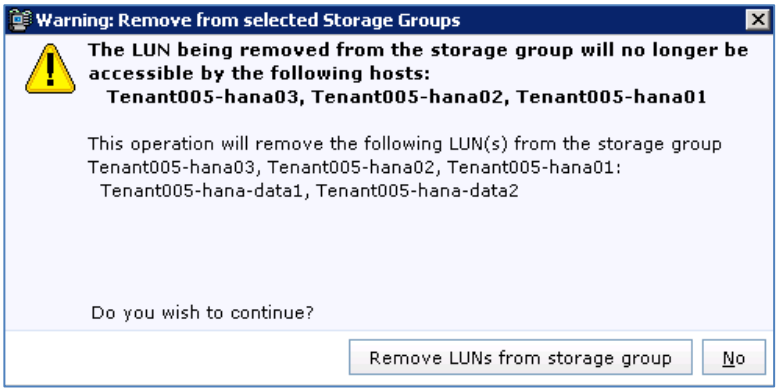




16. Under “Select Storage Groups” select <<var_ucs_t005_hana1_sp_name>>, <<var_ucs_t005_hana2_sp_name>> and <<var_ucs_t005_hana3_sp_name>> and Click <- Icon.


Add to selected Storage Groups
Storage System
VNX8000
Select Storage Groups
Available Storage Groups
Name
ESX-Host1
ESX-Host2
MDC-hana01
Tenant002-hana1
Tenant002-hana1-data
Tenant004-dt1
Tenant004-hana1
Tenant004-hana1-data
~filestorage
Selected Storage Groups
Name
Tenant005-hana03
Tenant005-hana02
Tenant005-hana01
Tenant005-hana01-data
Tenant005-hana02-data
Tenant005-hana03-data
OK
Cancel
Help


Add to selected Storage Groups
Storage System
VNX8000
Select Storage Groups
Available Storage Groups
Name
Tenant002-hana1
Tenant002-hana1-data
Tenant004-dt1
Tenant004-hana1
Tenant004-hana1-data
Tenant005-hana01
Tenant005-hana02
Tenant005-hana03
~filestorage
Selected Storage Groups
Name
Tenant005-hana01-data
Tenant005-hana02-data
Tenant005-hana03-data
OK
Cancel
Help

17. Click OK


Warning: Remove from selected Storage Groups
The LUN being removed from the storage group will no longer be accessible by the following hosts:
Tenant005-hana03, Tenant005-hana02, Tenant005-hana01
This operation will remove the following LUN(s) from the storage group Tenant005-hana03, Tenant005-hana02, Tenant005-hana01:
Tenant005-hana-data1, Tenant005-hana-data2
Do you wish to continue?
Remove LUNs from storage group
No

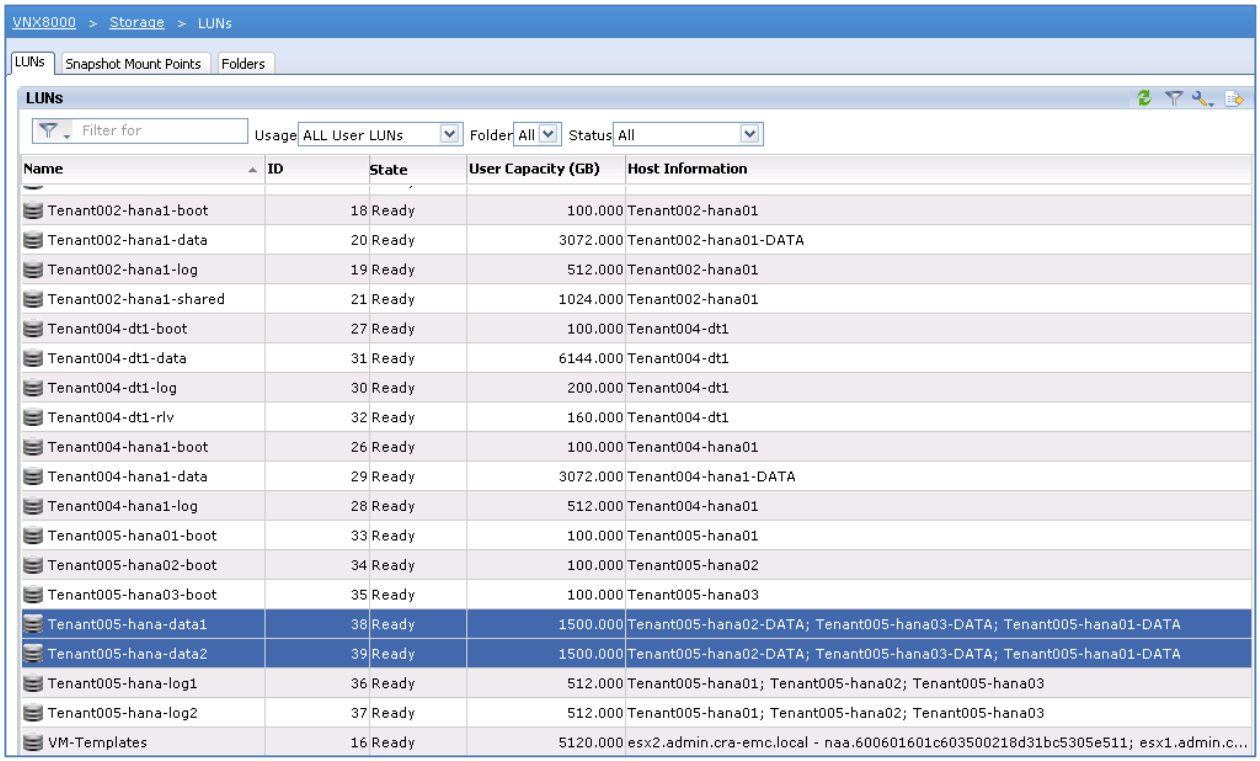
18. Click “Remove LUNs from storage group”

19. Click Yes

20. Click Yes

21. Click OK

22. The result is shown below:




| Name | ID | State | User Capacity (GB) | Host Information |
|---|---|---|---|---|
| Tenant002-hana1-boot | 18 | Ready | 100.000 | Tenant002-hana01 |
| Tenant002-hana1-data | 20 | Ready | 3072.000 | Tenant002-hana01-DATA |
| Tenant002-hana1-log | 19 | Ready | 512.000 | Tenant002-hana01 |
| Tenant002-hana1-shared | 21 | Ready | 1024.000 | Tenant002-hana01 |
| Tenant004-dt1-boot | 27 | Ready | 100.000 | Tenant004-dt1 |
| Tenant004-dt1-data | 31 | Ready | 6144.000 | Tenant004-dt1 |
| Tenant004-dt1-log | 30 | Ready | 200.000 | Tenant004-dt1 |
| Tenant004-dt1-rlv | 32 | Ready | 160.000 | Tenant004-dt1 |
| Tenant004-hana1-boot | 26 | Ready | 100.000 | Tenant004-hana01 |
| Tenant004-hana1-data | 29 | Ready | 3072.000 | Tenant004-hana1-DATA |
| Tenant004-hana1-log | 28 | Ready | 512.000 | Tenant004-hana01 |
| Tenant005-hana01-boot | 33 | Ready | 100.000 | Tenant005-hana01 |
| Tenant005-hana02-boot | 34 | Ready | 100.000 | Tenant005-hana02 |
| Tenant005-hana03-boot | 35 | Ready | 100.000 | Tenant005-hana03 |
| Tenant005-hana-data1 | 38 | Ready | 1500.000 | Tenant005-hana02-DATA; Tenant005-hana03-DATA; Tenant005-hana01-DATA |
| Tenant005-hana-data2 | 39 | Ready | 1500.000 | Tenant005-hana02-DATA; Tenant005-hana03-DATA; Tenant005-hana01-DATA |
| Tenant005-hana-log1 | 36 | Ready | 512.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |
| Tenant005-hana-log2 | 37 | Ready | 512.000 | Tenant005-hana01; Tenant005-hana02; Tenant005-hana03 |
| VM-Templates | 16 | Ready | 5120.000 | esx2.admin.cra-emc.local - naa.600601601c603500218d31bc5305e511; esx1.admin.c... |

23. Create directory for HANA DATA and LOG filesystems on all the nodes

    mkdir –p /hana/data/<<var_t005_hana_sid>> and

    mkdir –p /hana/log/<<var_t005_hana_sid>>

24. Boot/reboot the servers

## Install SAP HANA

1. Mount the Software share to access the SAP HANA installation files.

```
mkdir /software
mount 172.30.113.11:/FS_Software /software
```

2. Place a copy global.ini file prepared in earlier step 306 temporarily on (say, /tmp of) the first node where we intend to start the HANA install to be used with hdblcm in the next step.

3. Use the SAP HANA installation Guide provided by SAP for the software revision you plan to install. The program to install SAP HANA Revision 100 is hdblcm located in the directory <Installation source>/DATA_UNITS/HDB_LCM_LINUX_X86_64.

```
cd /software/SAP/SPS10/REV100/DATA_UNITS/HDB_LCM_LINUX_X86_64

./hdblcm --action=install --component_root=/software/SAP/ --addhosts=t005-
hana02:storage_partition=2,t005-hana03:role=standby --storage_cfg=/tmp/


SAP HANA Lifecycle Management - SAP HANA 1.00.100.00.1434512907
************************************************************


Scanning Software Locations...
Detected components:
    SAP HANA Database (1.00.100.00.1434512907) in
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA AFL (Misc) (1.00.100.00.1434529984) in
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA LCAPPS (1.00.100.000.454467) in
/software/SAP/SPS10/REV100/DATA_UNITS/HANA_LCAPPS_10_LINUX_X86_64/packages
    SAP TRD AFL FOR HANA (1.00.100.00.1434529984) in
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_TRD_AFL_LINUX_X86_64/packages
    SAP HANA Database Client (1.00.100.00.1434512907) in
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Studio (2.1.4.000000) in
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Smart Data Access (1.00.4.004.0) in
/software/SAP/SPS10/REV100/DATA_UNITS/SAP_HANA_SDA_10/packages
    SAP HANA Dynamic Tiering (16.0.0.995) in
/software/SAP/DT_1/SAP_HANA_DYNAMIC_TIERING/es


SAP HANA Database version '1.00.100.00.1434512907' will be installed.

Select additional components for installation:

  Index | Components | Description
  -------------------------------------------------------------------------------
--
  1     | server     | No additional components
  2     | all        | All components
  3     | client     | Install SAP HANA Database Client version
1.00.100.00.1434512907
  4     | afl        | Install SAP HANA AFL (Misc) version 1.00.100.00.1434529984
  5     | lcapps     | Install SAP HANA LCAPPS version 1.00.100.000.454467
  6     | smartda    | Install SAP HANA Smart Data Access version 1.00.4.004.0
  7     | studio     | Install SAP HANA Studio version 2.1.4.000000
  8     | trd        | Install SAP TRD AFL FOR HANA version 1.00.100.00.1434529984
  9     | es         | Install SAP HANA Dynamic Tiering version 16.0.0.995
```

```
Enter comma-separated list of the selected indices [3]:
Enter Installation Path [/hana/shared]:
Enter Local Host Name [t005-hana01]:
Do you want to add additional hosts to the system? (y/n): y
Enter comma-separated host names to add: t005-hana02,t005-hana03
Enter Root User Name [root]:
Collecting information from host 't005-hana02'...
Collecting information from host 't005-hana03'...
Information collected from host 't005-hana02'.
Information collected from host 't005-hana03'.

Select roles for host 't005-hana02':

  Index | Host Role                | Description
  ------------------------------------------------------------------
  1     | worker                   | Database Worker
  2     | standby                  | Database Standby
  3     | extended_storage_worker  | Dynamic Tiering Worker
  4     | extended_storage_standby | Dynamic Tiering Standby
  5     | streaming                | Smart Data Streaming
  6     | rdsync                   | Remote Data Sync
  7     | ets_worker               | Accelerator for SAP ASE Worker
  8     | ets_standby              | Accelerator for SAP ASE Standby

Enter comma-separated list of selected indices [1]:
Enter Host Failover Group for host 't005-hana02' [default]:
Enter Storage Partition Number for host 't005-hana02' [<<assign automatically>>]:

Select roles for host 't005-hana03':

  Index | Host Role                | Description
  ------------------------------------------------------------------
  1     | worker                   | Database Worker
  2     | standby                  | Database Standby
  3     | extended_storage_worker  | Dynamic Tiering Worker
  4     | extended_storage_standby | Dynamic Tiering Standby
  5     | streaming                | Smart Data Streaming
  6     | rdsync                   | Remote Data Sync
  7     | ets_worker               | Accelerator for SAP ASE Worker
  8     | ets_standby              | Accelerator for SAP ASE Standby

Enter comma-separated list of selected indices [1]: 2
Enter Host Failover Group for host 't005-hana03' [default]:
Enter SAP HANA System ID: TS5
Enter Instance Number [00]: 55

  Index | Database Mode       | Description
  ------------------------------------------------------------------------------
-------------
  1     | single_container    | The system contains one database
  2     | multiple_containers | The system contains one system database and 1..n
tenant databases

Select Database Mode / Enter Index [1]: 1
```

```
  Index | System Usage | Description
  -------------------------------------------------------------------------------
  1     | production   | System is used in a production environment
  2     | test         | System is used for testing, not production
  3     | development  | System is used for development, not production
  4     | custom       | System usage is neither production, test nor development

Select System Usage / Enter Index [4]: 1
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 't005-hana01' [t005-hana01]:
Enter Certificate Host Name For Host 't005-hana03' [t005-hana03]:
Enter Certificate Host Name For Host 't005-hana02' [t005-hana02]:
Enter SAP Host Agent User (sapadm) Password:
Confirm SAP Host Agent User (sapadm) Password:
Enter System Administrator (ts5adm) Password:
Confirm System Administrator (ts5adm) Password:
Enter System Administrator Home Directory [/usr/sap/TS5/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1000]:
Enter ID of User Group (sapsys) [79]:
Enter Database User (SYSTEM) Password:
Confirm Database User (SYSTEM) Password:
Restart instance after machine reboot? [n]: y

Summary before execution:
=========================

SAP HANA Components Installation
   Installation Parameters
      Remote Execution: ssh
      Installation Path: /hana/shared
      Local Host Name: t005-hana01
      Root User Name: root
      Directory containing a storage configuration: /tmp/
      SAP HANA System ID: TS5
      Instance Number: 55
      Database Mode: single_container
      System Usage: production
      Location of Data Volumes: /hana/data/TS5
      Location of Log Volumes: /hana/log/TS5
      Certificate Host Names: t005-hana01 -> t005-hana01, t005-hana03 -> t005-
hana03, t005-hana02 -> t005-hana02
      System Administrator Home Directory: /usr/sap/TS5/home
      System Administrator Login Shell: /bin/sh
      System Administrator User ID: 1000
      ID of User Group (sapsys): 79
      Restart instance after machine reboot?: Yes
      Directory root to search for components: /software/SAP/
      SAP HANA Database Client Installation Path: /hana/shared/TS5/hdbclient
   Software Components
      SAP HANA Database
         Install version 1.00.100.00.1434512907
         Location:
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
```

```
      SAP HANA AFL (Misc)
         Do not install
      SAP HANA LCAPPS
         Do not install
      SAP TRD AFL FOR HANA
         Do not install
      SAP HANA Database Client
         Install version 1.00.100.00.1434512907
         Location:
/software/SAP/SPS10/REV100/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
      SAP HANA Studio
         Do not install
      SAP HANA Smart Data Access
         Do not install
      SAP HANA Dynamic Tiering
         Do not install
   Additional Hosts
      t005-hana03
         Role: Database Standby (standby)
         Storage Partition: N/A
      t005-hana02
         Role: Database Worker (worker)
         Storage Partition: 2

Do you want to continue? (y/n):

Installing components...
Installing SAP HANA Database...
  Preparing package 'Saphostagent Setup'...
  Preparing package 'Python Support'...
  Preparing package 'Python Runtime'...
  Preparing package 'Product Manifest'...
  Preparing package 'Binaries'...
  Preparing package 'Installer'...
  Preparing package 'Ini Files'...
  Preparing package 'HWCCT'...
  Preparing package 'Emergency Support Package'...
  Preparing package 'EPM'...
  Preparing package 'Documentation'...
  Preparing package 'Delivery Units'...
  Preparing package 'DAT Languages'...
  Preparing package 'DAT Configfiles'...
  Creating System...
  Extracting software...
  Installing package 'Saphostagent Setup'...
  Installing package 'Python Support'...
  Installing package 'Python Runtime'...
  Installing package 'Product Manifest'...
  Installing package 'Binaries'...
  Installing package 'Installer'...
  Installing package 'Ini Files'...
  Installing package 'HWCCT'...
  Installing package 'Emergency Support Package'...
  Installing package 'EPM'...
  Installing package 'Documentation'...
```

```
  Installing package 'Delivery Units'...
  Installing package 'DAT Languages'...
  Installing package 'DAT Configfiles'...
  Creating instance...
  Starting 7 processes on host 't005-hana01':
      Starting on 't005-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't005-hana01': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 't005-hana01': hdbdaemon, hdbindexserver, hdbwebdispatcher,
hdbxsengine
      Starting on 't005-hana01': hdbdaemon, hdbwebdispatcher, hdbxsengine
      Starting on 't005-hana01': hdbdaemon, hdbwebdispatcher
    All server processes started on host 't005-hana01'.
  Importing delivery units...
  Importing delivery unit HCO_INA_SERVICE
  Importing delivery unit HANA_DT_BASE
  Importing delivery unit HANA_IDE_CORE
  Importing delivery unit HANA_TA_CONFIG
  Importing delivery unit HANA_UI_INTEGRATION_SVC
  Importing delivery unit HANA_UI_INTEGRATION_CONTENT
  Importing delivery unit HANA_XS_BASE
  Importing delivery unit HANA_XS_DBUTILS
  Importing delivery unit HANA_XS_EDITOR
  Importing delivery unit HANA_XS_IDE
  Importing delivery unit HANA_XS_LM
  Importing delivery unit HDC_ADMIN
  Importing delivery unit HDC_IDE_CORE
  Importing delivery unit HDC_SEC_CP
  Importing delivery unit HDC_XS_BASE
  Importing delivery unit HDC_XS_LM
  Importing delivery unit SAPUI5_1
  Importing delivery unit SAP_WATT
  Importing delivery unit HANA_BACKUP
  Importing delivery unit HANA_HDBLCM
  Importing delivery unit HANA_SEC_BASE
  Importing delivery unit HANA_SEC_CP
  Importing delivery unit HANA_ADMIN
  Adding 2 additional hosts in parallel
  Adding host 't005-hana03'...
  Adding host 't005-hana02'...
    Adding host 't005-hana02' to instance '55'...
  hdbnsutil: adding host t005-hana02 to distributed landscape with role=worker,
group=default, subpath=2 ...
Starting SAP HANA Database...
Starting 5 processes on host 't005-hana02':
    Starting on 't005-hana02': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor
    Starting on 't005-hana02': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbpreprocessor
    Starting on 't005-hana02': hdbcompileserver, hdbdaemon, hdbindexserver
    Starting on 't005-hana02': hdbdaemon, hdbindexserver
  All server processes started on host 't005-hana02'.
  hdbaddhost done
    Adding host 't005-hana03' to instance '55'...
```

```
  hdbnsutil: adding host t005-hana03 to distributed landscape with role=standby,
group=default ...
Starting SAP HANA Database...
Starting 5 processes on host 't005-hana03':
    Starting on 't005-hana03': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbnameserver, hdbpreprocessor
    Starting on 't005-hana03': hdbcompileserver, hdbdaemon, hdbindexserver,
hdbpreprocessor
    Starting on 't005-hana03': hdbcompileserver, hdbdaemon, hdbindexserver
    Starting on 't005-hana03': hdbdaemon, hdbindexserver
  All server processes started on host 't005-hana03'.
  hdbaddhost done...
…
SAP HANA system installed
….
Log file written to '/var/tmp/hdb_TS5_hdblcm_install_2016-01-11_08.00.00/hdblcm.log'
on host 't004-hana01'.
```

4. Check the SAP HANA status on all both nodes.

5. Log into t005-hana01 as td4adm and run the sapcontrol command to check the status

```
t005-hana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 55 -prot NI_HTTP -function
GetSystemInstanceList

17.05.2016 05:09:33
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus
t005-hana03, 55, 55513, 55514, 0.3, HDB, GREEN
t005-hana01, 55, 55513, 55514, 0.3, HDB, GREEN
t005-hana02, 55, 55513, 55514, 0.3, HDB, GREEN
t005-hana01:~ #


t005-hana01:~ # su - ts5adm
t005-hana01:/usr/sap/TS5/HDB55> ./HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
ts5adm   19836 19835  0.6  13896  2732 -sh
ts5adm   19894 19836 16.6  12912  1736  \_ /bin/sh ./HDB info
ts5adm   19917 19894  0.0   4956   852      \_ ps fx -U ts5adm -o
user,pid,ppid,pcpu,vsz,rss,args
ts5adm   11178     1  0.0  22336  1560 sapstart
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana01
ts5adm   11186 11178  0.0 547984 292916  \_ /usr/sap/TS5/HDB55/t005-
hana01/trace/hdb.sapTS5_HDB55 -d -nw -f /usr/sap/TS5/HDB5
ts5adm   11200 11186  0.6 4140344 1225740      \_ hdbnameserver
ts5adm   11822 11186  2.2 3604992 1133652      \_ hdbcompileserver
ts5adm   11825 11186 18.4 11608856 9054128       \_ hdbpreprocessor
ts5adm   11847 11186 14.6 13463796 10231124      \_ hdbindexserver
ts5adm   11850 11186  1.5 4415032 1338336      \_ hdbxsengine
ts5adm   12250 11186  0.4 3392504 741252      \_ hdbwebdispatcher
ts5adm   11083     1  0.0 211088 73668 /usr/sap/TS5/HDB55/exe/sapstartsrv
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana01 -
```

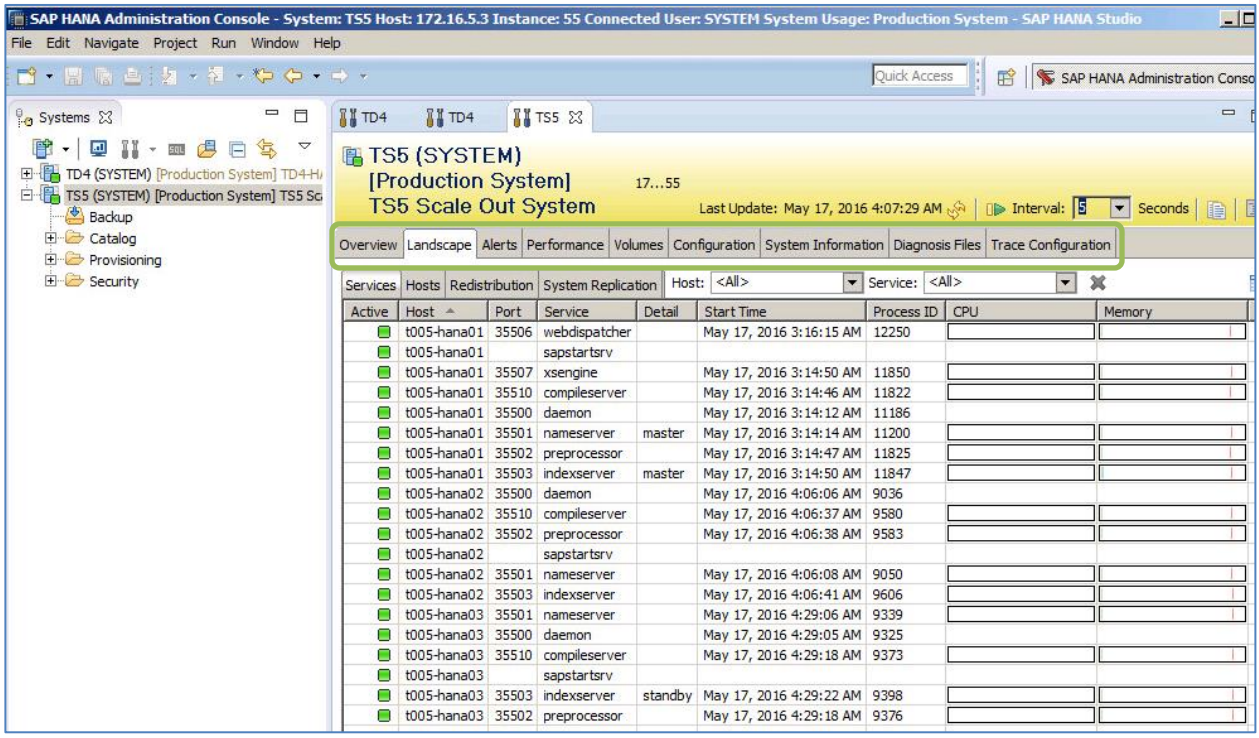
```
t005-hana01:/usr/sap/TS5/HDB55>

t005-hana02:/usr/sap/TS5/HDB55> ./HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
ts5adm    9858  9857  0.2  13896  2776 -sh
ts5adm    9916  9858 20.0  12912  1732  \_ /bin/sh ./HDB info
ts5adm    9939  9916  0.0   4956   864      \_ ps fx -U ts5adm -o
user,pid,ppid,pcpu,vsz,rss,args
ts5adm    9027     1  0.0  22336  1556 sapstart
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana02
ts5adm    9036  9027  0.0 482432 289316  \_ /usr/sap/TS5/HDB55/t005-
hana02/trace/hdb.sapTS5_HDB55 -d -nw -f /usr/sap/TS5/HDB5
ts5adm    9050  9036  0.8 3334220 791288      \_ hdbnameserver
ts5adm    9580  9036  0.6 2933448 471648      \_ hdbcompileserver
ts5adm    9583  9036  0.5 2812860 458396      \_ hdbpreprocessor
ts5adm    9606  9036  5.0 5835980 2744308      \_ hdbindexserver
ts5adm    8932     1  0.0 211084 73264 /hana/shared/TS5/HDB55/exe/sapstartsrv
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana
t005-hana02:/usr/sap/TS5/HDB55>


t005-hana03:/usr/sap/TS5/HDB55> ./HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
ts5adm    9513  9512  1.1  13896  2688 -sh
ts5adm    9570  9513  0.0  12912  1736  \_ /bin/sh ./HDB info
ts5adm    9593  9570  0.0   4956   864      \_ ps fx -U ts5adm -o
user,pid,ppid,pcpu,vsz,rss,args
ts5adm    9316     1  0.0  22336  1556 sapstart
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana03
ts5adm    9325  9316  0.0 482444 291368  \_ /usr/sap/TS5/HDB55/t005-
hana03/trace/hdb.sapTS5_HDB55 -d -nw -f /usr/sap/TS5/HDB5
ts5adm    9339  9325  0.6 3461820 786968      \_ hdbnameserver
ts5adm    9373  9325  0.5 3062208 477020      \_ hdbcompileserver
ts5adm    9376  9325  0.4 3073848 461868      \_ hdbpreprocessor
ts5adm    9398  9325  0.5 3396864 573108      \_ hdbindexserver
ts5adm    9221     1  0.0 210968 73504 /hana/shared/TS5/HDB55/exe/sapstartsrv
pf=/hana/shared/TS5/profile/TS5_HDB55_t005-hana
t005-hana03:/usr/sap/TS5/HDB55>
```

6. Connect through HANA Studio for status check and verification. Use the SAP HANA Studio on a system with network access to the installed SAP HANA system and add the SAP HANA Database. The information you need are as follows:

- Hostname or IP address <<var_t005_hana01_access_ip>>
- SAP HANA System Number <<var_t005_hana_nr>>
- SAP HANA database user (default: SYSTEM)
- SAP HANA database user password <<var_t005_hana_sys_passwd>>


SAP HANA Administration Console - System: TS5 Host: 172.16.5.3 Instance: 55 Connected User: SYSTEM System Usage: Production System - SAP HANA Studio
File Edit Navigate Project Run Window Help
Quick Access
SAP HANA Administration Conso
Systems
TD4 (SYSTEM) [Production System] TD4-Hi
TS5 (SYSTEM) [Production System] TS5 Sc
Backup
Catalog
Provisioning
Security
TD4
TD4
TS5
TS5 (SYSTEM)
[Production System]
TS5 Scale Out System
17...55
Last Update: May 17, 2016 4:07:29 AM
Interval: 5 Seconds
Overview Landscape Alerts Performance Volumes Configuration System Information Diagnosis Files Trace Configuration
Services Hosts Redistribution System Replication Host: <All> Service: <All>
Active Host Port Service Detail Start Time Process ID CPU Memory
t005-hana01 35506 webdispatcher May 17, 2016 3:16:15 AM 12250
t005-hana01 sapstartsrv
t005-hana01 35507 xsengine May 17, 2016 3:14:50 AM 11850
t005-hana01 35510 compileserver May 17, 2016 3:14:46 AM 11822
t005-hana01 35500 daemon May 17, 2016 3:14:12 AM 11186
t005-hana01 35501 nameserver master May 17, 2016 3:14:14 AM 11200
t005-hana01 35502 preprocessor May 17, 2016 3:14:47 AM 11825
t005-hana01 35503 indexserver master May 17, 2016 3:14:50 AM 11847
t005-hana02 35500 daemon May 17, 2016 4:06:06 AM 9036
t005-hana02 35510 compileserver May 17, 2016 4:06:37 AM 9580
t005-hana02 35502 preprocessor May 17, 2016 4:06:38 AM 9583
t005-hana02 sapstartsrv
t005-hana02 35501 nameserver May 17, 2016 4:06:08 AM 9050
t005-hana02 35503 indexserver May 17, 2016 4:06:41 AM 9606
t005-hana03 35501 nameserver May 17, 2016 4:29:06 AM 9339
t005-hana03 35500 daemon May 17, 2016 4:29:05 AM 9325
t005-hana03 35510 compileserver May 17, 2016 4:29:18 AM 9373
t005-hana03 sapstartsrv
t005-hana03 35503 indexserver standby May 17, 2016 4:29:22 AM 9398
t005-hana03 35502 preprocessor May 17, 2016 4:29:18 AM 9376

# Validating Cisco UCS Integrated Infrastructure with SAP HANA

This section provides a list of items that should be reviewed when the solution is configured. The goal of this section is to verify the configuration and functionality of specific aspects of the solution, and to make sure the configuration supports core availability requirements.

## Post Install Checklist

The following configuration items are critical to functionality of the solution, and should be verified prior to deployment into production:

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

## Verify the Redundancy of the Solution Components

The following redundancy checks were performed at the Cisco lab to verify solution robustness. A continuous ping from SP to SP, VM to VM, and vCenter to ESXi hosts should not show significant failures (one or two ping drops might be observed at times, such as FI reboot). Also, all the data must be visible and accessible from all the hosts at all the time.

- Administratively shutdown one of the two server ports connected to the Fabric Extender A. Make sure that connectivity is not affected. When 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 or Service Profiles on the Nexus switches.
- Administratively shutdown both server ports connected to Fabric Extender A. ESXi hosts and SAP HANA hosts should be able to use fabric B in this case.
- Administratively shutdown one of the data links connected to the storage array from FI. Make sure that storage is still available from all the hosts. When administratively enabling the shutdown port, the traffic should be rebalanced. Repeat this step for each link connected to the Storage Processors one after another.
- Reboot one of the two Fabric Interconnects while storage and network access from the servers are going on. The switch reboot should not affect the operations of storage and network access from the Operating systems. When rebooting the FI, the network access load should be rebalanced across the two fabrics.

- Reboot the active storage processor of the VNX storage array and make sure that all the datastores, LUNs and shares are still accessible during and after the reboot of the storage processor.
- 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.
- Reboot the host in maintenance mode, and put it out of the maintenance mode. This should rebalance the VM distribution across the cluster.

# Optional Components

Using Cisco UCS Central can help you to simplify the management and monitoring of multiple Cisco UCS domains across multiple data centers. In addition to Cisco UCS Central, the Cisco UCS Platform Emulator can help to test configuration changes and the impact to other systems. It is not required to use these tools in your deployment but it is recommended to do so.

In this section you will find a high-level information about how to install Cisco UCS Central and Cisco UCS Platform Emulator. The detailed configuration options based on the use cases are documented in the product documents and best practice guides that you can find on the Cisco.com web site.

## Cisco UCS Central

Using Cisco UCS Central is optional and is not a mandatory part of this Datacenter Reference Architecture. If you plan to install more than one Cisco UCS, using Cisco UCS Central can be helpful to manage multiple Cisco UCS from a single place.

The Cisco UCS Central OVA file can be loaded from the Cisco web site.

Table 37 lists the information used to setup the Cisco UCS Central system in this Cisco UCS Integrated Infrastructure.

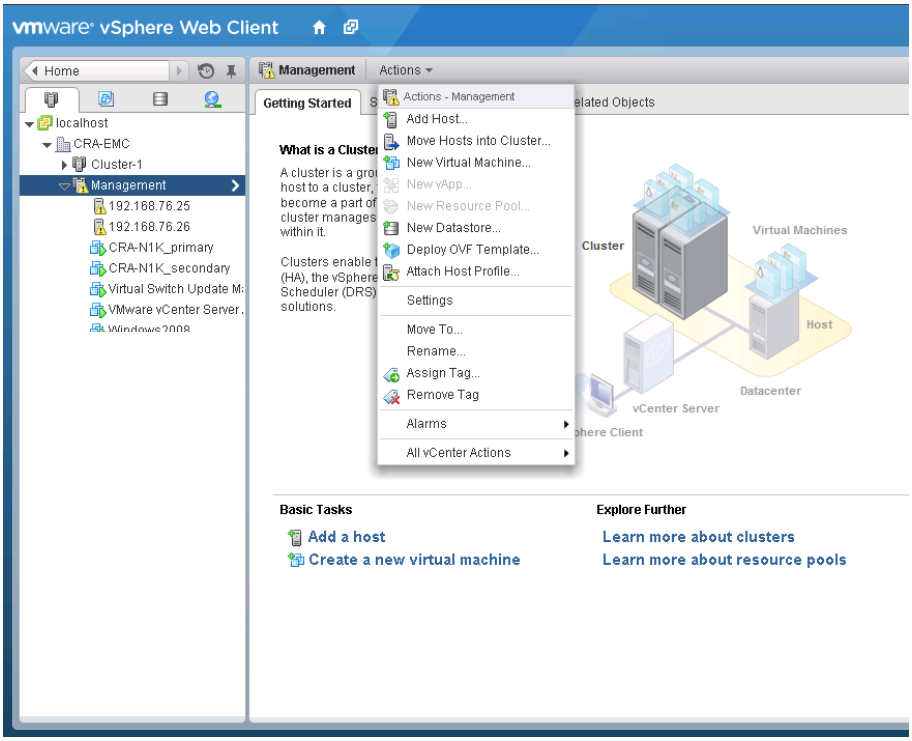
**Table 37 Information to Setup Cisco UCS Central**

| Name | Variable |
|---|---|
| | <<var_vc_mgmt_cluster_name>> |
| | <<var_vc_ucscentral_vm_name>> |
| | <<var_vc_datacenter_name>> |
| | <<var_vc_mgmt_datastore_1>> |
| | <<var_esx_mgmt_network>> |
| | <<var_ucsc_ip>> |
| | <<var_mgmt_netmask>> |
| | <<var_mgmt_gw>> |
| | <<var_ucsc_hostname>> |
| | <<var_nameserver_ip>> |
| | <<var_mgmt_dns_domain_name>> |
| | <<var_mgmt_passwd>> |

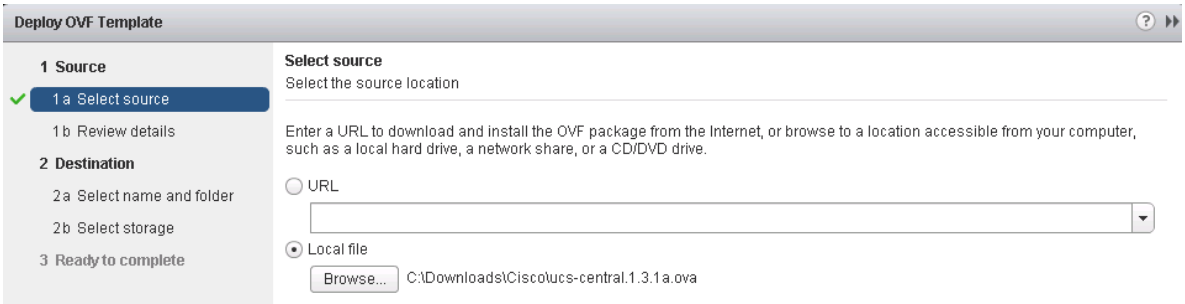
| Name | Variable |
| --- | --- |
| | <<var_shared_secret>> |

To deploy and configure Cisco UCS Central, complete the following high-level steps:

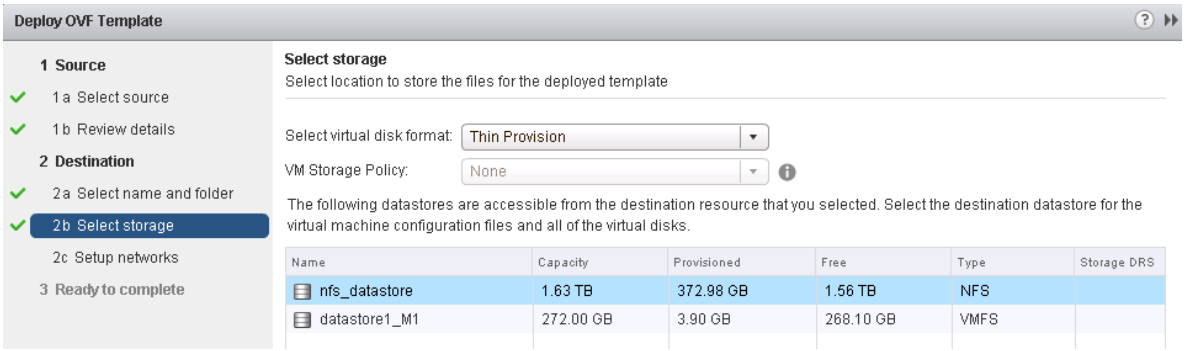
1. Log in to the vSphere Web Client.
2. Click Hosts and Clusters in the Home Screen.
3. Click the <<var_vc_mgmt_cluster_name>>.
4. Click Actions and select Deploy OVF Template.



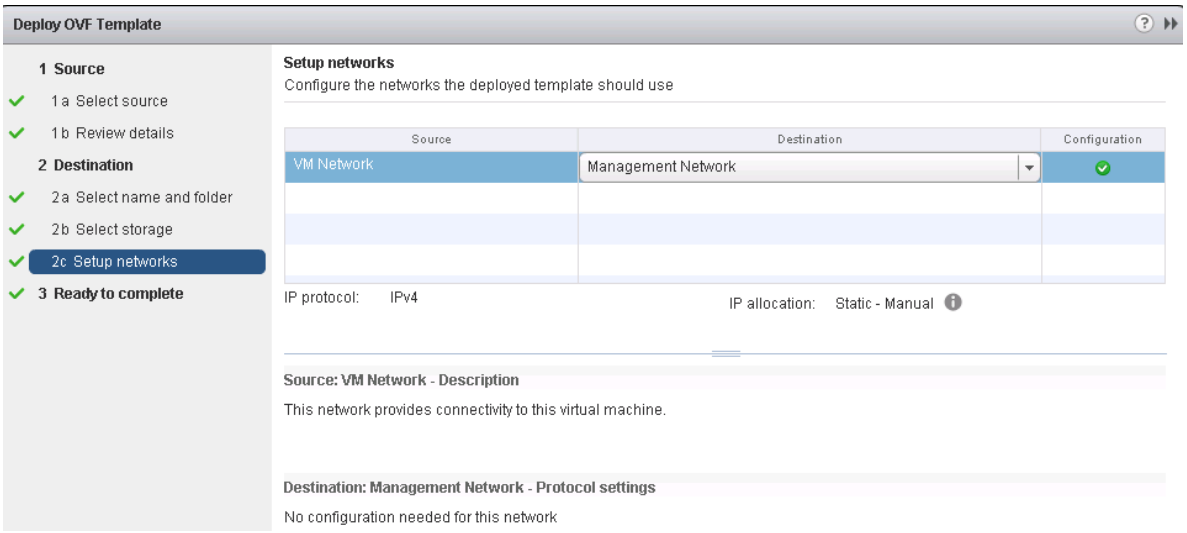

5. Click Browse and select the Cisco UCS Central OVA file.



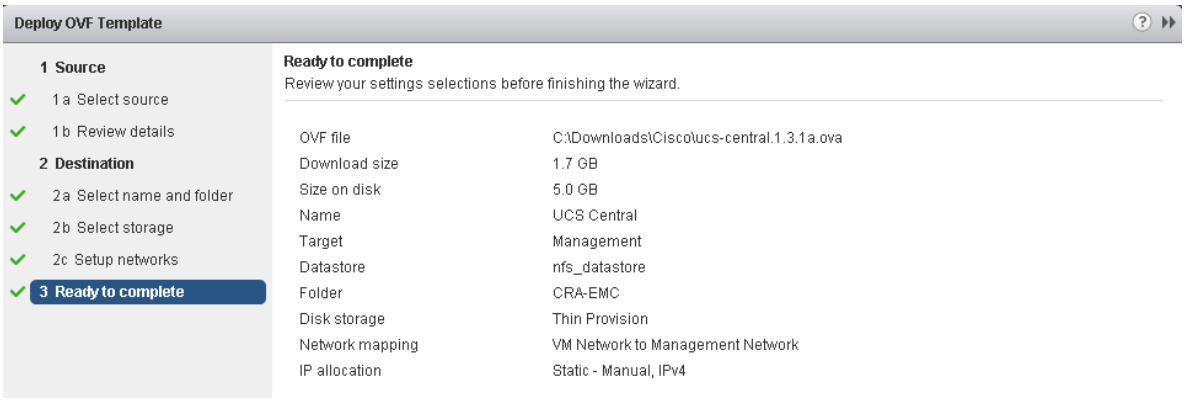
6. Review the Details.
7. Click Next.
8. Enter <<var_vc_ucscentral_vm_name>> as the name.
9. Select <<var_vc_datacenter_name>> as destination.
10. Click Next.
11. Select <<var_vc_mgmt_datastore_1>> as the Storage.
12. Click Next.




13. Select <<var_esx_mgmt_network>> as the Destination for VM Network.
14. Click Next.




15. Review the information.
16. Click Finish.

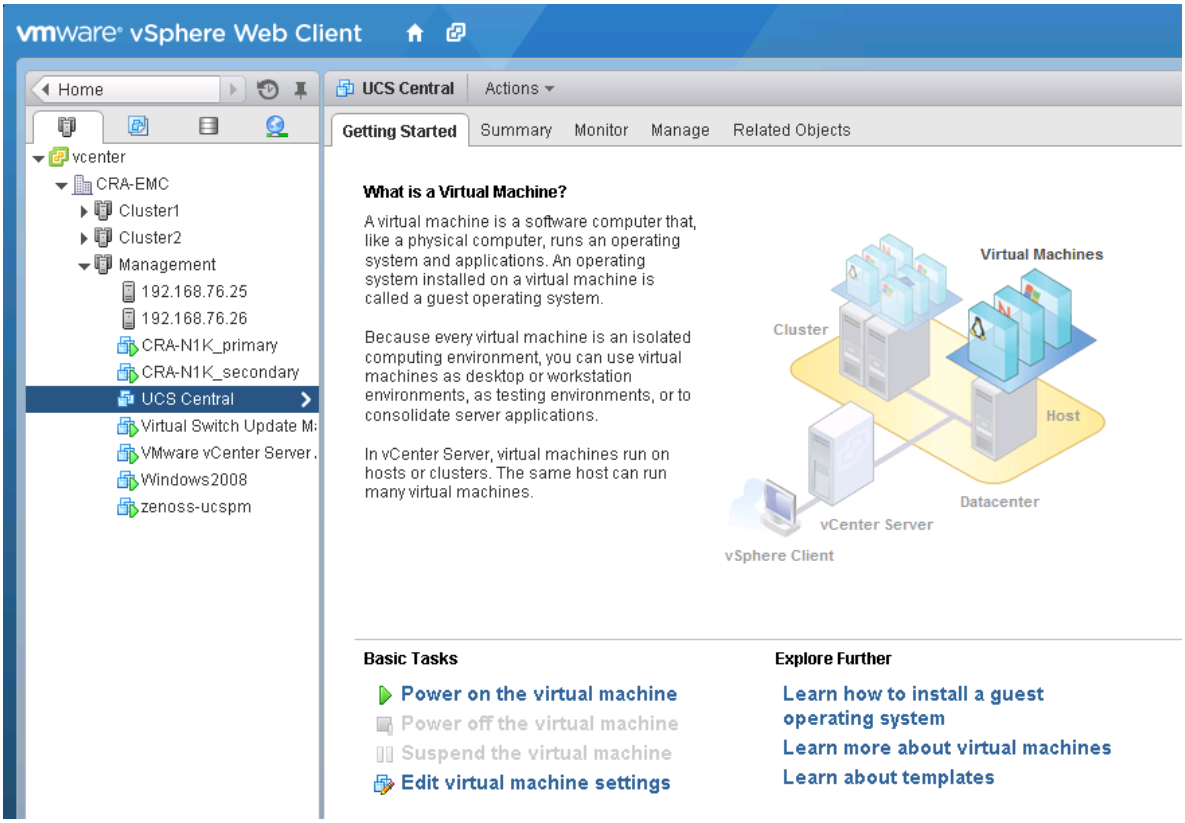



17. Go to the vCenter Home screen.

18. Click Hosts and Clusters.

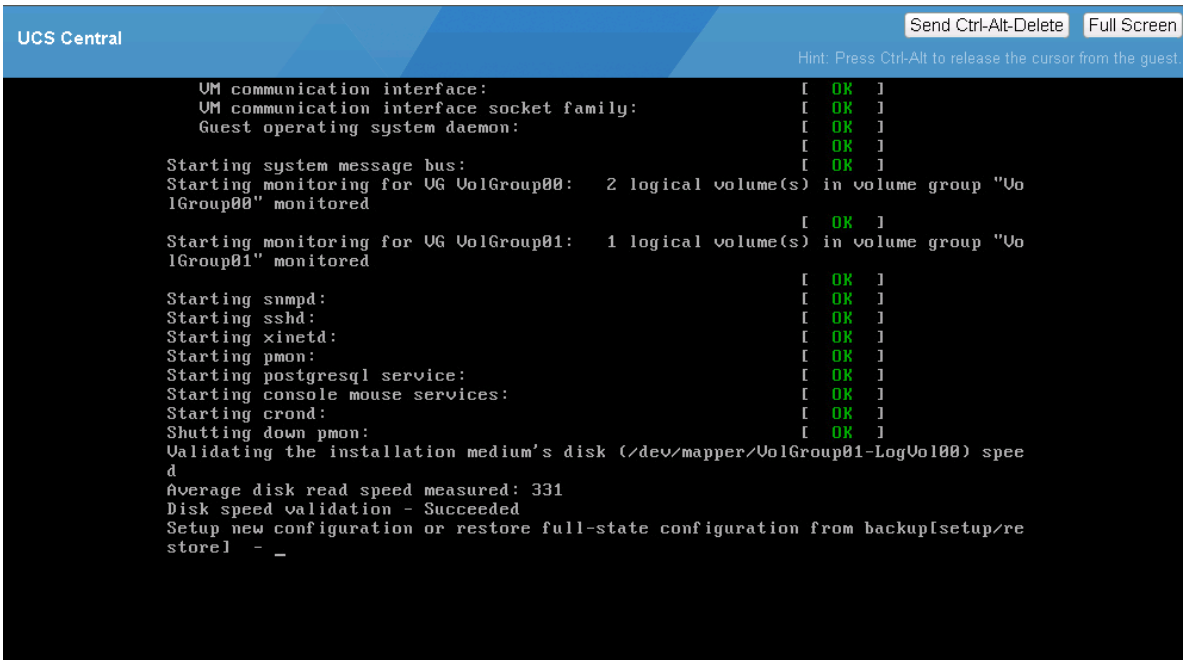
19. Select <<var_vc_ucscentral_vm_name>>.

20. Click Power on the virtual machine.



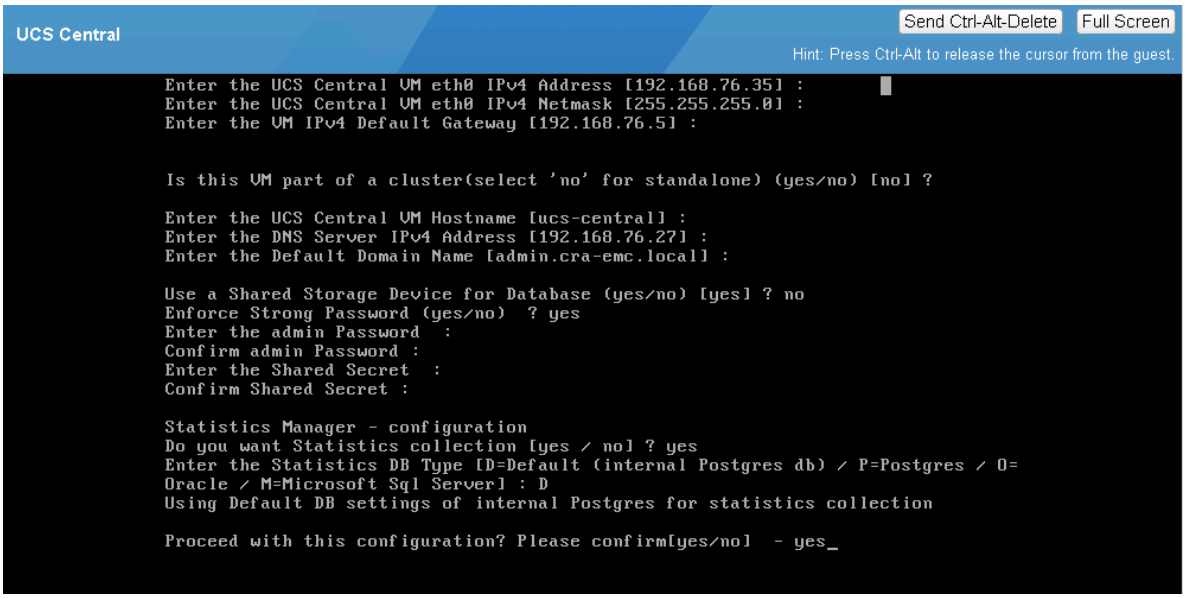

21. Click Actions.

22. Open Console.



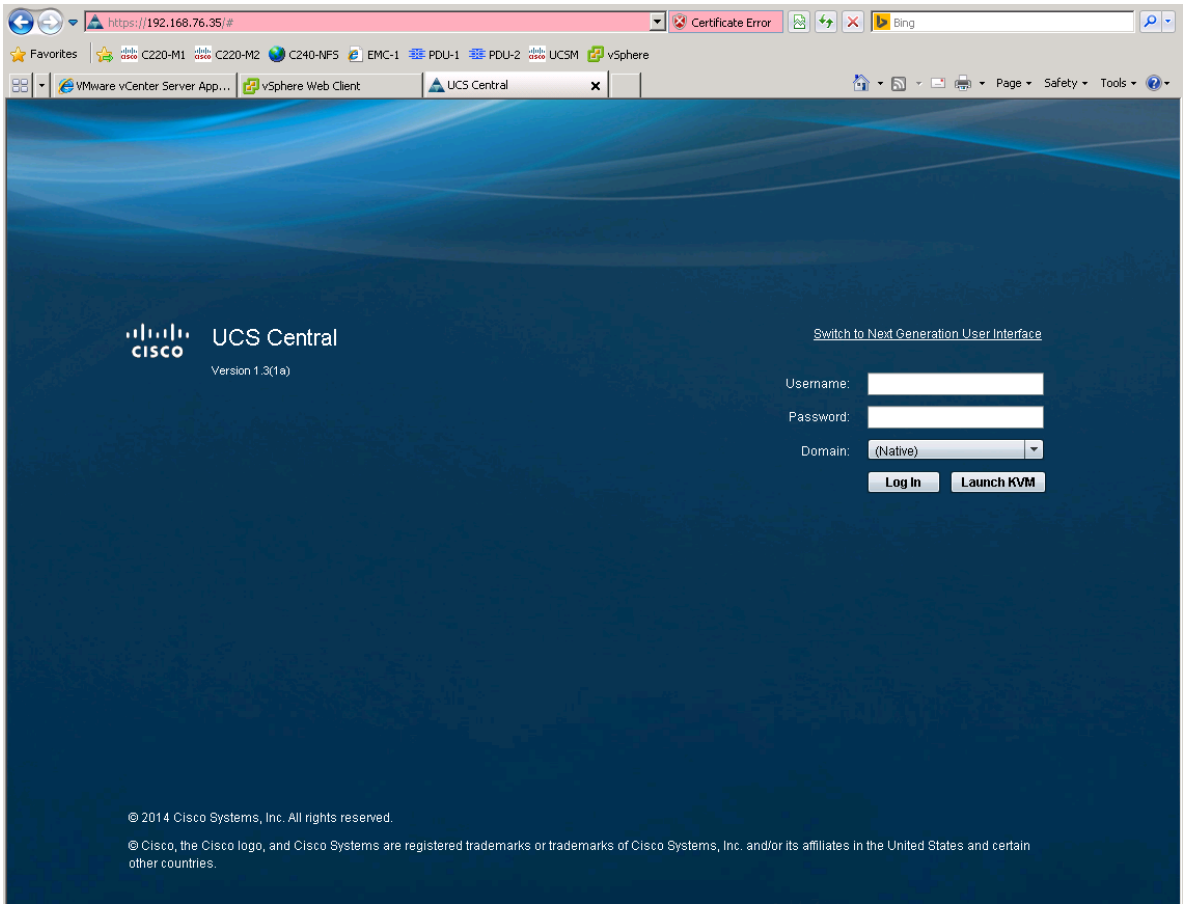

23. Enter setup and press Enter.
24. Enter <<var_ucsc_ip>> for the IP Address.
25. Enter <<var_mgmt_netmask>> a for s the netmask.
26. Enter <<var_mgmt_gw>> for the Default Gateway.
27. Enter <<var_ucsc_hostname>> for the hostname.
28. Enter <<var_nameserver_ip>> for the DNS server.
29. Enter <<var_mgmt_dns_domain_name>> for the default domain name.
30. Enter no since no shared storage is used.
31. Enter yes for strong password.
32. Enter <<var_mgmt_passwd>> for the password and confirm it.
33. Enter <<var_shared_secret>> for the shared secret and confirm it.
34. Enter yes to collect statistics.
35. Enter D for default database.
36. Enter yes and press Enter.

The setup will configure the system and reboot the virtual machine.

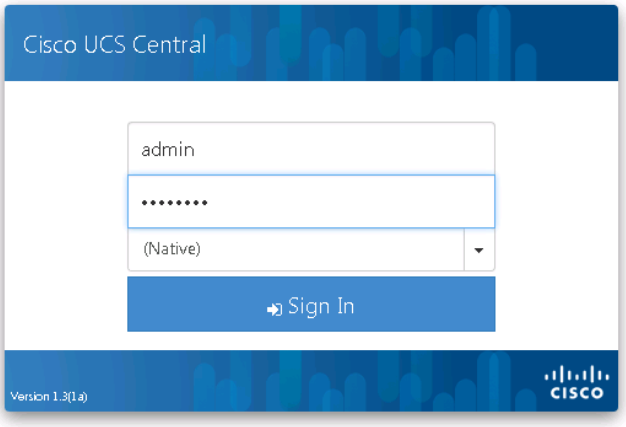



37. Open http:// <<var_ucsc_ip>>/ with a web browser.

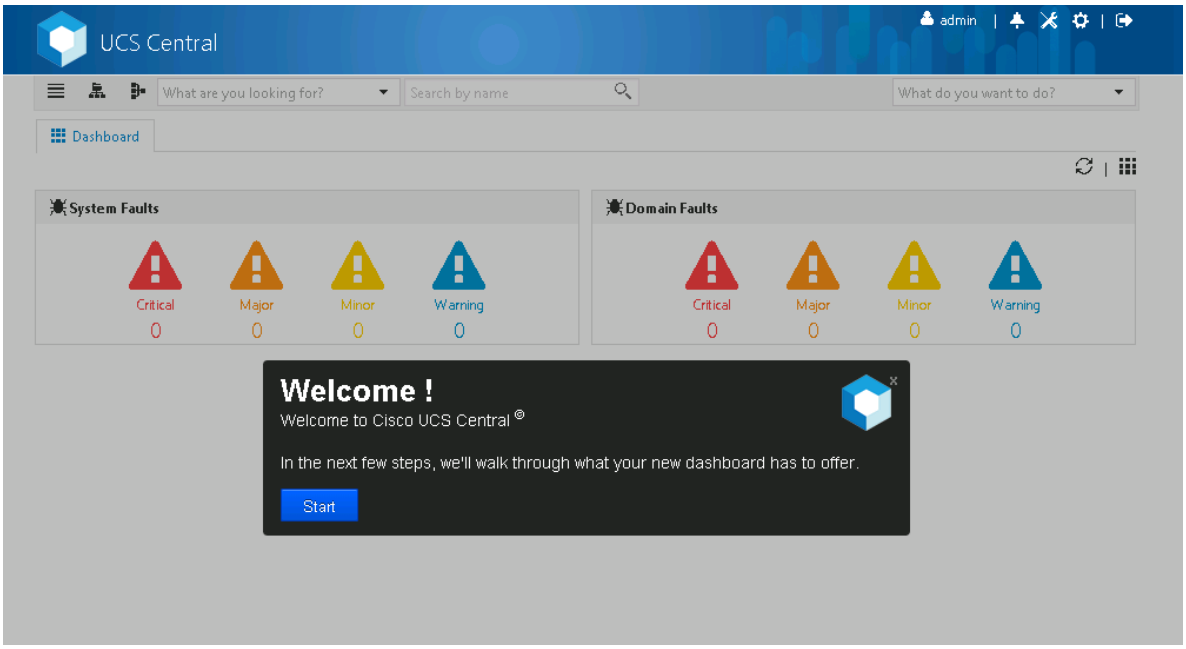
38. Click Switch to Next Generation User Interface.



39. Enter admin as User.
40. Enter <<var_mgmt_passwd>> as Password.
41. Click Sign In.

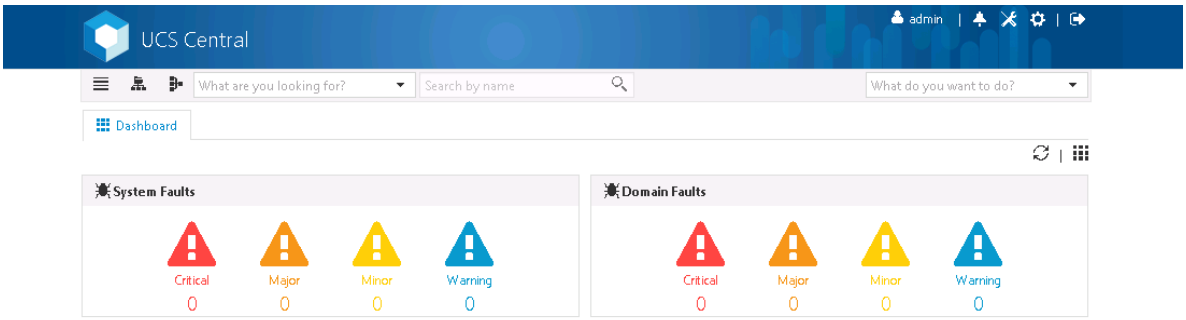



The Welcome Message displays to guide you through the new GUI.



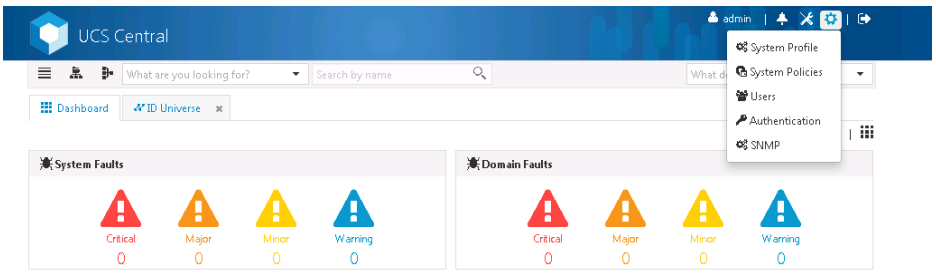

Take the short tour to see where to find information.

After the tour is finished the Cisco UCS Central Dashboard displays.



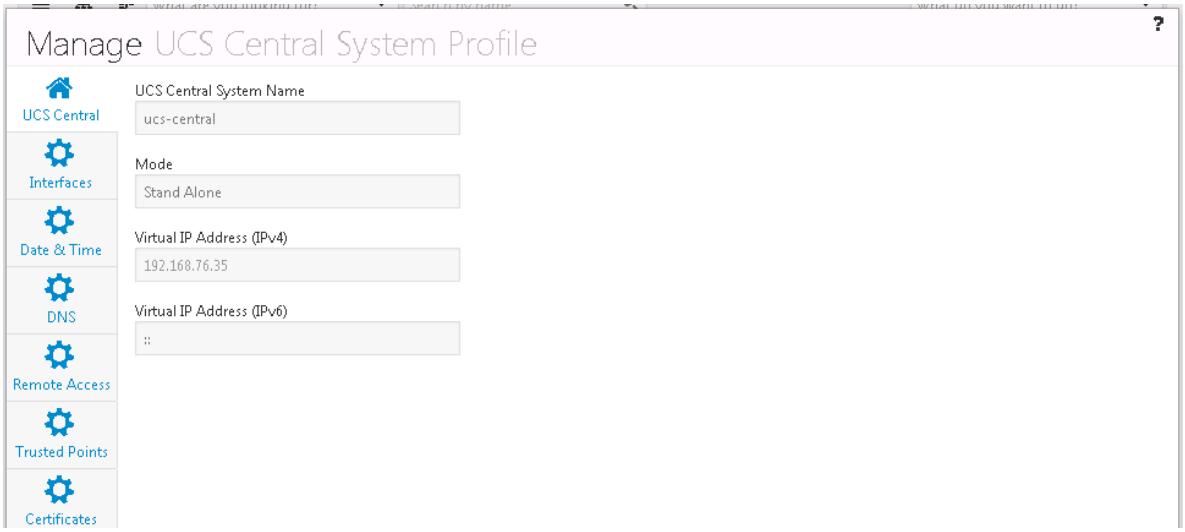

42. Click the Symbol on the top right.

43. Click System Profile.



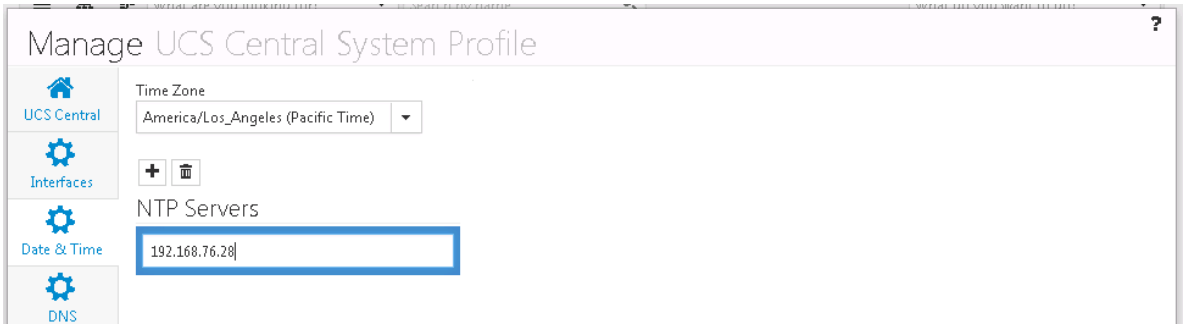

In the initial screen of the Manage UCS Central System Profile Window the configured parameters are displayed.

44. Click Date & Time.

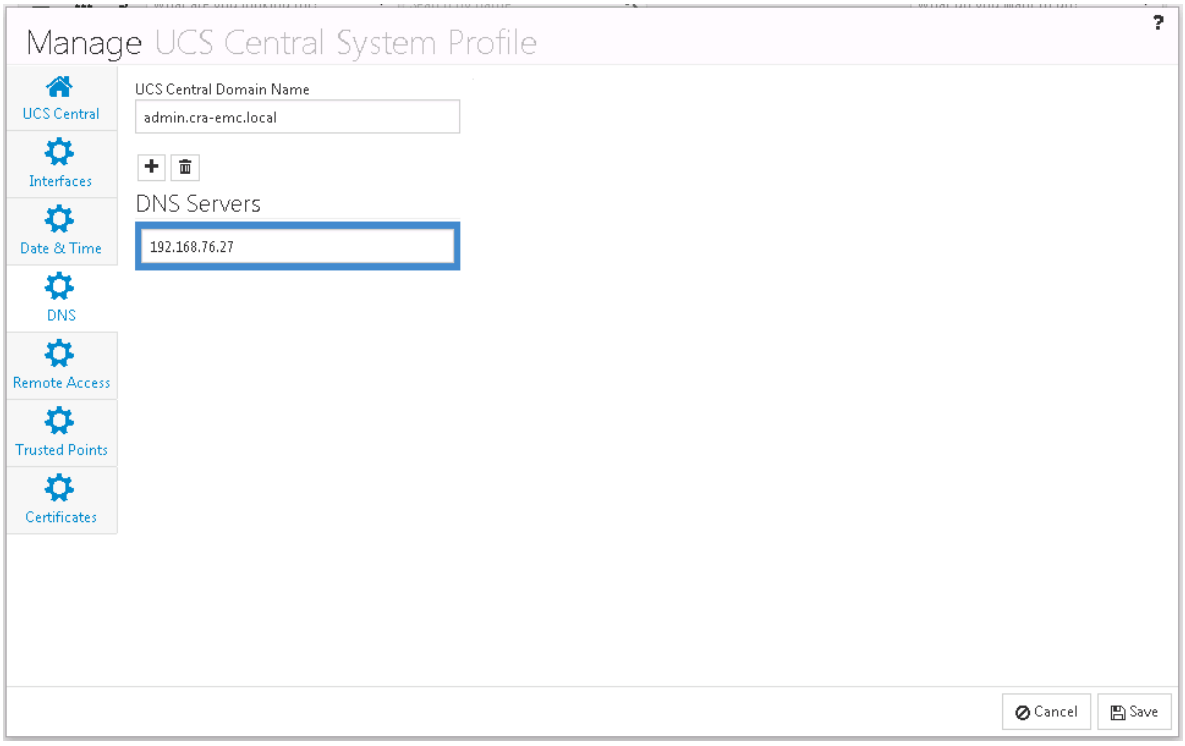



45. Select the Time Zone from the drop-down menu.

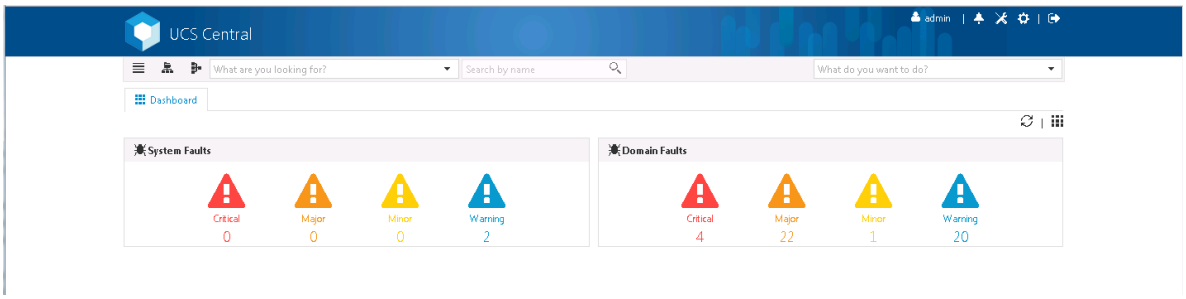
46. Click the + Sign to add a NTP server.
47. Enter <<var_global_ntp_server_ip>> in the highlighted Field.
48. Click DNS




49. Enter <<var_mgmt_dns_domain_name>> for the UCS Central Domain Name.
50. Click the + sign.
51. Enter <<var_nameserver_ip>> in the highlighted field.
52. Click Save.



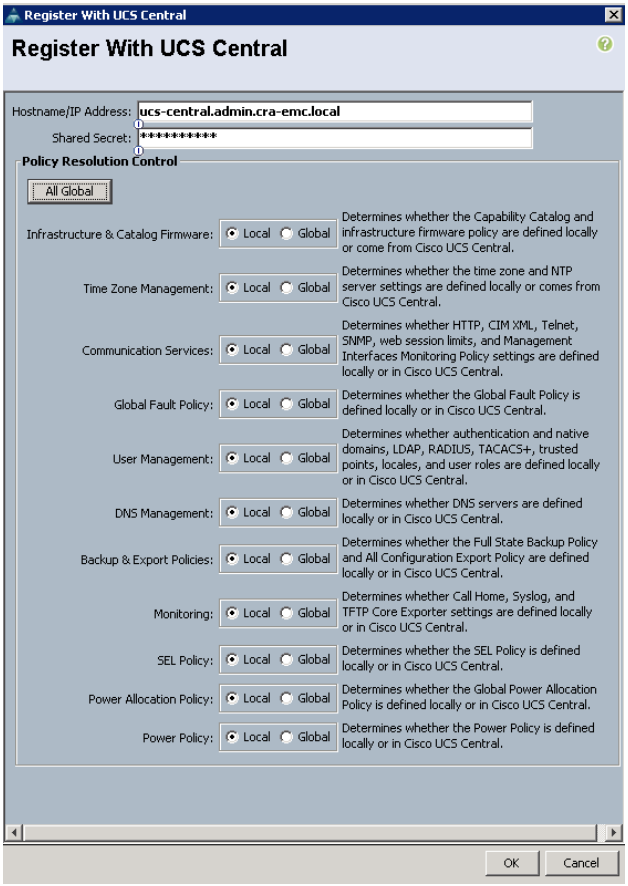

The Cisco UCS Central Dash Board appears. The registration of the Cisco UCS will be part of the Cisco UCS installation and configuration chapter later in this document.



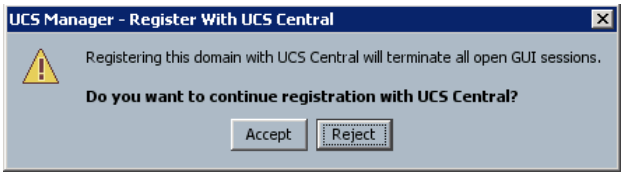

## Register Cisco UCS Manager with Cisco UCS Central

Using Cisco UCS Central is not mandatory to build and manage this Cisco Data Center Reference Architecture but it helps you to manage multiple Cisco UCS domains installed in different locations from a single point. You can register the Cisco UCS now with Cisco UCS Central or you can do it later after Cisco UCS Central is installed. To register Cisco UCS Manager, complete the following steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select Communication Management > UCS Central.
3. Click Register With UCS Central.
4. Enter <<var_ucsc_ip>> as the Hostname/IP Address.
5. Enter <<var_shared_secret>> as the Shared Secret.
6. Keep all Policy Resolution Control selections on Local.
7. Click OK.



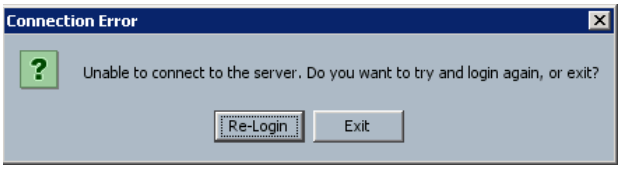

8. Click Accept.




9. Click OK.

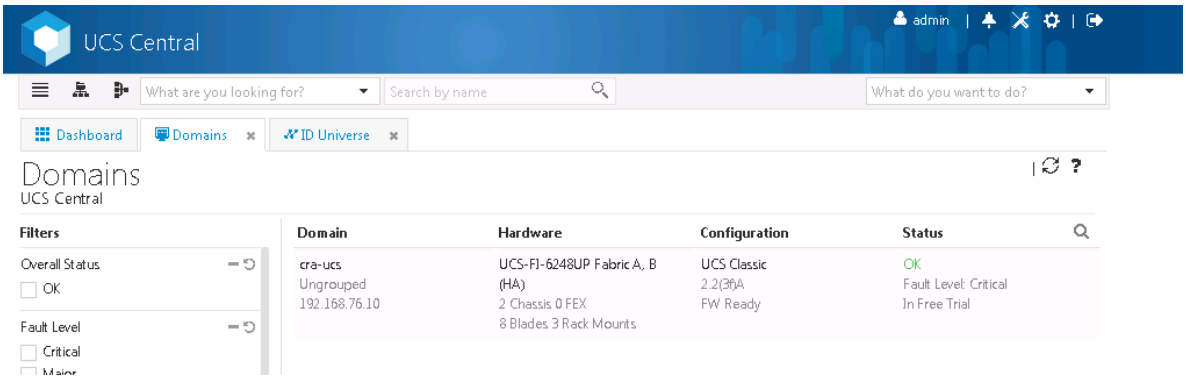
The Cisco UCS Manager Session will be closed as part of the registration process.

10. Click Exit.

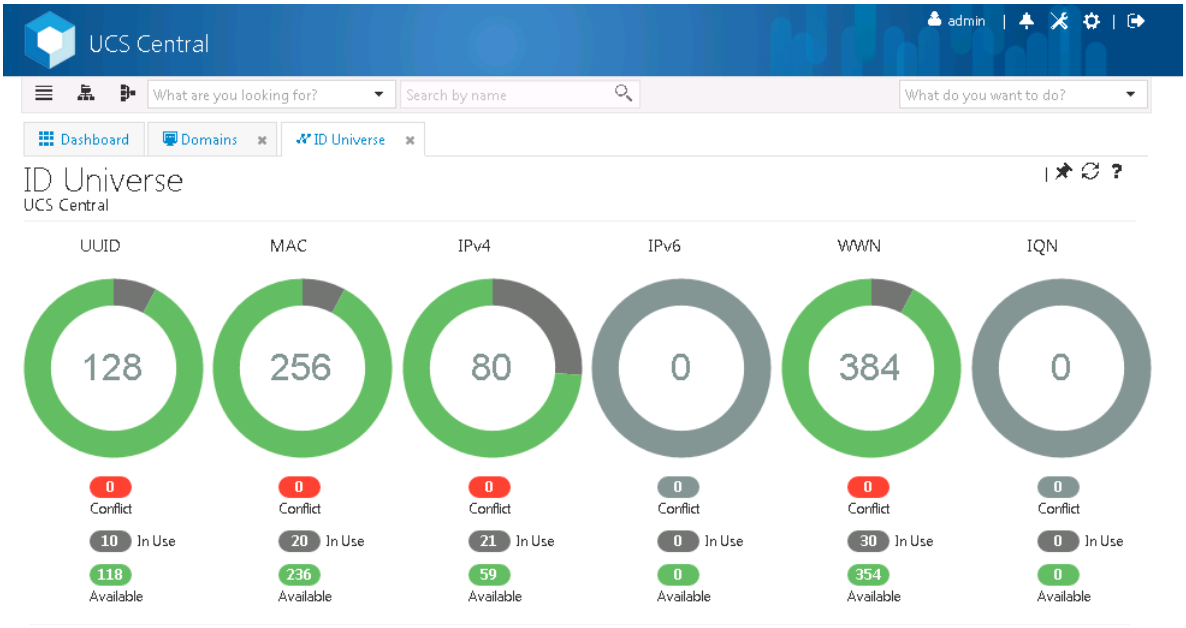



11. Log in to the UCS Central system to check the registration.

12. In the Domains View, the registered UCS Domain must be listed with the Status OK.




13. In the ID Universe you will see the information about Configured and Used IDs.




## Cisco UCS Platform Emulator

The Cisco UCS Platform Emulator can help you to plan and test configuration changes in the deployed landscape. It is a good practice to test changes in the Cisco UCS Platform Emulator, after that validate the changes as documented on a physical Cisco UCS domain that is not used to run productive systems. After the validation is done, deploy the changes on the productive systems. The Cisco UCS Platform Emulator works together with the Cisco UCS Central and can simulate changes on Global Policies and Pools.

The Cisco UCS Platform Emulator OVA file can be loaded from the Cisco web site.

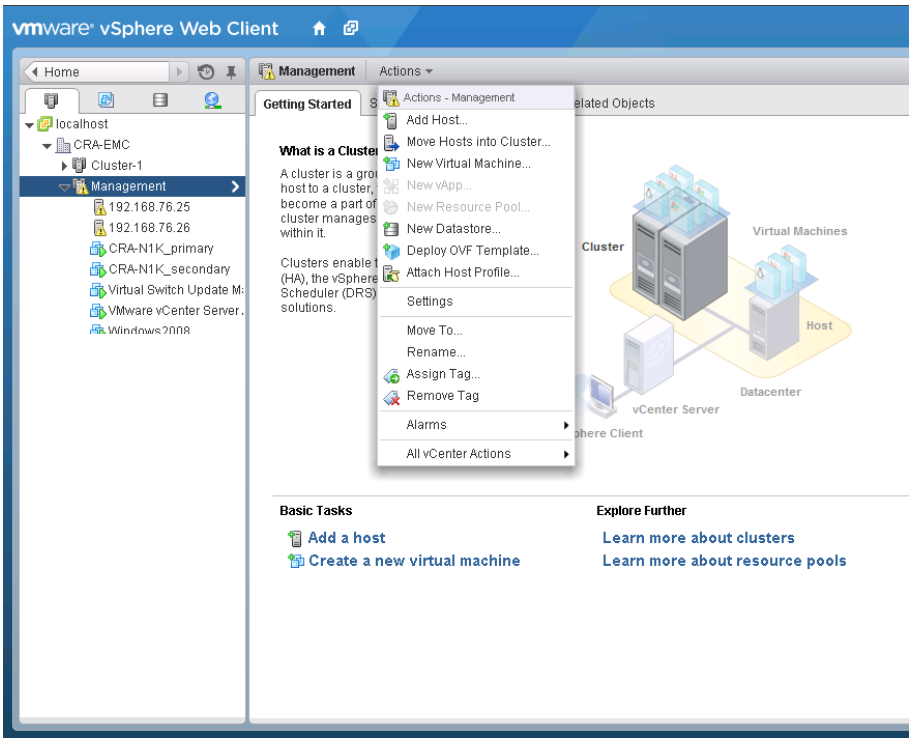
Table 38 list the information to setup the Cisco UCS Platform Emulator in this Cisco UCS Integrated Infrastructure:

**Table 38 Information to Setup Cisco UCS Central**

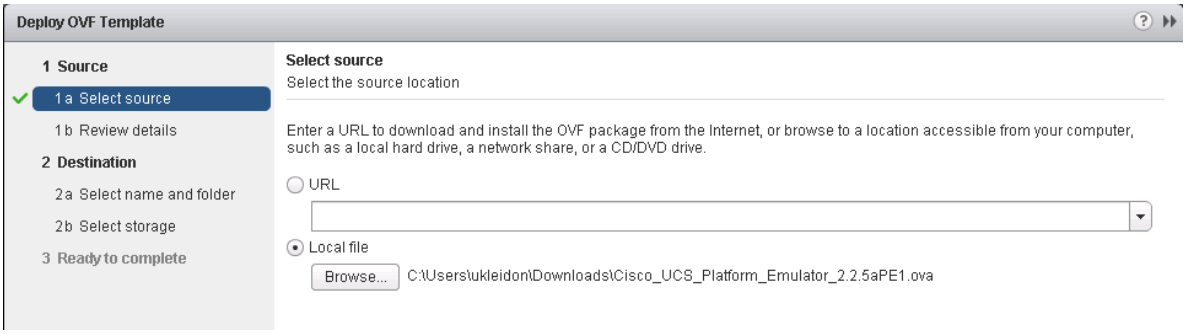
| Name | Variable |
|---|---|
| | <<var_vc_mgmt_cluster_name>> |
| | <<var_vc_ucspe_vm_name>> |
| | <<var_vc_datacenter_name>> |
| | <<var_vc_mgmt_datastore_1>> |
| | <<var_esx_mgmt_network>> |
| | <<var_ucspe_ip>> |
| | <<var_mgmt_netmask>> |
| | <<var_mgmt_gw>> |
| | <<var_ucspe_hostname>> |
| | <<var_nameserver_ip>> |
| | <<var_mgmt_dns_domain_name>> |
| | <<var_mgmt_passwd>> |
| | <<var_shared_secret>> |

To deploy and configure Cisco UCS Central, complete the following high-level steps:

1. Log in to the vSphere Web Client.
2. Click Hosts and Clusters in the Home Screen.
3. Click the <<var_vc_mgmt_cluster_name>>.
4. Click Actions and select Deploy OVF Template.




5. Click Browse and select the Cisco UCS Platform Emulator OVA file.
6. Click Next

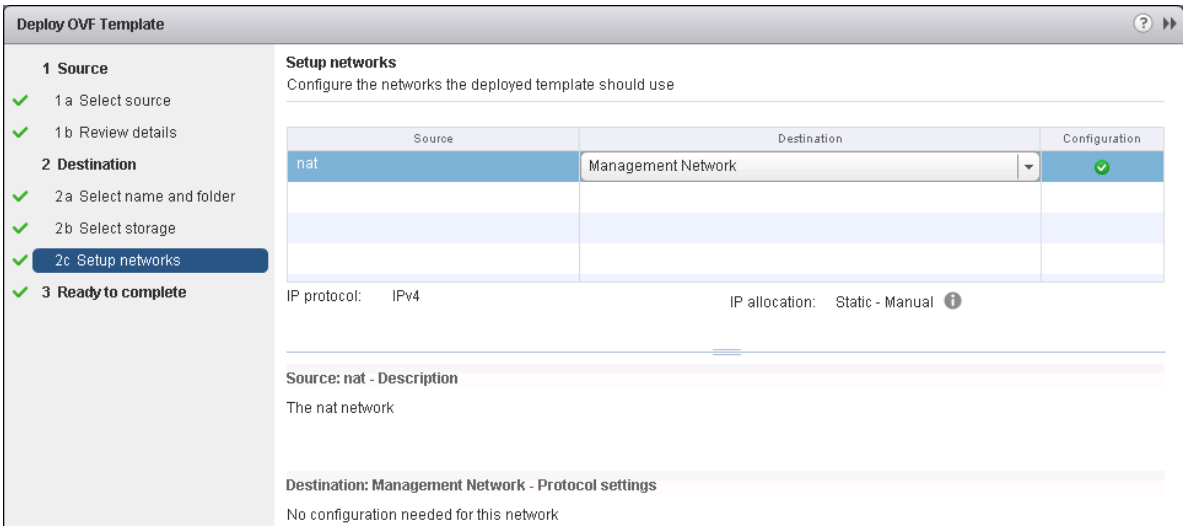



7. Review the Details.
8. Click Next.
9. Enter <<var_vc_ucspe_vm_name>> as the name.
10. Select <<var_vc_datacenter_name>> as destination.
11. Click Next.
12. Select <<var_vc_mgmt_datastore_1>> as the Storage.

13. Click Next.

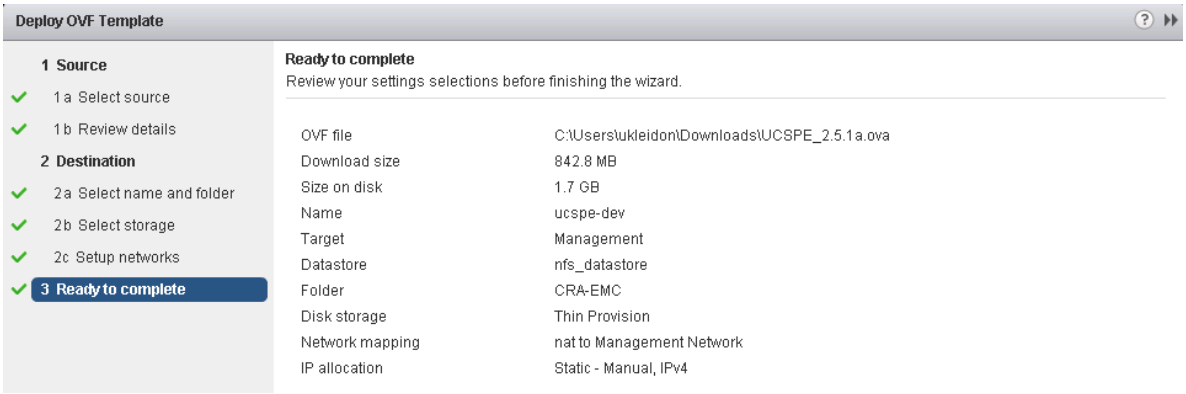
14. Select <<var_esx_mgmt_network>> as the Destination for VM Network.

15. Click Next.




16. Review the information.

17. Click Finish.

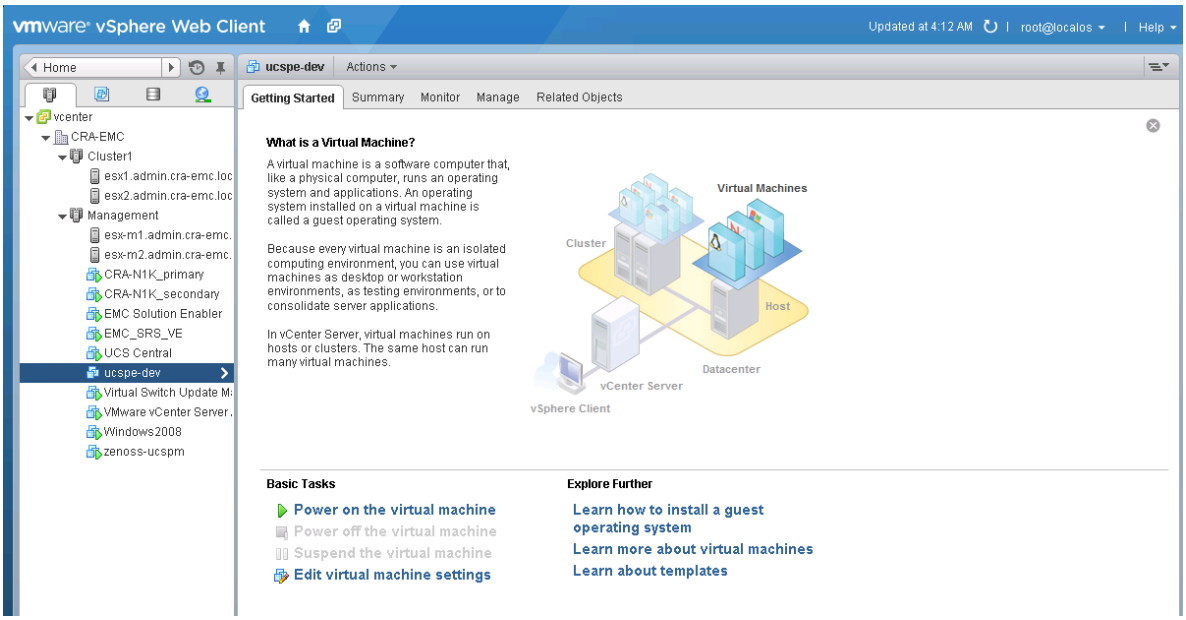



18. Go to the vCenter Home screen.

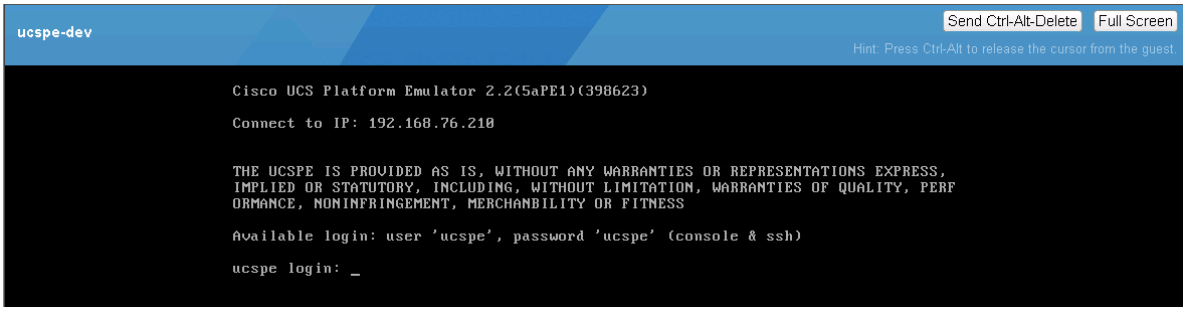
19. Click Hosts and Clusters.

20. Select <<var_vc_ucspe_vm_name>>.

21. Click Power on the Virtual Machine.



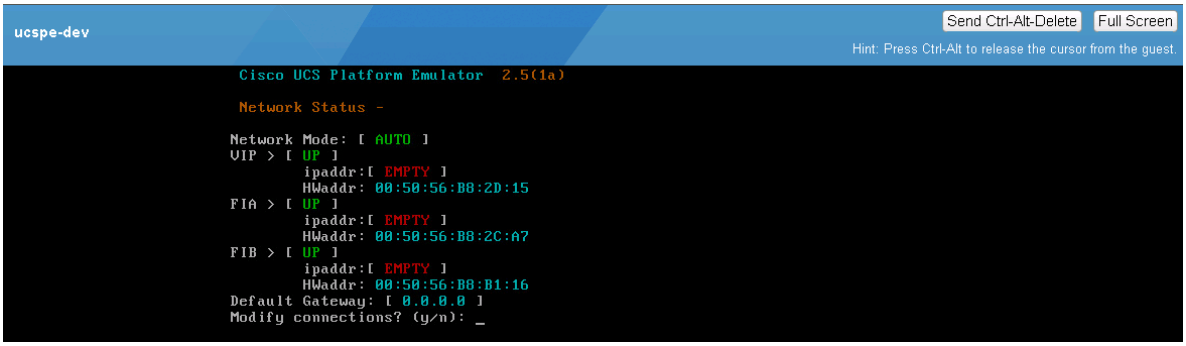

22. Click Actions.




23. Log in to the system with the user and password shown on the screen.

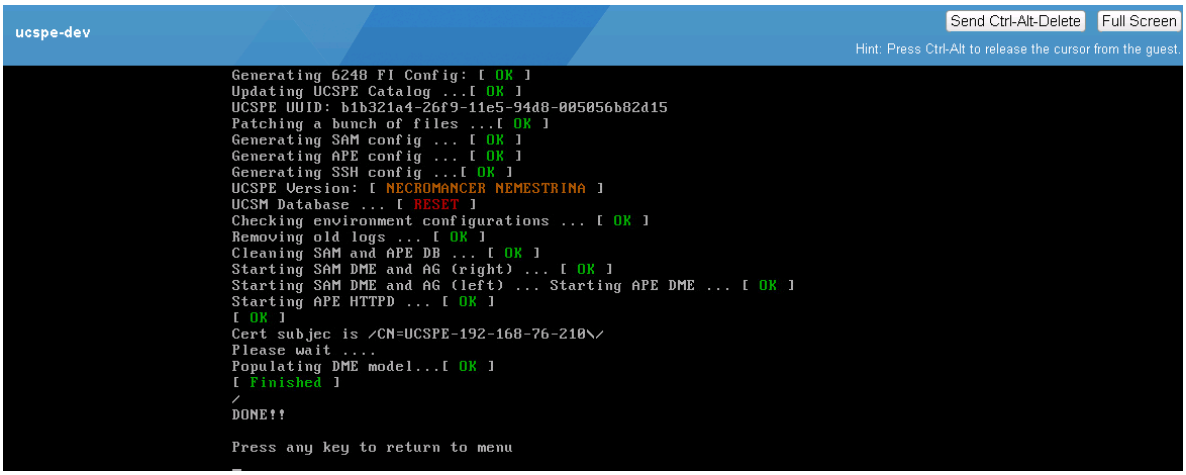
24. Enter n and press Enter.

25. Enter y and press Enter.




26. Enter c for custom and press Enter.

27. Enter <<var_ucspe_vip>> for the VIP Address.
28. Enter <<var_mgmt_netmask>> for the VIP Netmask.
29. Enter <<var_ucspe_fia_ip>> for the FIA Address.
30. Enter <<var_mgmt_netmask>> for the FIA Netmask.
31. Enter <<var_ucspe_fib_ip>> for the FIB Address.
32. Enter <<var_mgmt_netmask>> for the FIB Netmask.
33. Enter <<var_mgmt_gw>> for the Gateway IP.
34. Press Enter to return to the menu.

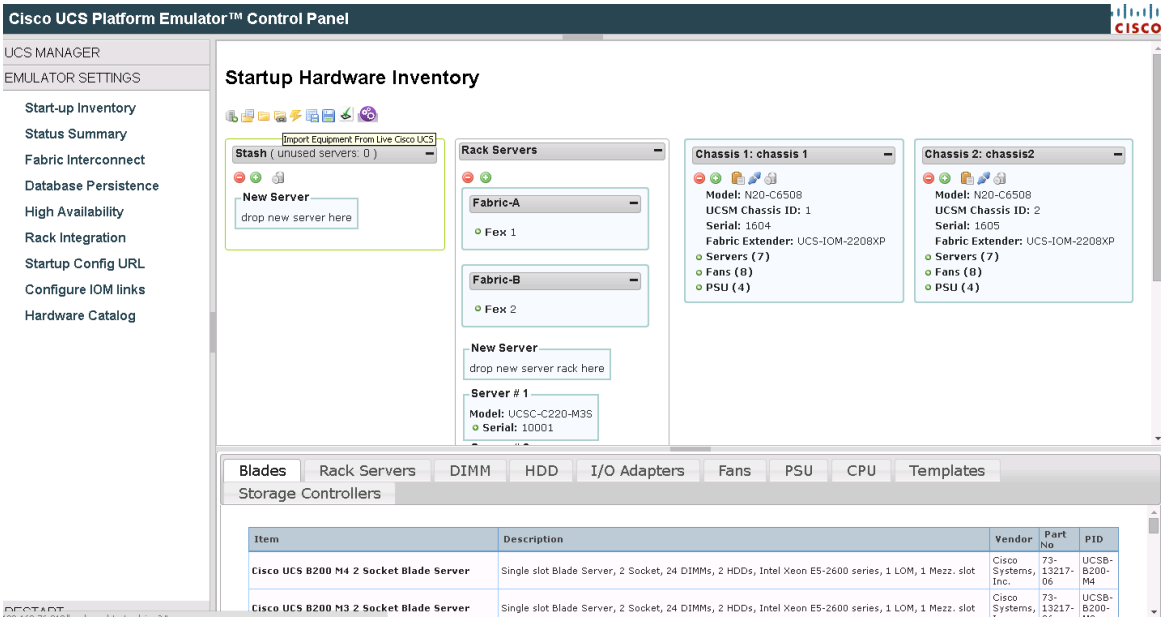



35. Enter x and press Enter.
36. Enter y and press Enter to confirm to logout.
37. Open http:// <<var_ucspe_vip>>/ with a web browser.




38. Click Emulator Settings.

39. Click  Import Equipment From Live Cisco UCS.



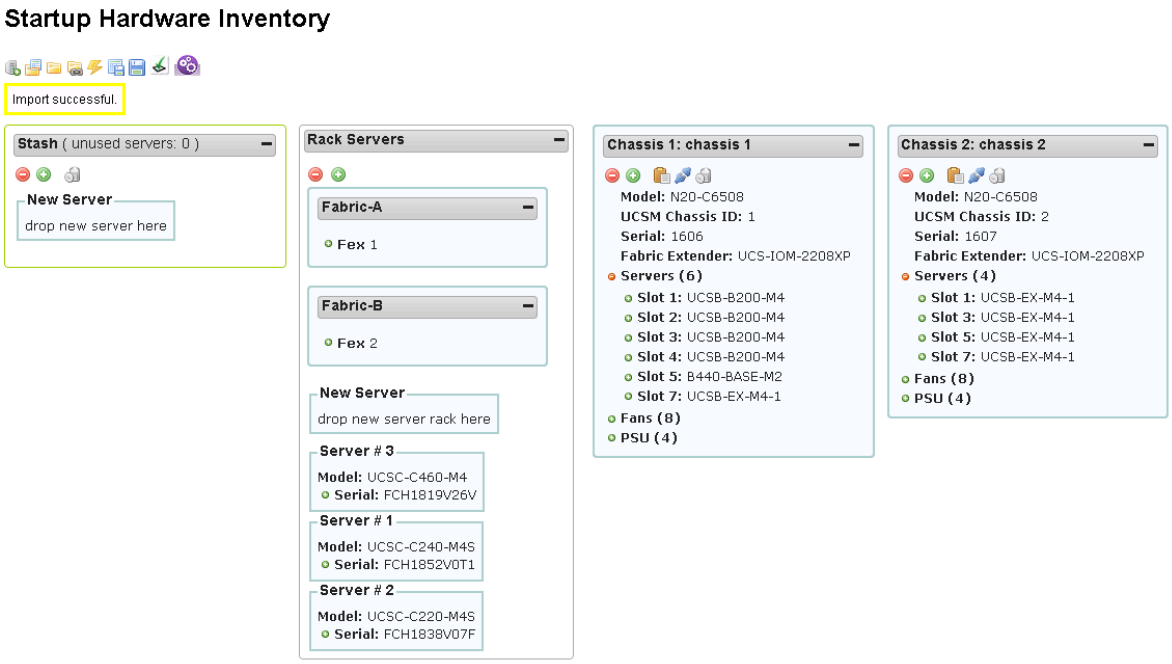

40. Enter the <<var_ucs_cluster_ip>> as the Cisco UCS Server http address.

41. Enter admin as User and <<var_mgmt_passwd>> as the Password.

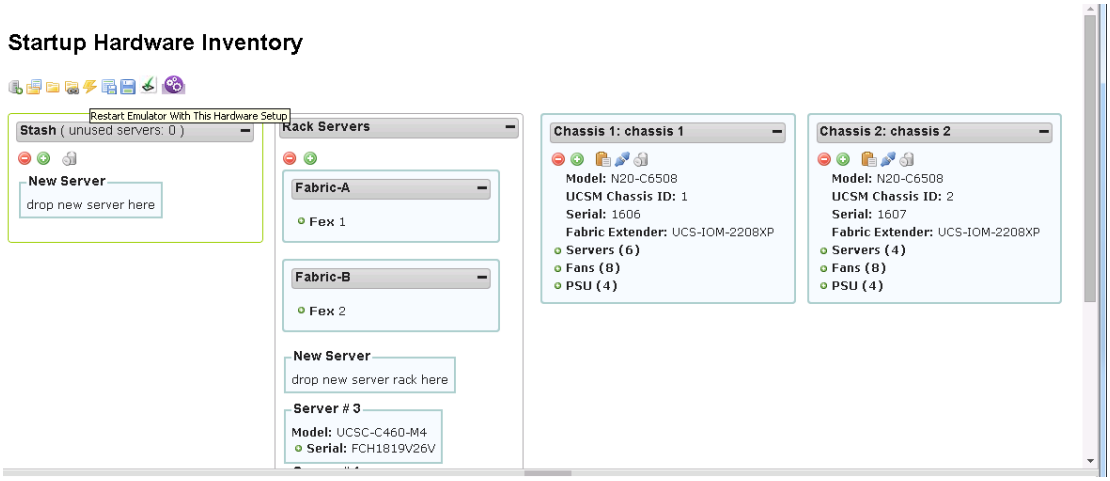
42. Click Load.




The Cisco UCS Platform Emulator imports the configuration form the Live System.




43. Click  Restart Emulator with This Hardware Setup.




44. Select the Radio button for Yes.

45. Click Restart UCS Emulator with Current Settings.






The Cisco UCS PE undergoes a restart, this may take several minutes. Monitor the status in the Virtual Machine console.

46. Return to the UCS Manager tab > UCS Manager Home on the left side.

47. Click Launch UCS Manager.

48. Log in to UCS Manager GUI with user admin and <<var_mgmt_passwd>>.

49. Make sure the Hardware components are imported.

50. Import an All Configuration file from the Live Cisco UCS system.

# Appendix–Solution Variables Data Sheet

Before starting the configuration, gather some specific configuration information. The following tables provide information about assembling the required network and host address, numbering, and naming information. This worksheet can also be used as a “leave behind” document for future reference.

**Table 39 Common Server Information**

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| Management POD | | |
| CISCO Nexus3000 | | |
| <<var_management_vlan_id>> | Infrastructure Management Network VLAN ID | 76 |
| <<var_admin_vlan_id>> | Global Administration Network VLAN ID | 177 |
| <<var_backup_vlan_id>> | Global Backup Network | 199 |
| <<var_n1k_control_vlan_id>> | Cisco Nexus1000V Control Network VLAN ID | 2121 |
| <<var_mgmt_vmotion_vlan_id>> | VMware Vmotion Network VLAN ID within the Management POD | 1031 |
| <<var_mgmt_esx_nfs_vlan_id>> | VMware ESX Storage access Network VLAN ID within the Management POD | 1034 |
| <<var_mgmt_netmaks>> | Management network Netmask | 255.255.255.0 |
| <<var_mgmt_gw>> | Management network default Gateway | 192.168.76.5 |
| <<var_mgmt_passwd>> | Global default administrative password | ucs4sap! |
| <<var_global_ntp_server_ip>> | NTP server IP address | 192.168.76.28 |
| <<var_mgmt_dns_domain_name>> | DNS domain name | admin.cra-emc.local |
| <<var_nameserver_ip>> | DNS server 1 IP Address | 192.168.76.27 |
| <<var_nameserver2_ip>> | DNS server 2 IP Address | |
| <<var_snmp_ro_string>> | SNMP Community String for Read Only access | monitor |
| <<var_nexus_m1_hostname> | Nexus 3500 M1 Hostname | cra-n3-m1 |
| <<var_nexus_m1_mgmt0_ip>> | Nexus 3500 M1 IP address for mgmt0 | 192.168.177.1 |
| <<var_nexus_m2_hostname> | Nexus 3500 M2 Hostname | cra-n3-m2 |
| <<var_nexus_m2_mgmt0_ip>> | Nexus 3500 M2 IP address for mgmt0 | 192.168.177.2 |
| <<var_mgmt_nexus_vpc_domain_id>> | Virtual Port Channel Domain ID for N9Ks M1 and M2 | 139 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_nexus_m1_mgmt_ip>> | Nexus 3500 M1 IP address for HRSP option | 192.168.76.251 |
| <<var_nexus_m2_mgmt_ip>> | Nexus 3500 M1 IP address for HRSP option | 192.168.76.252 |
| <<var_nexus_hsrp_id>> | HSRP ID for the Nexus 3500 switches | 23 |
| <<var_nexus_hsrp_mgmt_ip>> | Nexus 3500 HSRP Virtual IP address | 192.168.76.5 |
| | | |
| CISCO ISR | | |
| <<var_mgmt_isr_hostname>> | Hostname of the Cisco 2911 ISR | cra-emc-2911 |
| <<var_mgmt_isr_ip>> | Management IP address for C2911 ISR | 192.168.76.6 |
| | | |
| CISCO Management Server | | |
| <<var_mgmt_c220-m1_cimc_ip>> | IP address Cisco UCS C220 M1 CIMC Interface | 192.168.76.20 |
| <<var_mgmt_c220-m2_cimc_ip>> | IP address Cisco UCS C220 M2 CIMC Interface | 192.168.76.21 |
| | | |
| EMC VNX | | |
| <<var_mgmt_vnx_cs1_ip>> | Infrastructure Management IP for EMC VNX5400-M01 Control Station | 192.168.76.111 |
| <<var_mgmt_vnx_cs1_hostname>> | Hostname for EMC VNX5400-M01 Control Station | mgmt-vnx1-cs1 |
| <<var_mgmt_vnx_spa_ip>> | IP address for EMC VNX5400-M1 Storage Processor A | 192.168.76.112 |
| <<var_mgmt_vnx_spa_hostname>> | Hostname for EMC VNX5400-M1 Storage Processor A | mgmt-vnx1-spa |
| <<var_mgmt_vnx_spb_ip>> | IP address for EMC VNX5400-M1 Storage Processor B | 192.168.76.113 |
| <<var_mgmt_vnx_spb_hostname>> | Hostname for EMC VNX5400-M1 Storage Processor B | mgmt-vnx1-spb |
| <<var_mgmt_storage_pool_name>> | Storage Pool Name on VNX1 for the initial Setup | Pool3 |
| <<var_mgmt_number_disks>> | Number of Disks used for Storage Pool | 5 |
| <<var_mgmt_lun_size>> | LUN size used for the Datastore 1 | 800GB |
| <<var_mgmt_number_luns>> | Number of LUNs | 20 |
| <<var_mgmt_vnx_user>> | Default Admin User on the EMC | sysadmin |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| | VNX | |
| <<var_mgmt_vnx_passwd>> | Password for the Admin User | sysadmin |
| <<var_mgmt_vnx_dm2_ip>> | DataMover IP Address within the MGMT-ESX-NFS-Network | 172.31.251.2 |
| <<var_mgmt_vnx_dm2_fsn>> | Fail Save Network or Trunk with LACP !!! vPC on N9K required for LACP | |
| <<var_mgmt_nfs_volume_path>> | Name of the NFS share for ESX datastore | datastore01 |
| <<var_mgmt_vnx_lacp_name>> | Name of the LACP device | lacp-1 |
| <<var_mgmt_vnx_if1_name>> | Name of the Network interface for the NFS VLAN | fs1 |
| <<var_mgmt_vnx_fs1_name>> | File System Name for NFS Datastore 1 | NFS-DS-1 |
| <<var_mgmt_nfs_volume_path>> | NFS Export Name for Datastore 1 | /NFS-DS-a |
| <<var_mgmt_fs_size>> | Size of the File System for NFS Datastore 1 | 5 TB |
| <<var_mgmt_fs_max_capa>> | Maximum Capacity of Files Sys-tem Datastore 1 | 7340032 |
| | | |
| ESX HOSTS | | |
| <<var_mgmt_esx1_ip>> | ESX-1 IP Addess in the Admin Network | 192.168.76.26 |
| <<var_mgmt_esx1_fqdn>> | Full Qualified Domain name of ESX host 1 | esx-m1.cra-emc.local |
| <<var_mgmt_esx1_nfs_ip>> | ESX-1 IP Addess in the MGMT-ESX-NFS-Network | 172.31.249.26 |
| <<var_mgmt_esx1_vmotion_ip>> | ESX-1 IP Addess in the MGMT-ESX-vMotion-Network | 172.31.251.26 |
| <<var_mgmt_esx2_ip>> | ESX-2 IP Addess in the Admin Network | 192.168.76.25 |
| <<var_mgmt_esx2_fqdn>> | Full Qualified Domain name of ESX host 2 | esx-m2.cra-emc.local |
| <<var_mgmt_esx2_nfs_ip>> | ESX-2 IP Addess in the MGMT-ESX-NFS-Network | 172.31.249.25 |
| <<var_mgmt_esx2_vmotion_ip>> | ESX-2 IP Addess in the MGMT-ESX-vMotion-Network | 172.31.251.25 |
| <<var_vmkern_mgmt_name>> | VMKernel Management Network Name | VMKernel-Mgmt |
| <<var_esx_mgmt_network>> | Management Network Name for <<var_mgmt_vlan_id>> | Management Network |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_esx_vmkernel_nfs>> | NFS Network Name for <<var_mgmt_esx_nfs_vlan_id>> | VMKernel-NFS |
| <<var_esx_vmkernel_vmotion>> | VMKernel Vmotion Network Name | VMKernel-vMotion |
| <<var_n1k_control_network>> | Nexus1000V Control Network Name | N1Kv_Control |
| <<var_vc_mgmt_datastore_1>> | Name of the first Datastore on ESXi | nfs_datastore |
| | | |
| VCENTER SERVER | | |
| <<var_vc_ip_addr>> | Virtual Center Server IP address | 192.168.76.24 |
| <<var_vc_hostname>> | Virtual Center Server Hostname | vcenter |
| <<var_vc_datacenter_name>> | Name of the first DataCenter in Virtual Center | CRA-EMC |
| <<var_vc_cluster1_name>> | Name of the first Host Cluster for the managed system | Cluster1 |
| <<var_vc_mgmt_cluster_name>> | Name of the Host Cluster for the Management Hosts | Management |
| | | |
| Cisco Nexus1000V VSM | | |
| <<var_n1k_vsum_ip>> | Cisco Virtual Switch Update Manager IP Address | 192.168.76.30 |
| <<var_n1k_switch_name>> | Nexus1000V Virtual Switch Name | CRA-N1K |
| <<var_n1k_domain_id>> | Nexus1000V Switch Domain ID | 393 |
| <<var_n1k_vsm_ip>> | Nexus1000V Virtual Switch Supervisor Module IP Address | 192.168.76.31 |
| <<var_n1k_passwd>> | Nexus1000V Admin User Password | SAPhana10 |
| <<var_vc_mgmt_cluster_name>> | Name of the Management cluster within the Datacenter | Management |
| <<var_n1k_control_network>> | Nexus-1000v-Control-Network Name in vCenter | N1Kv_Control |
| <<var_mgmt_network_name>> | Management Network Name in vCenter | Management Network |
| | | |
| EMC Secure Remote Service | | |
| <<var_esx_emcsrs_vm_name>> | EMC Secure Remote Service Virtual Machine Name | EMC_SRS_VE |
| <<var_emcsrs_ip> | EMC Secure Remote Service IP Address | 192.168.76.52 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_emcsrs_hostname>> | EMC Secure Remote Service hostname | emc-srs |
| <<var_emcsrs_admin_name>> | Esrs Web Administrator User Name | admin |
| <<var_emcsrs_admin_passwd>> | Esrs Web Administrator User Name | |
| | | |
| EMC SMIS | | |
| <<var_vc_emc-smis_vm_name>> | Name of the Virtual Machine for EMC SMIS system | EMC_SE801_3 |
| <<var_emc-smis_ip>> | IP Address of the EMC SMIS system | 192.168.76.51 |
| | | |
| Cisco UCS PERFORMANCE MANAGER | | |
| <<var_vc_ucspm_vm_name>> | Name of the Virtual Machine for the Cisco UCS Performance Manager | zenoss-ucspm |
| <<var_ucspm_ip>> | IP Address of the Cisco UCS Performance Manager | 192.168.76.50 |
| | | |
| Cisco UCS-II | | |
| NEXUS 9000 SWITCHES | | |
| <<var_nexus_A_hostname> | Nexus 9000 A hostname | cra-n9k-a |
| <<var_nexus_A_mgmt0_ip>> | Nexus 9000 A Management IP Address | 192.168.76.1 |
| <<var_nexus_B_hostname> | Nexus 9000 B hostname | cra-n9k-b |
| <<var_nexus_B_mgmt0_ip>> | Nexus 9000 B Management IP Address | 192.168.76.2 |
| <<var_nexus_vpc_domain_id>> | Virtual Port Channel Domain ID for N9K A and B | 25 |
| <<var_vmotion_vlan_id>> | VMware Vmotion Network VLAN ID | 2031 |
| <<var_nfs_netmask>> | Netmask of the NFS network | 255.255.255.0 |
| <<var_esx_nfs_vlan_id>> | VMware ESX Storage access Network VLAN ID | 2034 |
| <<var_temp_vlan_id>> | Temporary used VLAN ID | 2 |
| <<var_backup_node01>> | Name of the Backup Destination | backup-01 |
| | | |
| MDS SWITCHES | | |
| <<var_mds_a_ip>> | MDS 9000 A Management IP | 192.168.76.3 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| | Address | |
| <<var_mds_a_name>> | MDS 9000 A hostname | CRA-EMC-A |
| <<var_mds_b_ip>> | MDS 9000 B Management IP Address | 192.168.76.4 |
| <<var_mds_b_name>> | MDS 9000 B hostname | CRA-EMC-B |
| <<var_mds_timezone>> | Time Zone in a format required by the MDS switches | PST -8 0 |
| <<var_fc-pc_a_id>> | Fibre Channel - Port Channel ID for MDS A | 110 |
| <<var_fc-pc_b_id>> | Fibre Channel - Port Channel ID for MDS B | 120 |
| <<var_san_a_id>> | VSAN ID for MDS A | 10 |
| <<var_san_b_id>> | VSAN ID for MDS B | 20 |
| <<var_zone_temp_name>> | Name of Zone Template with multiple paths | zone_templ |
| <<var_zone_temp_1path_name>> | Name of Zone Template with a single paths | zone_temp_1 |
| <<var_zoneset_name> | Name of the Zone Set | EMC-CRA |
| | | |
| Cisco UCS | | |
| <<var_ucs_clustername>> | UCS Domain Cluster Name | cra-ucs |
| <<var_ucsa_mgmt_ip>> | UCS Fabric Interconnect A Management IP Address | 192.168.76.8 |
| <<var_ucs_cluster_ip>> | UCS Manager Cluster IP Address | 192.168.76.10 |
| <<var_ucsb_mgmt_ip>> | UCS Fabric Interconnect B Management IP Address | 192.168.76.9 |
| | | |
| LAN TAB | | |
| <<var_eth_adapter_policy_name>> | Name of the Eth Adapter Policy for SAP HANA Scale-Out | Linux-B460 |
| <<var_ucs_global_mac_pool_name>> | Name of the Global MAC Address Pool | Global_MAC_Pool |
| <<var_ucs_access_mac_pool_name>> | Name of the MAC Address Pool for the Access/Client Network Group | Access_MAC_Pool |
| <<var_ucs_besteffort_policy_name>> | Name of the BestEffort Network Policy | BestEffort |
| <<var_ucs_platinum_policy_name>> | Name of the Platinum Network Policy | Platinum |
| <<var_ucs_gold_policy_name>> | Name of the Gold Network Poli- | Gold |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| | cy | |
| <<var_ucs_silver_policy_name>> | Name of the Silver Network Policy | Silver |
| <<var_ucs_bronze_policy_name>> | Name of the Bronze Network Policy | Bronze |
| <<var_ucs_management_vlan_name>> | Name of the Management VLAN | Global-Mgmt-Network |
| <<var_ucs_temp_vlan_name>> | Name of the Temporary VLAN | Temp-Network |
| <<var_ucs_admin_vlan_name>> | Name of the Global Admin VLAN | Global-Admin-Network |
| <<var_ucs_esx_nfs_vlan_name>> | Name of the NFS VLAN for ESX and other use cases | Global-ESX-NFS-Network |
| <<var_ucs_vmotion_vlan_name>> | Name of the Vmotion VLAN | Global-vMotion-Network |
| <<var_backup_vlan_name>> | Name of the Global Backup VLAN | Global-Backup-Network |
| <<var_ucs_n1k_control_vlan_name>> | Name of the Nexus1000V Control VLAN | Global-N1K-Control-Network |
| <<var_ucs_admin_zone>> | Name of the Network Group for Admin tasks | Admin-Zone |
| <<var_ucs_backup_zone>> | Name of the Network Group for Backup tasks | Backup-Zone |
| <<var_ucs_client_zone>> | Name of the Network Group for Client Access | Client-Zone |
| <<var_ucs_internal_zone>> | Name of the Network Group for HANA internal traffic | Internal-Zone |
| <<var_ucs_replication_zone>> | Name of the Network Group for HANA replication traffic | Replication-Zone |
| <<var_ucs_esx_a_vnic_name>> | Name of the vNIC on Fabric A for ESXi Admin traffic | ESX-A |
| <<var_ucs_esx_b_vnic_name>> | Name of the vNIC on Fabric B for ESXi Admin traffic | ESX-B |
| <<var_ucs_esx_a_appl_vnic_name>> | Name of the vNIC on Fabric A for ESXi Application/VM traffic | ESX-A-Appl |
| <<var_ucs_esx_b_appl_vnic_name>> | Name of the vNIC on Fabric B for ESXi Application/VM traffic | ESX-B-Appl |
| <<var_ucs_esx_lan_connect_policy_name>> | Name of the LAN Connection Policy for ESX server | ESX-LAN |
| SAN TAB | | |
| <<var_ucs_fcpc_a_id>> | Fibre Channel Port Channel ID on Fabric A | 110 |
| <<var_ucs_fcpc_a_name>> | Fibre Channel Port Channel Name on Fabric A | FC-PC110 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_ucs_fcpc_b_id>> | Fibre Channel Port Channel ID on Fabric B | 120 |
| <<var_ucs_fcpc_b_name>> | Fibre Channel Port Channel Name on Fabric B | FC-PC120 |
| <<var_ucs_global_wwnn_pool_name>> | Name of the Global World Wide Node Name Pool | Global_WWNN_Pool |
| <<var_ucs_global_wwpn_a_pool_name>> | Name of the Global World Wide Port Name Pool on Fabric A | Global_WWPN_A_Pool |
| <<var_ucs_global_wwpn_b_pool_name>> | Name of the Global World Wide Port Name Pool on Fabric B | Global_WWPN_B_Pool |
| <<var_ucs_vsan_a_name>> | Name of the VSAN on Fabric A | VSAN10 |
| <<var_vsan_a_id>> | ID of the VSAN on Fabric A | 10 |
| <<var_vsan_a_fcoe_id>> | VLAN ID for FCoE traffic of the VSAN on Fabric A | 10 |
| <<var_ucs_vsan_b_name>> | Name of the VSAN on Fabric B | VSAN20 |
| <<var_vsan_b_id>> | ID of the VSAN on Fabric B | 20 |
| <<var_vsan_b_fcoe_id>> | VLAN ID for FCoE traffic of the VSAN on Fabric B | 20 |
| <<var_ucs_vhba_a_templ_name>> | Name of the vHBA Template on Fabric A | vHBA_A |
| <<var_ucs_vhba_b_templ_name>> | Name of the vHBA Template on Fabric B | vHBA_B |
| <<var_ucs_vhba_1_name>> | Name of the first vHBA in a Service Profile | vHBA1 |
| <<var_ucs_vhba_2_name>> | Name of the second vHBA in a Service Profile | vHBA2 |
| <<var_ucs_vhba_3_name>> | Name of the third vHBA in a Service Profile | vHBA3 |
| <<var_ucs_vhba_4_name>> | Name of the forth vHBA in a Service Profile | vHBA4 |
| <<var_ucs_esx_san_connect_policy_name>> | Name of the SAN Connection Policy for ESX | ESX-VNX |
| <<var_ucs_hana_su_connect_policy_name>> | SAN Connection Policy for SAP HANA Scale-Up | HANA-SU |
| <<var_ucs_hana_so_connect_policy_name>> | SAN Connection Policy for SAP HANA Scale-Out | HANA-SO |
| SERVER TAB | | |
| <<var_ucs_power_cont_policy>> | Name of the Power Control Policy | HANA |
| <<var_ucs_hana_fw_package_name>> | Name of Firmware Package for SAP HANA | HANA |
| <<var_ucs_manager_version>> | UCS Manager Version | 2.2(3c) |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_ucs_hana_bios_policy_name>> | Name of the BIOS Policy for SAP HANA | HANA-BIOS |
| <<var_ucs_esx_bios_policy_name>> | Name of the BIOS Policy for VMware ESX | ESX-BIOS |
| <<var_ucs_sol_profile>> | Name of the Serial Over LAN Profile | SoL-Console |
| <<var_ucs_ipmi_policy>> | Name of the IPMI Policy | HANA-IPMI |
| <<var_ucs_ipmi_user>> | IPMI Admin User Name | sapadm |
| <<var_ucs_ipmi_user_passwd>> | Password for the IPMI Admin User | cisco |
| <<var_ucs_uuid_pool_name>> | Name of the global UUID Pool | Global_UUID_Pool |
| <<var_ucs_hana_server_pool>> | Name of the Server Pool for SAP HANA | HANA-1TB |
| <<var_ucs_hana_server_pool_qual_policy>> | Name of the Server Qualification Policy for SAP HANA | HANA-4890-1TB |
| <<var_ucs_hana_server_pool_policy>> | Name of the Server Pool Policy for SAP HANA | HANA-Pool-Policy |
| <<var_ucs_non-hana_server_pool>> | Name of the Server Pool for Non-SAP HANA Workloads | Non-HANA |
| <<var_ucs_san_boot_policy>> | Name of the Boot Policy for SAN Boot | SAN_BOOT_VNX1 |
| <<var_ucs_esx_template_name>> | Name of the Service Profile Template for Vmware ESX | ESX-Template |
| <<var_ucs_esx_sub-org>> | Name of the UCS Sub-Organization for ESX hosts | ESX |
| <<var_ucs_esx1_sp_name>> | Name of the Service Profile for ESX host 1 | ESX-host1 |
| | | |
| EMC VNX | | |
| <<var_vnx1_name>> | Name of the first VNX in the Solution | VNX8000 |
| <<var_vnx1_cs1_ip>> | IP Address of the Control Station | 192.168.76.11 |
| <<var_vnx1_cs1_hostname>> | Hostname of the Control Station | VNX8000-CS1 |
| <<var_vnx1_spa_ip>> | IP Address of the Storage Processor A | 192.168.76.12 |
| <<var_vnx1_spa_hostname>> | Hostname of the Storage Processor A | VNX8000-SPA |
| <<var_vnx1_spb_ip>> | IP Address of the Storage Processor B | 192.168.76.13 |
| <<var_vnx1_spb_hostname>> | Hostname of the Storage Processor B | VNX8000-SPB |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_vnx1_pool1_name>> | Name of the first Storage pool on VNX1 - for Non-HANA usage | Pool 0 |
| <<var_vnx1_fs-pool1_name>> | Name of the first Storage pool for File on VNX1 - for Non-HANA usage | Pool 1 |
| <<var_vnx1_lacp_dev_name>> | Name of the LACP Device for NFS traffic | lacp-1 |
| <<var_vnx1_dm2_nfs_ip>> | IP Address of Datamover2 on the NFS Network | 172.30.113.11 |
| <<var_nfs_netmask>> | Netmask of the NFS Network | 255.255.255.0 |
| <<var_vnx1_fs1_name>> | Name of the first File System on VNX1 | FS_Software |
| <<var_vnx1_fs1_size>> | Size of the Filesystem in Mega-byte | 1024000 |
| <<var_vnx1_nfs1_name>> | Name of the NFS share for the first File System | /FS_Software |
| <<var_vnx1_dm2_mgmt_ip>> | IP Address of Datamover2 on the Management Network | 192.168.76.99 |
| <<var_vnx1_dm2_mgmt_name>> | Name of the Interface for the Management Network | 192-168-76-99 |
| <<var_vnx1_cifs_workgroup>> | Name of the CIFS Workgroup if required | workgroup |
| <<var_vnx1_netbios_name>> | NetBIOS Name of VNX1 | CRA-VNX1 |
| <<var_vnx1_cifs_share1_name>> | Name of the CIFS share for File System 1 | FS_Software |
| | | |
| ESX HOSTS | | |
| | | |
| <<var_esx1_fqdn>> | Full Qualified Domain Name of ESX host 1 | esx1.admin.cra-emc.local |
| <<var_esx1_ip>> | Management Network IP Ad-dress of ESX host 1 | 192.168.76.100 |
| <<var_esx2_fqdn>> | Full Qualified Domain Name of ESX host 2 | esx2.admin.cra-emc.local |
| <<var_esx2_ip>> | Management Network IP Ad-dress of ESX host 1 | 192.168.76.101 |
| <<var_esx1_nfs_ip>> | NFS Network IP Address of ESX host 1 | 172.30.113.100 |
| <<var_nfs_netmask>> | Netmask of the NFS Network | 255.255.255.0 |
| <<var_esx1_vmotion_ip>> | VMotion Network IP Address of ESX host 1 | 192.168.11.100 |
| <<var_vmotion_netmask>> | Netmask of the Vmotion Net- | 255.255.255.0 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| | work | |
| <<var_vmkern_mgmt_name>> | Name of the Management Network for the VMKernel | VMKernel-Mgmt |
| <<var_esx_mgmt_network>> | Name of the Management Network with VM access | Managemen Network |
| <<var_esx_vmkernel_nfs>> | Name of the NFS Network for the VMKernel | VMKernel-NFS |
| <<var_esx_vmkernel_vmotion>> | Name of the VMotion Network for the VMKernel | VMKernel-vMotion |
| <<var_n1k_mgmt_pp-name>> | Port Profile name for Management traffic | Admin-Zone |
| <<var_n1k_client_pp_name>> | Port Profile name for Client Access traffic | Client-Zone |
| <<var_n1k_nfs_pp_name>> | Port Profile name for NFS traffic | Storage-Zone |
| | | |
| VM Templates | | |
| | | |
| <<var_mgmt_temp_ip>> | Temporary used IP Address | 192.168.76.199 |
| <<var_vc_rhel_template>> | Name of the VM Template for RHEL | RHEL-VM |
| <<var_vc_sles_template>> | Name of the VM Template for SLES | SLES-VM |
| <<var_vc_windows_template>> | Name of the VM Template for Windows | Windows-VM |
| | | |
| Use Cases | | |
| Virtualized SAP HANA Scale-Up System (vHANA) | | |
| | | |
| <<var_t001_access_vlan_id>> | | 3001 |
| <<var_ucs_t001_access_vlan_name>> | Tenant001 Access VLAN ID | Tenant001-Access |
| <<var_vnx_hana_datastore1>> | Name of the Datastore for SAP HANA | HANA-Datastore-1 |
| <<var_vc_t001_vm01_name>> | Name of Tenant001 Virtual Machine 1 | Tenant001-vHANA01 |
| <<var_vc_t001_profile_name>> | Name of the Customization Profile within vCenter | Tenant001-Profile |
| <<var_vc_t001_hostname_prefix>> | Hostname Prefix defined in the Customization Profile | t001vhana |
| <<var_t001_vhana1_access_ip>> | IP Address of the first system in the Access Network | 172.16.1.3 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_t001_domain>> | DNS Domain for Tenant001 - can be the customer domain name | t001.cra-emc.local |
| <<var_t001_ns1>> | Name Server 1 IP Address | 208.67.222.222 |
| <<var_t001_ns2>> | Name Server 2 IP Address | 208.67.220.220 |
| <<var_t001_access_mask>> | Tenant001 Access Network Netmask | 255.255.255.248 |
| <<var_t001_hana01_hostname>> | Hostname for Tenant001 server01 | t001vhana01 |
| <<var_t001_access_netmask>> | Netmask of the Access Network | 255.255.255.248 |
| <<var_t001_hana_sid>> | SAP HANA System ID | T01 |
| <<var_t001_hana_nr>> | SAP HANA System Number | .01 |
| <<var_t001_hana_sys_passwd>> | SAP HANA Database Administrator Password (SYSTEM) | SAPhana10 |
| | | |
| SAP HANA Scale-Up on a Bare Metal Server | | |
| | | |
| <<var_tenant002_access_vlan_id>> | Tenatant002 Access VLAN ID | 3002 |
| <<var_ucs_hana01_org>> | UCS Organization for SAP HANA systems | HANA01 |
| <<var_ucs_tenant002_access_vlan_name>> | Access VLAN Name | Tenant002-Access |
| <<var_ucs_t002_hana1_sp_name>> | Service Profile Name for Tenant002 server01 | Tenant002-hana01 |
| <<var_t002_hana1_access_ip>> | IP Address for Tenant002 server01 | 172.16.2.3 |
| <<var_t002_hana01_hostname>> | Hostname for Tenant002 server01 | t002hana01 |
| <<var_t002_domain>> | DNS Domain for Tenant002 - can be the customer domain name | t002.cra-emc.local |
| <<var_t002_access_mask>> | Tenant002 Access Network Netmask | 255.255.255.248 |
| <<var_t002-hana01_nfs_ip>> | IP Address for Tenant002 server01 in the NFS network | 172.30.113. |
| <<var_t002_access_gw>> | Default Gateway for Tenant002 in the Access network | 172.16.2.1 |
| <<var_t002_hana1_sid>> | System ID for this SAP HANA System (SID) | T02 |
| <<var_t002_hana1_nr>> | System Number for this SAP HANA System (Nr) | 12 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_t002_hana_sys_passwd>> | Password for database user SYSTEM | SAPhana10 |
| <<var_zone_t002-hana1>> | SAN Zone name for Boot and Log on MDS | zone_t002-hana1 |
| <<var_zone_t002-hana1-data>> | SAN Zone name for Data on MDS | zone_t002-hana1-data |
| | | |
| SAP HANA Scale-Up with Multi Database Container | | |
| <<var_mdc_access_vlan_id>> | MDC Access VLAN ID | 3003 |
| <<var_ucs_mdc_access_vlan_name>> | Access VLAN Name | MDC-Access |
| <<var_ucs_mdc1_sp_name>> | Service Profile Name for Multi Database Container server01 | MDC-hana01 |
| <<var_mdc_hana1_access_ip>> | IP Address for MDC server01 | 173.16.3.3 |
| <<var_mdc_hana01_hostname>> | Hostname for MDC server01 | MDC-hana01 |
| <<var_mdc_domain>> | DNS Domain for MDC - can be the customer domain name | mdc.cra-emc.local |
| <<var_mdc_access_mask>> | MDC Access Network Netmask | 255.255.255.248 |
| <<var_mdc-hana01_nfs_ip>> | IP Address for MDC server01 in the NFS network | 172.30.113. |
| <<var_mdc_access_gw>> | Default Gateway for MDC in the Access network | 172.16.3.1 |
| <<var_zone_MDC-hana01>> | SAN Zone name for Boot and Log on MDS | zone_MDC-hana01 |
| <<var_zone_mdc-hana01-data>> | SAN Zone name for Data on MDS | zone_mdc-hana01-data |
| <<email_address>> | Email Address to register the system at SUSE | user@company.com |
| <<registration_code>> | Registration Code to register the system at SUSE | 1234567890 |
| <<var_mdc_hana1_sid>> | System ID for this SAP HANA System (SID) | MDC |
| <<var_mdc_hana1_nr>> | System Number for this SAP HANA System (Nr) | 30 |
| <<var_mdc_hana1_sys_passwd>> | Password for database user SYSTEM | SAPhana10 |
| <<var_hana-mdc1_db1_os-user>> | OS User to run DB Container 1 | t03adm |
| <<var_hana-mdc1_admin>> | Database User to create the Database containers | ADMIN |
| <<var_hana-mdc1_temp- | TEMP Passwd to run HANA- | Abc12345 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| passwd>> | MDC Container 1 | |
| <<var_hana-mdc1_admin_passwd>> | Password for database user ADMIN | SAPhana10 |
| <<var_hana-mdc1_db1_name>> | Name of the Database Container | TENANT03 |
| <<var_hana-mdc1_db1_system_passwd>> | Password for user SYSTEM in the Database container | SAPhana10 |
| | | |
| Tenant 004 - DT | | |
| <<var_t004_access_vlan_id>> | HANA system Access VLAN ID | 3004 |
| <<var_ucs_t004_access_vlan_name>> | Access VLAN name | Tenant004-Access |
| <<var_ucs_t004_hana1_sp_name>> | Service Profile Name for HANA system | t004-hana01 |
| <<var_zone_t004-hana01>> | SAN zone name for Boot | zone_t004-hana01 |
| <<var_ucs_t004_hana1_name>> | HANA/DT system Org name in UCS | T004-hana01 |
| <<var_t004_hana1_access_ip>> | Access IP | 173.16.4.3 |
| <<var_t004_hana01_hostname>> | HANA system t004 hostname | T004-hana01 |
| <<var_t004_domain>> | FQDN for HANA system | t004.cra-emc.local |
| <<var_t004_access_mask>> | Access Network Netmask | 255.255.255.248 |
| <<var_t004-hana01_nfs_ip>> | HANA system NFS IP network | 172.30.113. |
| <<var_nfs_mask>> | HANA system NFS IP mask | 255.255.255.0 |
| <<var_t004_access_gw>> | HANA system Access Network Gateway | 172.16.4.1 |
| <<var_zone_t004-hana01-data>> | SAN zone name for Data and Log | zone_t004-hana01-data |
| <<email_address>> | Email address used for Linux registration | user@company.com |
| <<registration_code>> | Registration Code to be used with email for Linux host registration | 1234567890 |
| <<var_t004_hana1_sid>> | HANA system SID | T4D |
| <<var_t004_hana1_nr>> | HANA System Instance Number | 82 |
| <<var_t004_hana1_sys_passwd>> | HANA Database SYSTEM user password | SAPhana10 |
| <<var_hana-t004_db1_os-user>> | HANA System Database user | t04adm |
| | | |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_t004_internal_vlan_id>> | HANA Node - DT Node Internal Network VLAN ID | 3204 |
| <<var_ucs_t004_internal_vlan_name>> | HANA Node - DT Node Internal Network VLAN name | Tenant004-Internal |
| <<var_t004_nfs_vlan_id>> | HANA Node - DT Node NFS VLAN ID | 3304 |
| <<var_ucs_t004_nfs_vlan_name>> | HANA Node - DT Node NFS VLAN Name | T004-NFS |
| <<var_vnx_tenant004_nfs_storage_ip>> | HANA Node - DT Node NFS Share IP address from VNX | 172.30.4.6 |
| <<var_vnx_tenant004_if_name>> | HANA system's VNX Network Filesytem Network Name | Tenant004 |
| <<var_tenant004_nfs_mask>> | NFS Mask for export for HANA | 255.255.255.248 |
| <<var_vnx_t004_fs_name>> | Filesystem name for HANA system usage | Tenant004-hana1-share |
| <<var_vnx_t004_share_name>> | NFS export/Fileshare name | Tenant004-hana1-share |
| <<var_vnx_t004_network>> | VNX Datamover Network | 172.30.4.0 |
| | | |
| Tenant 005 - Scale Out Sytem | | |
| <<var_t005_access_vlan_id>> | ScaleOut System Access VLAN ID | 3005 |
| <<var_ucs_t005_access_vlan_name>> | ScaleOut System Access VLAN name | Tenant005-Access |
| <<var_t005_Internal_vlan_id>> | ScaleOut System Inter-node VLAN ID | 3205 |
| <<var_ucs_t005_Internal_vlan_name>> | ScaleOut System Inter-node VLAN name | Tenant005-Internal |
| <<var_t005_nfs_vlan_id>> | ScaleOut System NFS-shared VLAN ID | 3305 |
| <<var_ucs_t005_nfs_vlan_name>> | ScaleOut System NFS-shared VLAN Name | Tenant005-NFS |
| <<var_t005_client_vlan_id>> | ScaleOut System Client VLAN ID | 3405 |
| <<var_ucs_t005_client_vlan_name>> | ScaleOut System Client VLAN name | Tenant005-Client |
| <<var_t005_backup_vlan_id>> | ScaleOut System Backup VLAN ID | 3505 |
| <<var_ucs_t005_backup_vlan_name>> | ScaleOut System Backup VLAN name | Tenant005-Backup |
| <<var_t005_replication_vlan_id>> | ScaleOut System Replication VLAN ID | 3605 |
| <<var_ucs_t005_replication_vla | ScaleOut System Replication | Tenant005-Replication |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| n_name>> | VLAN name | |
| <<var_t005_datasource_vlan_id>> | ScaleOut System Datasource VLAN ID | 3705 |
| <<var_ucs_t005_datasource_vlan_name>> | ScaleOut System DatasourceVLAN name | Tenant005-Datasource |
| <<var_t005_appserver_vlan_id>> | ScaleOut System AppServer VLAN ID | 3805 |
| <<var_ucs_t005_appserver_vlan_name>> | ScaleOut System AppServer VLAN name | Tenant005-Appserver |
| <<var_ucs_t005_hana1_sp_name>> | Service Profile Name for HANA system | Tenant005-hana01 |
| <<var_ucs_t005_hana2_sp_name>> | Service Profile Name for HANA system | Tenant005-hana02 |
| <<var_ucs_t005_hana3_sp_name>> | Service Profile Name for HANA system | Tenant005-hana03 |
| <<var_ucs_hana01_name>> | ScaleOut System Org name in UCS | HANA01 |
| <<var_ucs_t005-hana_sys-name>> | HANA System name | Tenant005-hana |
| <<var_t005_hana1_access_ip>> | HANA Node01 Access IP | 173.16.5.10 |
| <<var_t005_hana2_access_ip>> | HANA Node02 Access IP | 173.16.5.11 |
| <<var_t005_hana3_access_ip>> | HANA Node03 Access IP | 173.16.5.12 |
| <<var_t005_access_gw>> | HANA system Access Network Gateway | 172.16.5.1 |
| <<var_t005_hana1_name>> | HANA Node01 hostname | t005-hana01 |
| <<var_t005_hana2_name>> | HANA Node02 hostname | t005-hana02 |
| <<var_t005_hana3_name>> | HANA Node03 hostname | t005-hana03 |
| <<var_t005_domain>> | FQDN for HANA system | t005.cra-emc.local |
| <<var_t004_access_mask>> | Access Network Netmask | 255.255.255.248 |
| <<var_t004-hana1_nfs_ip>> | HANA Node01 NFS-storage Vlan IP | 172.30.5.3 |
| <<var_t004-hana2_nfs_ip>> | HANA Node02 NFS-storage Vlan IP | 172.30.5.4 |
| <<var_t004-hana3_nfs_ip>> | HANA Node03 NFS-storage Vlan IP | 172.30.5.5 |
| <<var_zone_t005-hana01>> | SAN zone name for Boot and Log - Node01 | zone_t005-hana01 |
| <<var_zone_t005-hana02>> | SAN zone name for Boot and Log - Node02 | zone_t005-hana02 |

| Variable Name | Description | Value used in the Lab for this Document |
|---|---|---|
| <<var_zone_t005-hana03>> | SAN zone name for Boot and Log - Node03 | zone_t005-hana03 |
| <<var_zone_t005-hana01-data>> | SAN zone name for Data - Node01 | zone_t005-hana01-data |
| <<var_zone_t005-hana02-data>> | SAN zone name for Data - Node02 | zone_t005-hana02-data |
| <<var_zone_t005-hana03-data>> | SAN zone name for Data - Node03 | zone_t005-hana03-data |
| <<email_address>> | Email address used for Linux registration | user@company.com |
| <<registration_code>> | Registration Code to be used with email for Linux host registration | 1234567890 |
| <<var_t005_hana_sid>> | HANA system SID | T5S |
| <<var_t005_hana_sid_passwd>> | SAP HANA system <sid>adm Pasword | SAPhana10 |
| <<var_t005_hana_nr>> | HANA System Instance Number | 55 |
| <<var_t005_hana_sapadm_passwd>> | SAP Hostagent sapadm user password | SAPhana10 |
| <<var_t005_hana_sys_passwd>> | HANA Database SYSTEM user password | SAPhana10 |
| <<var_hana-t005_db_os-user>> | HANA System Database user | ts5adm |
| <<var_vnx_tenant005_nfs_storage_ip>> | ScaleOut System VNX file settings IP | 172.30.5.6 |
| <<var_vnx_tenant005_if_name>> | HANA system's VNX Network Filesytem Network Name | Tenant005 |
| <<var_tenant005_nfs_mask>> | NFS Mask for export for HANA | 255.255.255.248 |
| <<var_vnx_t005_fs_name>> | Filesystem name for HANA system usage | Tenant005-hana1-share |
| <<var_vnx_t005_share_name>> | NFS export/Fileshare name | Tenant005-hana1-share |
| <<var_vnx_t005_network>> | VNX Datamover Network | 172.30.5.0 |
| <<var_vnx_t005_network_mask>> | HANA system NFS IP mask | 255.255.255.248 |
| <<var_vnx1_name>> | EMC VNX Array system name | VNX8000 |

# References

Cisco UCS

http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified_computing.html

Cisco UCSM 2.2(3) Configuration guides

CLI

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/cli/config/guide/2-2/b_UCSM_CLI_Configuration_Guide_2_2.html

GUI

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2.html

VMware vSphere

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

VMware vSphere 5.5 documentation

https://pubs.vmware.com/vsphere-55/index.jsp

EMC VNX5xxx series resources

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

# About the Authors

Ulrich Kleidon, Principal Engineer, Cisco Systems, Inc.

Ulrich Kleidon is a Principal Engineer with Cisco UCS Solutions and Performance Group. Ulrich has over 20 years of experience in compute, network, storage and server virtualization design. Ulrich has delivered solutions for server and SAP applications and has extensive experience with Cisco Unified Computing System, Cisco Nexus products, and Storage technologies. He has worked on performance and benchmarking with Cisco UCS servers. Ulrich holds a certification in SAP NetWeaver Administration and is Cisco Unified Computing Systems Design Specialist.

Shailendra Mruthunjaya, Technical Marketing Engineer, Cisco Systems, Inc.

Shailendra Mruthunjaya is a Technical Marketing Engineer with Cisco UCS Solutions and Performance Group. Shailendra has over four years of experience on SAP HANA with Cisco UCS platform. Shailendra has designed several SAP landscapes in public and private cloud environments. He is currently focused on developing and validating infrastructure best practices for SAP applications on Cisco UCS Servers, Cisco Nexus products and Storage technologies.

Ralf Klahr, Technical Marketing Engineer, Cisco Systems, Inc.

Ralf Klahr is a Technical Marketing Engineer at Cisco Systems is currently focusing on the SAP HANA infrastructure design and validation to help ensure reliable customer deployments. Ralf is a subject matter expert in SAP Landscape virtualization and SAP NetWeaver Basis technology with a focus of business continuity and high availability. Ralf has more than 20 years of experience in the IT industry focusing on SAP technologies.

Pramod Ramamurthy, Technical Marketing Engineer, Cisco Systems, Inc.

Pramod is a Technical Marketing Engineer with Cisco UCS Solutions and Performance Group. Pramod is currently focused on the SAP HANA appliance infrastructure build and validation and associated collaterals design. Pramod has more than 13 years of experience in the IT industry focusing on SAP technologies.

## Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, we would like to acknowledge the significant contribution and expertise that resulted in developing this document:

- Siva Sivakumar, Cisco Systems, Inc.
- Shanthi Adloori, Cisco Systems, Inc.
- Michael Dougherty, Cisco Systems, Inc.
- Chris O'Brien, Cisco Systems, Inc.
- Dan Laden, Cisco Systems, Inc.
- Bathumalai Krishnan, Cisco Systems, Inc.
- Matthias Schlarb, Cisco Systems, Inc.
- Lisa DeRuyter, Cisco Systems, Inc.
- Werner Katzenberger, EMC

- Michael Lang, EMC
- Thomas Weichert, EMC