Cisco Solution for EMC VSPEX End User Computing for 500 Citrix XenDesktop 5.6 Users

Enabled by Cisco Unified Computing System C220 M3 Servers, Cisco Nexus Switching, VMware vSphere 5, and Direct Attached EMC VNX5300

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Authors

Mike Brennan, Sr. Technical Marketing Engineer, VDI Performance and Solutions Team Lead, Cisco Systems

Mike Brennan is a Cisco Unified Computing System architect, focusing on Virtual Desktop Infrastructure solutions with extensive experience with EMC VNX, VMware ESX/ESXi, and VMware View. He has expert product knowledge in application and desktop virtualization across all three major hypervisor platforms, both major desktop brokers, Microsoft Windows Active Directory, User Profile Management, DNS, DHCP and Cisco networking technologies.

.

About Cisco Validated Design (CVD) Program

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

Cisco Solution for EMC VSPEX End User Computing for 500 Citrix XenDesktop 5.6 Users

1 Overview

Industry trends indicate a vast data center transformation toward shared infrastructures. Enterprise customers are moving away from silos of information and toward shared infrastructures, to virtualized environments, and eventually to the cloud to increase agility, improve availability and reduce costs.

This document reports the results of a study evaluating the scalability of Citrix XenDesktop 5.6 environment, utilizing Citrix Machine Creation Services, on managed Cisco UCS C-Series C220 M3 Rack-Mount Servers running VMware ESXi 5.0 Update 1 hypervisor software connected to an EMC VNX5300 Storage Array. We utilize second generation Unified Computing System hardware and software. We provide best practice recommendations and sizing guidelines for a 500-600 virtual desktop customer deployment of XenDesktop 5.6 on the Cisco Unified Computing System.

Five Cisco UCS C220 M3 Rack Servers were utilized in the design to provide N+1 fault tolerance for 500 Virtual Windows 7 desktops at the server level, guaranteeing the same end-user experience if just 4 C220 M3 servers are operational. In fact, the five server architecture can comfortably support 600 desktops with N+1 server fault tolerance. For that reason, the document architecture will refer to supporting a 600 desktop capacity with five Cisco UCS C220 M3 servers.

Alternatively, with just four Cisco UCS C220 M3 Rack Servers, we can effectively host 500 users with all servers online or 450 Users with 3 UCS C220 M3 servers running.

This study was performed in conjunction with EMC's VSPEX program and aligns closely with the Cisco Solution for EMC VSPEX C500 Reference Architecture and Deployment Guide.

1.1 Solution Components Benefits

Each of the components of the overall solution materially contributes to the value of functional design contained in this document.

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

1.1.1 Benefits of Cisco Unified Computing System

Cisco Unified Computing System™ is the first converged data center platform that combines industry-standard, x86-architecture servers with networking and storage access into a single converged system. The system is entirely programmable using unified, model-based management to simplify and speed deployment of enterprise-class applications and services running in bare-metal, virtualized, and cloud computing environments.

Benefits of the Unified Computing System include:

Architectural flexibility

- Cisco UCS B-Series blade servers for infrastructure and virtual workload hosting
- Cisco UCS C-Series rack-mount servers for infrastructure and virtual workload Hosting
- Cisco UCS 6200 Series second generation fabric interconnects provide unified blade, network and storage connectivity
- Cisco UCS 5108 Blade Chassis provide the perfect environment for multi-server type, multi-purpose workloads in a single containment

Infrastructure Simplicity

- Converged, simplified architecture drives increased IT productivity
- Cisco UCS management results in flexible, agile, high performance, self-integrating information technology with faster ROI. With Cisco UCS Manager 2.1 introduced on November 21, 2012, Cisco UCS C-Series Servers and Fibre Channel (FC) SAN storage can be managed end-to-end by Cisco UCS 6200 Series Fabric Interconnects
- Fabric Extender technology reduces the number of system components to purchase, configure and maintain
- Standards-based, high bandwidth, low latency virtualization-aware unified fabric delivers high density, excellent virtual desktop user-experience

Business Agility

- Model-based management means faster deployment of new capacity for rapid and accurate scalability
- Scale up to 16 Chassis and up to 128 blades in a single Cisco UCS management domain
- With Cisco UCS Manger 2.1 and Cisco UCS Central 1.0, the scope of management extends to many Cisco UCS Domains
- Leverage Cisco UCS Management Packs for System Center 2012 for integrated management

1.1.2 Benefits of Nexus Switching

1.1.2.1 Cisco Nexus 5548 (NFS Variant)

The Cisco Nexus 5548UP Switch, used exclusively in the NFS variant or the EMC VSPEX C500 architecture, delivers innovative architectural flexibility, infrastructure simplicity, and business agility, with support for networking standards. For traditional, virtualized, unified, and high-performance computing (HPC) environments, it offers a long list of IT and business advantages, including:

Architectural Flexibility

- Unified ports that support traditional Ethernet, Fibre Channel (FC),and Fibre Channel over Ethernet (FCoE)
- Synchronizes system clocks with accuracy of less than one microsecond, based on IEEE 1588
- Offers converged Fabric extensibility, based on emerging standard IEEE 802.1BR, with Fabric Extender (FEX) Technology portfolio, including:
- Nexus 1000V Virtual Distributed Switch
- Cisco Nexus 2000 FEX
- Adapter FEX
- VM-FEX

Infrastructure Simplicity

- Common high-density, high-performance, data-center-class, fixed-form-factor platform
- Consolidates LAN and storage
- Supports any transport over an Ethernet-based fabric, including Layer 2 and Layer 3 traffic
- Supports storage traffic, including iSCSI, NAS, FC, RoE, and IBoE
- Reduces management points with FEX Technology

Business Agility

- Meets diverse data center deployments on one platform
- Provides rapid migration and transition for traditional and evolving technologies
- Offers performance and scalability to meet growing business needs

Specifications At-a-Glance

- A 1 -rack-unit, 1/10 Gigabit Ethernet switch
- 32 fixed Unified Ports on base chassis and one expansion slot totaling 48 ports
- The slot can support any of the three modules: Unified Ports, 1/2/4/8 native Fibre Channel, and Ethernet or FCoE
- Throughput of up to 960 Gbps

1.1.2.2 Cisco Nexus 2232PP Fabric Extender (Fibre Channel Variant)

The Cisco Nexus 2232PP 10GE Fabric Extender provides 32 10 Gb Ethernet and Fibre Channel Over Ethernet (FCoE) Small Form-Factor Pluggable Plus (SFP+) server ports and eight 10 Gb Ethernet and FCoE SFP+ uplink ports in a compact 1 rack unit (1RU) form factor.

The Nexus 2232PP in conjunction with VIC1225 converged network adapters in the Cisco UCS C220 M3 rack servers provide fault-tolerant single wire management of the rack servers through up to 8 uplink ports to Cisco Fabric Interconnects.

Reduce TCO

- The innovative Fabric Extender approach reduces data center cabling costs and footprint with optimized inter-rack cabling
- Unified fabric and FCoE at the server access layer reduce capital expenditure and operating expenses Simplify Operation

- Cisco UCS 6248UP or 6296UP Fabric Interconnects provide a single point of management and policy enforcement
- Plug-and-play management includes auto-configuration

Cisco Nexus 2232PPs were utilized in the FC variant of the study only.

1.1.3 Benefits of EMC VNX Family of Storage Controllers

The EMC VNX Family delivers 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.

All of this is available in a choice of systems ranging from affordable entry-level solutions to high performance, petabyte-capacity configurations servicing the most demanding application requirements. The VNX family includes the VNXe Series, purpose-built for the IT generalist in smaller environments , and the VNX Series , designed to meet the high-performance, high scalability, requirements of midsize and large enterprises.

VNX Series - Simple, Efficient, Powerful

A robust platform for consolidation of legacy block storage, file-servers, and direct-attached application storage, the VNX series enables organizations to dynamically grow, share, and cost-effectively manage multi-protocol file systems and multi-protocol block storage access. The VNX Operating environment enables Microsoft Windows and Linux/UNIX clients to share files in multi-protocol (NFS and CIFS) environments. At the same time it supports iSCSI, Fiber Channel, and FCoE access for high bandwidth and latency-sensitive block applications. The combination of EMC Atmos Virtual Edition software and VNX storage supports object-based storage and enables customers to manage web applications from EMC Unisphere. The VNX series next generation storage platform is powered by Intel quad-core Xeon 5600 series with a 6 –Gb/s SAS drive back-end and delivers demonstrable performance improvements over the previous generation mid-tier storage:

- Run Microsoft SQL and Oracle 3x to 10x faster
- Enable 2x system performance in less than 2 minutes –non-disruptively
- Provide up to 10 GB/s bandwidth for data warehouse applications

1.1.4 Benefits of VMware ESXi 5.0

As virtualization is now a critical component to an overall IT strategy, it is important to choose the right vendor. VMware is the leading business virtualization infrastructure provider, offering the most trusted and reliable platform for building private clouds and federating to public clouds.

Find out how only VMware delivers on the core requirements for a business virtualization infrastructure solution.

1. Is built on a robust, reliable foundation
2. Delivers a complete virtualization platform from desktop through the datacenter out to the public cloud
3. Provides the most comprehensive virtualization and cloud management
4. Integrates with your overall IT infrastructure
5. Is proven over 350,000 customers

And best of all, VMware delivers while providing

6. Low total-cost-of-ownership (TCO)

1.1.5 Benefits of Citrix XenDesktop and Provisioning Server

XenDesktop is a comprehensive desktop virtualization solution that includes all the capabilities required to deliver desktops, apps and data securely to every user in an enterprise. Trusted by the world's largest organizations, XenDesktop has won numerous awards for its leading-edge technology and strategic approach to desktop virtualization.

XenDesktop helps businesses:

- Enable virtual workstyles to increase workforce productivity from anywhere
- Leverage the latest mobile devices to drive innovation throughout the business
- Rapidly adapt to change with fast, flexible desktop and app delivery for offshoring, M&A, branch expansion and other initiatives
- Transform desktop computing with centralized delivery, management and security

A complete line of XenDesktop editions lets you choose the ideal solution for your business needs and IT strategy. XenDesktop VDI edition, a scalable solution for delivering virtual desktops in a VDI scenario, includes Citrix HDX technology, provisioning services, and profile management. XenDesktop Enterprise edition is an enterprise-class desktop virtualization solution with FlexCast delivery technology that delivers the right type of virtual desktop with on-demand applications to any user, anywhere. The comprehensive Platinum edition includes advanced management, monitoring and security capabilities.

1.2 Audience

This document describes the architecture and deployment procedures of an infrastructure comprised of Cisco, EMC, VMware and Citrix virtualization. The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the solution described in this document.

2 Summary of Main Findings

The combination of technologies from Cisco Systems, Inc, Citrix Systems, Inc, VMware and EMC produced a highly efficient, robust and scalable Virtual Desktop Infrastructure (VDI) for a hosted virtual desktop deployment. Key components of the solution included:

- The combined power of the Unified Computing System, Nexus switching and EMC storage hardware with VMware ESXi 5.0 Update 1, and Citrix XenDesktop 5.6 with Machine Creation Services software produces a high density per rack-server Virtual Desktop delivery system.
- Cisco UCS C-220 M3 Rack-Mount Servers support 500-600 virtual desktops in N+1 server fault tolerance configuration based on the number of rack servers deployed.
- The 500 seat design providing N+1 server fault tolerance for 450 users is based on four Cisco UCS C220 M3 1U rack-mount servers, each with dual 8-core processors, 256GB of 1600 MHz memory and a Cisco VIC1225 converged network adapter
- The 600 seat design providing N+1 server fault tolerance for 600 users is based on five Cisco UCS C220 M3 1U rack-mount servers, each with dual 8-core processors, 256GB of 1600 MHz memory and a Cisco VIC1225 converged network adapter

- We were able to boot the full complement of desktops in under 15 minutes without pegging the processor, exhausting memory or storage subsystems
- We were able to ramp (log in and exercise workloads) up to steady state in thirty minutes without pegging the processor, exhausting memory or storage subsystems
- We maintain our industry leadership with our new Cisco UCS Manager 2.1(1a) software that makes scaling simple, consistency guaranteed and maintenance simple.
- Our 10G unified fabric story gets additional validation on second generation 6200 Series Fabric Interconnects and second generation Nexus 5500 Series access switches and Nexus 2200 Series fabric extenders as we run more challenging workload testing, maintaining unsurpassed user response times.
- For the Managed C-Series FC variant, utilizing Cisco UCS Manager 2.1 Service Templates and Service Profiles in conjunction with Nexus 2232PP Fabric Extenders, we were able fully configure all five Cisco UCS C220 M3 servers from cold start to ready to deploy VMware ESXi 5 boot from SAN in 30 minutes
- For the Managed C-Series FC variant of the study, utilizing Cisco UCS Manager 2.1, we were able to connect and integrate the EMC VNX5300 via FC on our Cisco UCS 6248UP Fabric Interconnects, including FC zoning, eliminating the requirement for upstream access layer switching or fiber channel switches for that purpose
- For the Unmanaged C-Series NFS variant of the study, we use a pair of Nexus 5548UP access layer switches to directly attach the unmanaged Cisco UCS C220 M3 servers and the EMC VNX5300
- Pure Virtualization: We continue to present a validated design that is 100 percent virtualized on ESXi 5.0 Update 1. All of the Windows 7 SP1 virtual desktops and supporting infrastructure components, including Active Directory, Profile Servers, SQL Servers, and XenDesktop delivery controllers were hosted as virtual servers.
- EMC's VNX5300 system provides storage consolidation and outstanding efficiency. Both block and NFS storage resources were provided by a single system, utilizing EMC Fast Cache technology.
- Whether using the Managed C-Series FC or the Unmanaged C-Series NFS variant and the EMC VNX storage layout prescribed in this document, the same outstanding end user experience is achieved as measured by Login VSI 3.6 testing
- Citrix HDX technology, extended in XenDesktop 5.6 Feature Pack 1 software, provides excellent performance with host-rendered flash video and other demanding applications.

3 Architecture

3.1 Hardware Deployed

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

The 500 User XenDesktop 5.6 solution with N+1 fault tolerance for 450 users, includes Cisco networking, four Cisco UCS C220 M3 Rack-Mount Servers and an EMC VNX5300 storage system.

The 600 User XenDesktop 5.6 solution with N+1 fault tolerance for 600 users, includes Cisco networking, five Cisco UCS C220 M3 Rack-Mount Servers and the same EMC VNX5300 storage system. The study will illustrate this configuration of the solution.

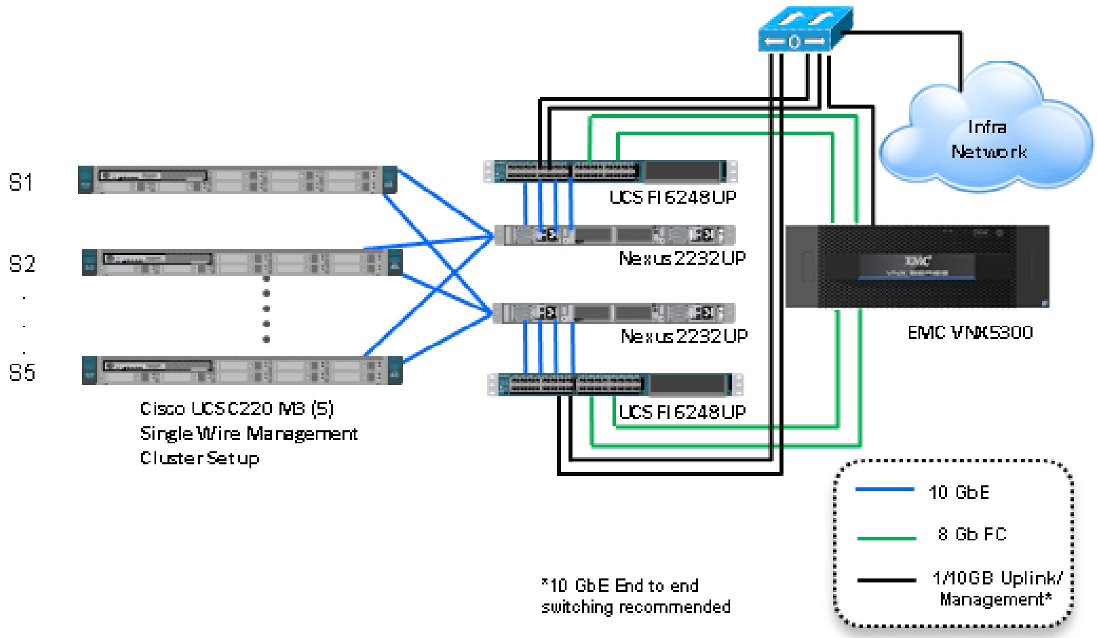
The same VNX5300 configuration is used with the 500 and 600 user examples.

Two variants to the design are offered:

- Managed C-Series with Fibre Channel (FC) Storage
- Unmanaged C-Series with NFS Storage

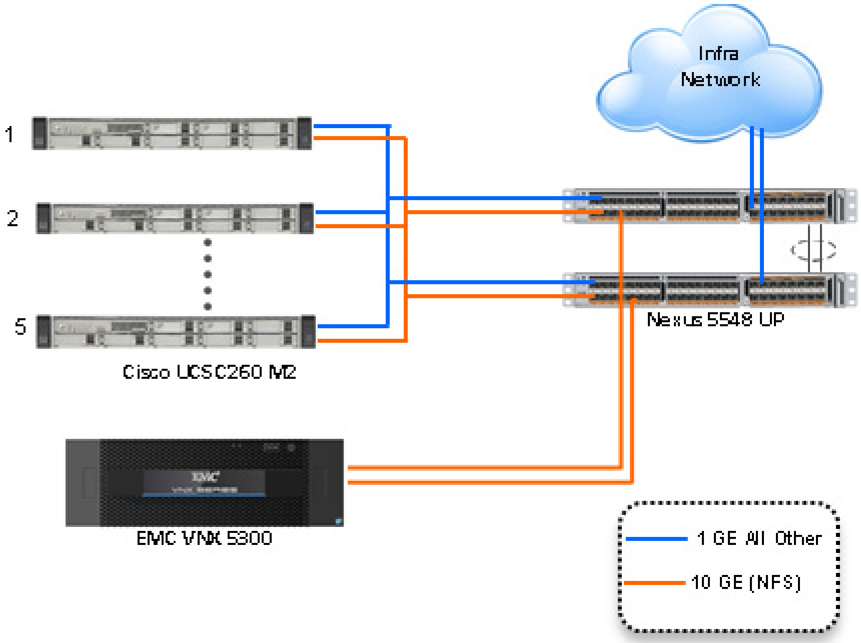
This document details the deployment of Citrix XenDesktop 5.6 with Machine Creation Service on VMware ESXi 5.0 Update 1

Figure 1 Citrix XenDesktop 5.6 600 User Hardware Components- Managed C220 M3 Rack-Mount Servers 8 Gb Fibre Channel Storage to Cisco UCS Connectivity



*10 GbE End to end switching recommended

Figure 2 Citrix XenDesktop 5.6 600 User Hardware Components- Unmanaged C220 M3 Rack-Mount Servers 10 Gb Ethernet NFS Storage to Cisco UCS Connectivity



The reference configuration includes:

- Two Cisco Nexus 5548UP switches (Unmanaged C-Series NFS Variant only)
- Two Cisco UCS 6248UP Series Fabric Interconnects (Managed C-Series FC Variant Only)
- Two Cisco Nexus 2232PP Fabric Extenders (Managed C-Series FC Variant Only)
- Five Cisco UCS C220 M3 Blade servers with Intel E5-2690 processors, 256 GB RAM, and VIC1225 CNAs for 600 VDI workloads with N+1 Server fault tolerance for 600 desktops.
- Four Cisco UCS C220 M3 Blade servers with Intel E5-2690 processors, 256 GB RAM, and VIC1225 CNAs for 500 VDI workloads with N+1 Server fault tolerance for 450 desktops
- One EMC VNX5300 dual controller storage system for HA, 2 Datamovers, 600GB SAS Drives and 200GB SSD Fast Cache Drives

The EMC VNX5300 disk shelf, disk and Fast Cache configurations are detailed in Section 5.4 Storage Architecture Design later in this document.

3.2 Software Revisions

Table 1 Software Used in this Deployment

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect (FC Variant) Cisco UCS C220 M3	2.1 (1a) 1.4 (7b)	Embedded Management Hardware BIOS
Network	Nexus Fabric Switch	5.2(1)N1(1)	Operating System Version

Storage	EMC VNX5300	Block: 5.31.000.5.704 File: 7.0.50-2	Operating System Version
Software	Cisco UCS C220 M3 Hosts	VMware ESXi 5.0 Update 1	Operating System Version

3.3 Configuration Guidelines

The 500-600 User XenDesktop 5.6 solution described in this document provides details for configuring a fully redundant, highly-available configuration. Configuration guidelines are provided that refer to which redundant component is being configured with each step, whether that be A or B. For example, SP A and SP B are used to identify the two EMC VNX storage controllers that are provisioned with this document while Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS Fabric Interconnects are configured similarly.

This document is intended to allow the reader to configure the Citrix XenDesktop 5.6 with the Machine Configuration Server customer environment as stand-alone solution.

3.3.1 VLANs

For the 500 User XenDesktop 5.6 solution, we utilized VLANs to isolate and apply access strategies to various types of network traffic. Table 2 details the VLANs used in this study.

Table 2 VLANS

VLAN Name	VLAN ID	Purpose	Native
ESXi_Management	132	ESXi Management	Yes
VDI	100	ESXi, N1KV Management	No
vMotion	51	vMotion	No

3.3.2 VMware Clusters

We utilized two VMware Clusters to support the solution and testing environment in both variants:

- Infrastructure Cluster (Active Directory, DNS, DHCP, SQL Server, File Shares for user profiles, XenDesktop controllers, etc.) This would likely be the Customer’s existing infrastructure cluster, adding a pair of XenDesktop 5.6 virtual machines and a SQL database to an existing SQL server to support them.
- VDA Cluster (Windows 7 SP1 32-bit pooled virtual desktops)

4 Infrastructure Components

This section describes all of the infrastructure components used in the solution outlined in this study.

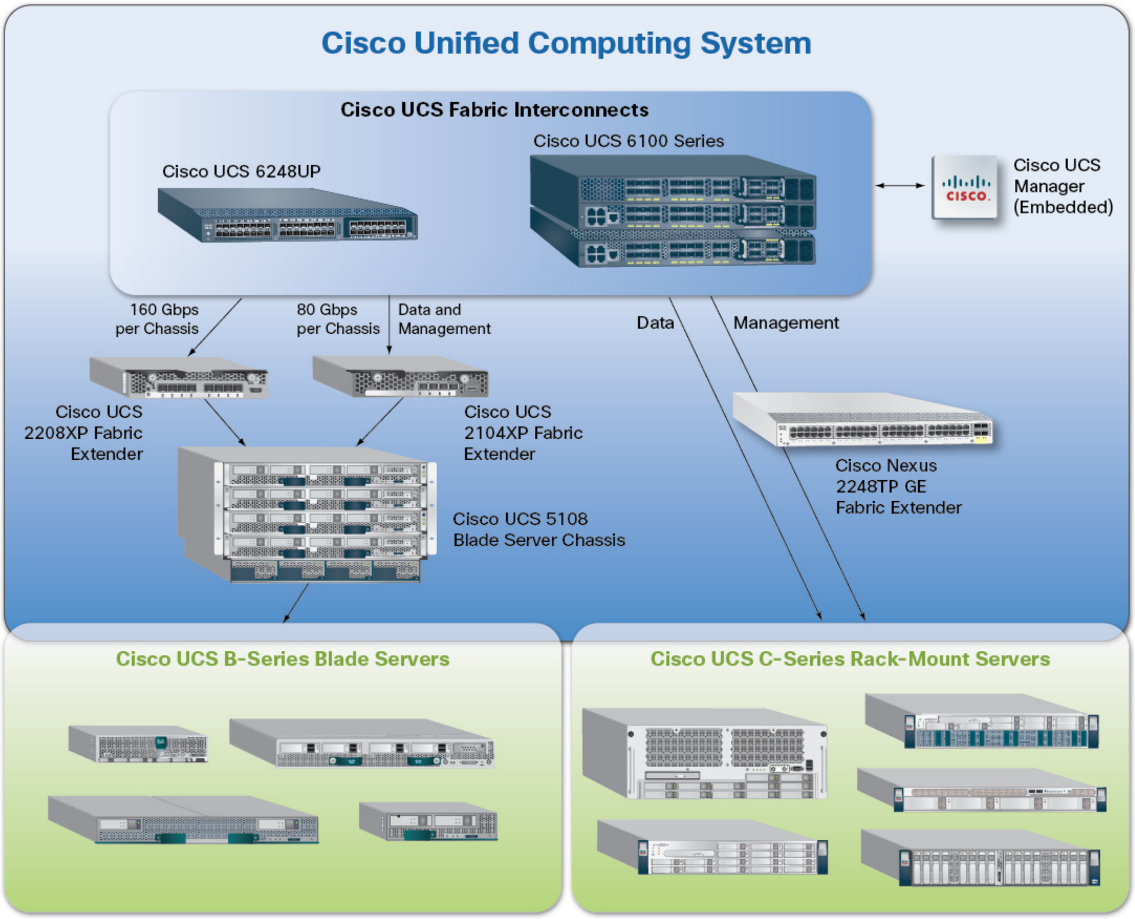
4.1 Cisco Unified Computing System (UCS)

Cisco Unified Computing System is a set of pre-integrated data center components that comprises blade servers, adapters, fabric interconnects, and extenders that are integrated under a common embedded management system. This approach results in far fewer system components and much better manageability, operational efficiencies, and flexibility than comparable data center platforms.

4.1.1 Cisco Unified Computing System Components

Cisco UCS components are shown in Cisco Unified Computing System Components.

Figure 3 Cisco Unified Computing System Components


Cisco Unified Computing System
Cisco UCS Fabric Interconnects
Cisco UCS 6100 Series
Cisco UCS 6248UP
Cisco UCS Manager (Embedded)
160 Gbps per Chassis
80 Gbps per Chassis
Data and Management
Data
Management
Cisco UCS 2208XP Fabric Extender
Cisco UCS 2104XP Fabric Extender
Cisco Nexus 2248TP GE Fabric Extender
Cisco UCS 5108 Blade Server Chassis
Cisco UCS B-Series Blade Servers
Cisco UCS C-Series Rack-Mount Servers

The Cisco Unified Computing System is designed from the ground up to be programmable and self-integrating. A server's entire hardware stack, ranging from server firmware and settings to network profiles, is configured through model-based management. With Cisco virtual interface cards, even the number and type of I/O interfaces is programmed dynamically, making every server ready to power any workload at any time.

With model-based management, administrators manipulate a model of a desired system configuration, associate a model's service profile with hardware resources and the system configures itself to match the model. This automation speeds provisioning and workload migration with accurate and rapid scalability. The result is increased IT staff productivity, improved compliance, and reduced risk of failures due to inconsistent configurations.

Cisco Fabric Extender technology reduces the number of system components to purchase, configure, manage, and maintain by condensing three network layers into one. It eliminates both blade server and hypervisor-based switches by connecting fabric interconnect ports directly to individual blade servers and virtual machines. Virtual networks are now managed exactly as physical networks are, but with massive scalability. This represents a radical simplification over traditional systems, reducing capital and operating costs while increasing business agility, simplifying and speeding deployment, and improving performance.

Note Only the Cisco UCS C-Series Rack-Mount Servers, specifically the Cisco UCS C220 M3, were used in both the Managed FC variant and the Unmanaged NFS variant for this study. For the Managed FC variant, Cisco UCS 6248UP Fabric Interconnects and Nexus 2232PPs were used in conjunction with the Cisco UCS C220 M3s and the EMC VNX5300. For the Unmanaged NFS variant, Nexus 5548UPs were used in conjunction with the Cisco UCS C220 M3s and the EMC VNX5300.

The components of the Cisco Unified Computing System and Nexus switches that were used in the study are discussed below

4.1.1 Cisco Fabric Interconnects (Managed FC Variant Only)

Cisco UCS Fabric Interconnects create a unified network, storage and management fabric throughout the Cisco UCS. They provide uniform access to both networks and storage, eliminating the barriers to deploying a fully virtualized environment based on a flexible, programmable pool of resources.

Cisco Fabric Interconnects comprise a family of line-rate, low-latency, lossless 10-GE, Cisco Data Center Ethernet, and FCoE interconnect switches. Based on the same switching technology as the Cisco Nexus 5000 Series, Cisco UCS 6000 Series Fabric Interconnects provide the additional features and management capabilities that make them the central nervous system of Cisco Unified Computing System.

The Cisco UCS Manager software runs inside the Cisco UCS Fabric Interconnects. The Cisco UCS 6000 Series Fabric Interconnects expand the Cisco UCS networking portfolio and offer higher capacity, higher port density, and lower power consumption. These interconnects provide the management and communication backbone for the Cisco UCS B-Series Blades and Cisco UCS Blade Server Chassis.

All chassis and all blades that are attached to the Fabric Interconnects are part of a single, highly available management domain. By supporting unified fabric, the Cisco UCS 6200 Series provides the flexibility to support LAN and SAN connectivity for all blades within its domain right at configuration time. Typically deployed in redundant pairs, the Cisco UCS Fabric Interconnect provides uniform access to both networks and storage, facilitating a fully virtualized environment.

The Cisco UCS Fabric Interconnect family is currently comprised of the Cisco 6100 Series and Cisco 6200 Series of Fabric Interconnects.

4.1.2.1 Cisco UCS 6248UP 48-Port Fabric Interconnect

The Cisco UCS 6248UP 48-Port Fabric Interconnect is a 1 RU, 10-GE, Cisco Data Center Ethernet, FCoE interconnect providing more than 1 Tbps throughput with low latency. It has 32 fixed ports of Fibre Channel, 10-GE, Cisco Data Center Ethernet, and FCoE SFP+ ports.

One expansion module slot can be up to sixteen additional ports of Fibre Channel, 10-GE, Cisco Data Center Ethernet, and FCoE SFP+. The expansion module was not required for this study.

4.1.2 Cisco UCS C220 M3 Rack-Mount Server

Cisco Unified Computing System is the first truly unified data center platform that combines industry-standard, x86-architecture blade and rack servers with networking and storage access into a single system. Key innovations in the platform include a standards-based unified network fabric, Cisco Virtualized Interface Card (VIC) support, and Cisco UCS Manager Service Profile and Direct Storage

Connection support. The system uses a wire- once architecture with a self-aware, self-integrating, intelligent infrastructure that eliminates the time-consuming, manual, error-prone assembly of components into systems.

Managed Cisco UCS C-Series Rack-Mount Servers reduce total cost of ownership (TCO) and increase business agility by extending Cisco Unified Computing System™ innovations to a rack-mount form factor. These servers:

- Can be managed and provisioned centrally using Cisco UCS Service Profiles with Cisco UCS Manager 2.1(1a,) Cisco UCS Fabric Interconnects and Nexus 2232PP Fabric Extenders
- Offer a form-factor-agnostic entry point into the Cisco Unified Computing System, which is a single converged system with configuration automated through integrated, model-based management
- Simplify and speed deployment of applications
- Increase customer choice with unique benefits in a familiar rack package
- Offer investment protection through the capability to deploy them either as standalone servers or as part of the Cisco Unified Computing System

Note This study highlights the use of Managed Cisco UCS C-Series Rack-Mount servers in the FC variant. The alternative NFS variant utilizes the Cisco UCS C220 M3 servers in stand-alone mode.

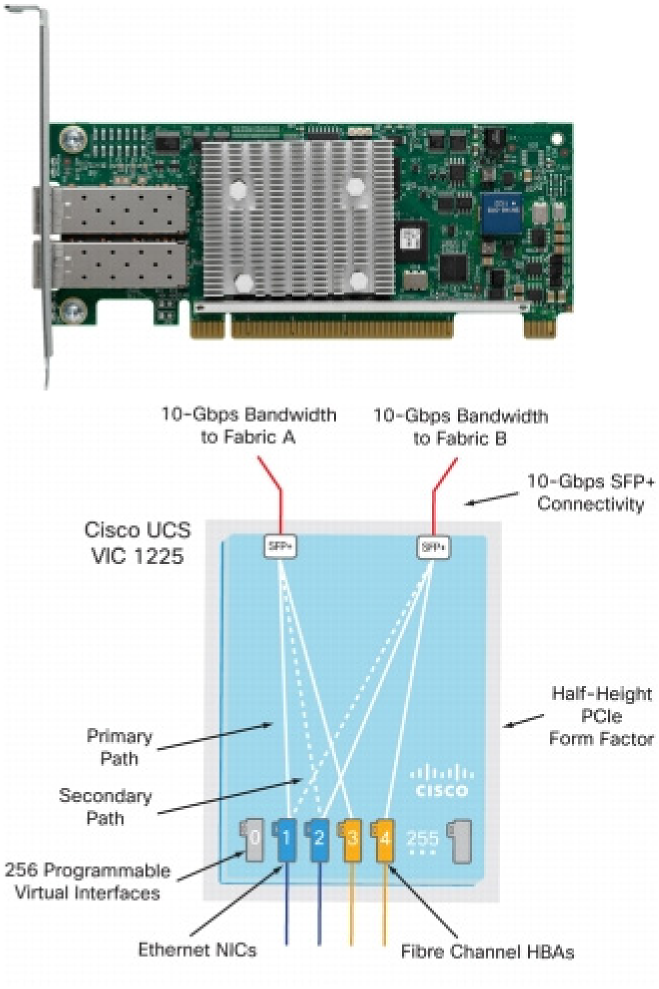
4.1.3 Cisco UCS Virtual Interface Card (VIC) Converged Network Adapter

A Cisco® innovation, the Cisco UCS Virtual Interface Card (VIC) 1225 (Figure 1) 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. With its half-height design, the card preserves full-height slots in servers for third-party adapters certified by Cisco. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases.

4.1.3.1 Cisco UCS Virtual Interface Card 1225

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 1225 supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

Figure 4 Cisco UCS VIC M81KR Converged Network Adapter


10-Gbps Bandwidth to Fabric A
10-Gbps Bandwidth to Fabric B
10-Gbps SFP+ Connectivity
Cisco UCS VIC 1225
SFP+
SFP+
Half-Height PCIe Form Factor
Primary Path
Secondary Path
256 Programmable Virtual Interfaces
0
1
2
3
4
255
cisco
Ethernet NICs
Fibre Channel HBAs

Note The Cisco UCS VIC 1225 virtual interface cards are deployed in the Cisco UCS C-Series C220 M3 rack-mount servers.

4.2 Citrix XenDesktop

Citrix XenDesktop is a desktop virtualization solution that delivers Windows desktops as an on-demand service to any user, anywhere. With FlexCast™ delivery technology, XenDesktop can quickly and securely deliver individual applications or complete desktops to the entire enterprise, whether users are task workers, knowledge workers or mobile workers. Users now have the flexibility to access their desktop on any device, anytime, with a high definition user experience. With XenDesktop, IT can manage single instances of each OS, application, and user profile and dynamically assemble them to increase business agility and greatly simplify desktop management. XenDesktop's open architecture enables customers to easily adopt desktop virtualization using any hypervisor, storage, or management infrastructure.

4.2.1 Enhancements in Citrix XenDesktop 5.6 Feature Pack 1

XenDesktop 5.6 Feature Pack 1, builds upon the themes of the last release which are about reducing cost and making it easier to do desktop virtualization. Below, is an overview of new or updated technologies and capabilities contained in Feature Pack 1:

- **Remote PC** – Extends the FlexCast physical delivery model to include secure remote connections to office-based PCs with a high-definition user experience leveraging Receiver and HDX technologies. Simple auto-assignment setup is included so Remote PC can be easily provisioned to thousands of users. With this new FlexCast delivery feature, Citrix is simplifying desktop transformation by creating an easy on-ramp for desktop virtualization. View the Remote PC video
- **Universal Print Server** – Combined with the previously available Universal Print Driver, administrators may now install a single driver in the virtual desktop image or application server to permit local or network printing from any device, including thin clients and tablets.
- **Optimized Unified Communications** – A new connector from Citrix enables Microsoft Lync 2010 clients to create peer-to-peer connections for the ultimate user experience, while taking the load off datacenter processing and bandwidth resources. The Cisco Virtualization Experience Client (VXC), announced October 2011, was the first in the industry to provide peer-to-peer connection capability to deliver uncompromised user experience benefits to Citrix customers. Download Cisco VXC . Webcam Video Compression adds support for WebEx (in addition to Office Communicator, GoToMeeting HDFaces, Skype and Adobe Connect).
- **Mobility Pack for VDI** – With the new Mobility Pack, XenDesktop dynamically transforms the user interfaces of Windows desktops and applications to look and feel like the native user interface of smartphones and tablets. Now, your existing Windows applications adapt to the way users interact with applications on smaller devices without any source code changes. Previously, this technology was available only for XenApp.
- **HDX 3D Pro** – This HDX update provides breakthrough visual performance of high-end graphics intensive applications obtained by producing much faster frame rates using NVIDIAs latest API and leveraging a new, ultra-efficient, deep compression codec.
- **XenClient Enterprise** – XenClient 4.1 now supports 9x more PCs, has wider graphics support with NVIDIA graphics & has broader server hypervisor support. Its backend management can now run on XenServer, vSphere & Hyper-V. The release brings robust policy controls to the platform & role based administration. XenClient 4.1 delivers enterprise level scalability with support of up to 10,000 endpoints.
- **Simple License Service –**This new license service automatically allocates and installs your XenDesktop and/or XenApp licenses directly from your license server, eliminating the need to go to My Citrix to fully allocate your licenses. For more details, reference Citrix edocs. Version 11.6.1 or higher of the License Server is required.

4.2.2 FlexCast Technology

Citrix XenDesktop with FlexCast is an intelligent delivery technology that recognizes the user, device, and network, and delivers the correct virtual desktop and applications specifically tailored to meet the performance, security, and flexibility requirements of the user scenario. FlexCast technology delivers any type of virtual desktop to any device and can change this mix at any time. FlexCast also includes on-demand applications to deliver any type of virtual applications to any desktop, physical or virtual.

The FlexCast delivery technologies can be broken down into the following categories:

- **Hosted Shared Desktops** provide a locked down, streamlined and standardized environment with a core set of applications, ideally suited for task workers running a few lower-intensity applications with light personalization requirements

- **Hosted VM Desktops** offer a personalized Windows desktop experience, typically needed by knowledge workers with higher application performance needs and high personalization requirements
- **Streamed Virtual Hard Disk (VHD) Desktops** use the local processing power of rich clients while providing centralized single image management of the desktop. These types of desktops are often used in computer labs and training facilities and when users require local processing for certain applications or peripherals.
- **Local VM Desktops** utilize XenClient to extend the benefits of centralized, single-instance management to mobile workers that need to use their laptops offline. When they are able to connect to a suitable network, changes to the OS, applications, and user data are automatically synchronized with the data center.
- **Physical Desktops** utilize the Remote PC feature in XenDesktop to create secure remote connections to physical PCs on a LAN without having to build out a large scale XenDesktop infrastructure in the data center.
- **On-demand Applications** allows any Windows® application to be centralized and managed in the data center, hosted either on multi-user terminal servers or VMs and instantly delivered as a service to physical and virtual desktops. Optimized for each user device, network, and location, applications are delivered through a high speed protocol for use while connected or streamed through Citrix application virtualization or Microsoft App-V directly to the endpoint for use when offline.

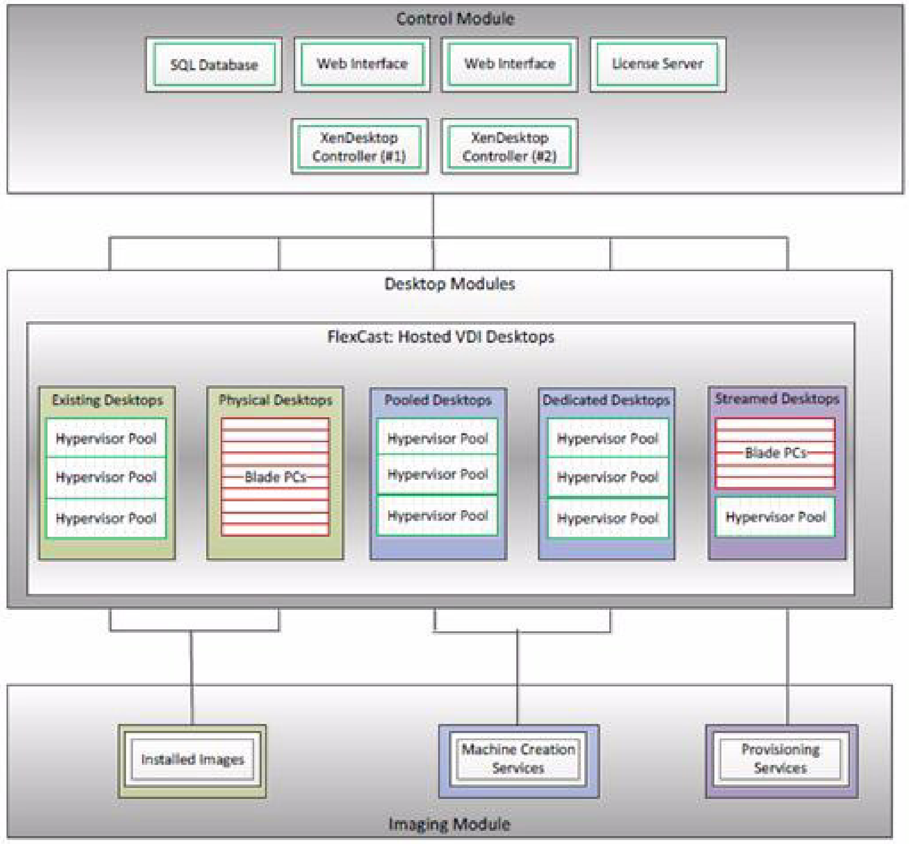
4.2.3 High-Definition User Experience Technology

Citrix High-Definition User Experience (HDX) technology is a set of capabilities that delivers a high definition desktop virtualization user experience to end users for any application, device, or network. These user experience enhancements balance performance with low bandwidth, whether it be plugging in a USB device, printing from a network printer or rendering real time video and audio. Citrix HDX technology provides network and application performance optimizations for a “like local PC” experience over LANs and a very usable experience over low bandwidth and high latency WAN connections.

4.2.4 Citrix XenDesktop Hosted VM Overview

Hosted VM uses a hypervisor to host all the desktops in the data center. Hosted VM desktops can either be pooled or assigned. Pooled virtual desktops use Citrix Provisioning Services to stream a standard desktop image to each desktop instance upon boot-up. Therefore, the desktop is always returned to its clean, original state. Citrix Provisioning Services enables the streaming of a single desktop image to create multiple virtual desktops on one or more hypervisors in a data center. This feature greatly reduces the amount of storage required compared to other methods of creating virtual desktops. The high-level components of a Citrix XenDesktop architecture utilizing the Hosted VM model for desktop delivery are shown in below Citrix XenDesktop on VMware vSphere

Figure 5 Citrix XenDesktop on VMware vSphere



Components of a Citrix XenDesktop architecture using Hosted VM include:

- **Virtual Desktop Agent**: The Virtual Desktop Agent (VDA) is installed on the virtual desktops and enables direct Independent Computing Architecture (ICA) connections between the virtual desktop and user devices with the Citrix online plug-in.
- **Desktop Delivery Controller**: The XenDesktop controllers are responsible for maintaining the proper level of idle desktops to allow for instantaneous connections, monitoring the state of online and connected virtual desktops and shutting down virtual desktops as needed. The primary XD controller is configured as the farm master server. The farm master is able to focus on its role of managing the farm when an additional XenDesktop Controller acts as a dedicated XML server. The XML server is responsible for user authentication, resource enumeration, and desktop launching process. A failure in the XML broker service will result in users being unable to start their desktops. This is why multiple controllers per farm are recommended.
- **Citrix Receiver**: Installed on user devices, Citrix Receiver enables direct HDX connections from user devices to virtual desktops. Receiver is a mobile workspace available on a range of platforms so users can connect to their Windows applications and desktops from devices of their choice. Receiver for Web is also available for devices that don’t support a native Receiver. Receiver incorporates the Citrix® ICA® client engine and other technologies needed to communicate directly with backend resources, such as StoreFront.
- **Citrix XenApp**: Citrix XenApp is an on-demand application delivery solution that enables any Windows application to be virtualized, centralized, managed in the data center, and instantly delivered as a service to users anywhere on any device. XenApp can be used to deliver both virtualized applications and virtualized desktops. In the Hosted VM model, XenApp is typically used for on-demand access to streamed and hosted applications.

- **Provisioning Services**: PVS creates and provisions virtual desktops from a single desktop image (vDisk) on demand, optimizing storage utilization and providing a pristine virtual desktop to each user every time they log on. Desktop provisioning also simplifies desktop images, provides the best flexibility, and offers fewer points of desktop management for both applications and desktops. The Trivial File Transfer Protocol (TFTP) and Pre-boot eXecution Environment (PXE) services are required for the virtual desktop to boot off the network and download the bootstrap file which instructs the virtual desktop to connect to the PVS server for registration and vDisk access instructions.
- **Personal vDisk**: Personal vDisk technology is a powerful new tool that provides the persistence and customization users want with the management flexibility IT needs in pooled VDI deployments. Personal vDisk technology gives these users the ability to have a personalized experience of their virtual desktop. Personal apps, data and settings are easily accessible each time they log on. This enables broader enterprise-wide deployments of pooled virtual desktops by storing a single copy of Windows centrally, and combining it with a personal vDisk for each employee, enhancing user personalization and reducing storage costs.
- **Hypervisor**: XenDesktop has an open architecture that supports the use of XenServer, Microsoft Hyper-V, or VMware vSphere. For the purposes of the testing documented in this paper, VMware vSphere was the hypervisor of choice.
- **Storefront**: Storefront is the next-generation of Web Interface and provides the user interface to the XenDesktop environment. Storefront broker user authentication, enumerates the available desktops and, upon launch, delivers an .ica file to Citrix Receiver on the user's local device to initiate a connection. Because StoreFront is a critical component, redundant servers must be available to provide fault tolerance.
- **License Server**: The Citrix License Server is responsible for managing the licenses for all of the components of XenDesktop. XenDesktop has a 90 day grace period which allows the system to function normally for 90 days if the license server becomes unavailable. This grace period offsets the complexity involved with building redundancy into the license server.
- **Data Store**: Each XenDesktop farm requires a database called the data store. Citrix XenDesktops use the data store to centralize configuration information for a farm in one location. The data store maintains all the static information about the XenDesktop environment.
- **Domain Controller**: The Domain Controller hosts Active Directory, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS). Active Directory provides a common namespace and secure method of communication between all the servers and desktops in the environment. DNS provides IP Host name resolution for the core XenDesktop infrastructure components. DHCP is used by the virtual desktop to request and obtain an IP address from the DHCP service. DHCP uses Option 66 and 67 to specify the bootstrap file location and file name to a virtual desktop. The DHCP service receives requests on UDP port 67 and sends data to UDP port 68 on a virtual desktop. The virtual desktops then have the operating system streamed over the network utilizing Citrix Provisioning Services (PVS).

All of the aforementioned components interact to provide a virtual desktop to an end user based on the FlexCast Hosted VM desktop delivery model leveraging the Provisioning Services feature of XenDesktop. This architecture provides the end user with a pristine desktop at each logon based on a centralized desktop image that is owned and managed by IT.

4.2.5 Citrix XenDesktop Hosted Shared Desktop Overview

In a typical large enterprise environment, IT will implement a mixture of Flexcast technologies to meet various workstyle needs. Like the test in this document, hosted shared desktops can be deployed alongside hosted VM desktops.

Host shared desktops has been a proven Citrix offering over many years and is deployed in some of the largest enterprises today due to its ease of deployment, reliability and scalability. Hosted shared desktops are appropriate for environments that have a standardized set of applications that do not deviate from one user to another. All users share the same desktop interface hosted on a Windows server in the backend datacenter. Hence, the level of desktop customization is limited compared to a Hosted VM desktop model.

If VM isolation is required and the ability to allocate resources to one user over another is important, the Hosted VM desktop should be the model of choice.

4.2.6 Citrix Machine Creation Services

Citrix Machine Creation Services (MCS) is the option for desktop image delivery used in this study. It uses the hypervisor APIs (XenServer, Hyper-V, and vSphere) to create, start, stop, and delete virtual machines. If you want to create a catalog of desktops with MCS, choose from the following:

- Pooled-Random: Pooled desktops are assigned to random users. When they logoff, the desktop is free for another user. When rebooted, any changes made are destroyed.
- Pooled-Static: Pooled desktops are permanently assigned to a single user. When a user logs off, only that user can use the desktop, regardless if the desktop is rebooted. During reboots, any changes made are destroyed.
- Pooled-Personal vDisk: Retains the single image management of pooled desktops while allowing the statically assigned user to install apps and change their desktop settings. These changes are stored on the users personal vDisk. The pooled desktop image is not altered with pooled with personal vDisk.
- Dedicated: Desktops are permanently assigned to a single user. When a user logs off, only that user can use the desktop, regardless if the desktop is rebooted. During reboots, any changes made will persist across subsequent startups.

In this study, Pooled-Random desktops were created and managed by Citrix Machine Creation Services.

4.3 EMC VNX Series

The VNX series delivers uncompromising scalability and flexibility for the mid-tier while providing market-leading simplicity and efficiency to minimize total cost of ownership. Customers can benefit from VNX features such as:

- Next-generation unified storage, optimized for virtualized applications.
- Extended cache by using Flash drives with Fully Automated Storage Tiering for Virtual Pools (FAST VP) and FAST Cache that can be optimized for the highest system performance and lowest storage cost simultaneously on both block and file.
- Multiprotocol supports for file, block, and object with object access through EMC Atmos™ Virtual Edition (Atmos VE).
- Simplified management with EMC Unisphere™ for a single management framework for all NAS, SAN, and replication needs.
- Up to three times improvement in performance with the latest Intel Xeon multicore processor technology, optimized for Flash.
- 6 Gb/s SAS back end with the latest drive technologies supported:
  - 3.5” 100 GB and 200 GB Flash, 3.5” 300 GB, and 600 GB 15k or 10k rpm SAS, and 3.5” 1 TB, 2 TB and 3 TB 7.2k rpm NL-SAS

  - 2.5” 100 GB and 200 GB Flash, 300 GB, 600 GB and 900 GB 10k rpm SAS

- Expanded EMC UltraFlex™ I/O connectivity—Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), Common Internet File System (CIFS), network file system (NFS) including parallel NFS (pNFS), Multi-Path File System (MPFS), and Fibre Channel over Ethernet (FCoE) connectivity for converged networking over Ethernet.

The VNX series includes five software suites and three software packs that make it easier and simpler to attain the maximum overall benefits.

Software suites available:

- VNX FAST Suite—Automatically optimizes for the highest system performance and the lowest storage cost simultaneously
- VNX Local Protection Suite—Practices safe data protection and repurposing.
- VNX Remote Protection Suite—Protects data against localized failures, outages, and disasters.
- VNX Application Protection Suite—Automates application copies and proves compliance.
- VNX Security and Compliance Suite—Keeps data safe from changes, deletions, and malicious activity.

Software packs available:

- VNX Total Efficiency Pack—Includes all five software suites (not available for VNX5100).
- VNX Total Protection Pack—Includes local, remote, and application protection suites.

4.3.1 EMC VNX5300 Used in Testing

EMC VNX 5300 provides storage by using FC (SAN) or IP (NAS) connections for virtual desktops, and infrastructure virtual machines such as Citrix XenDesktop controllers, VMware vCenter Servers, Microsoft SQL Server databases, and other supporting services. Optionally, user profiles and home directories are redirected to CIFS network shares on the VNX5300.

4.4 VMware ESXi 5.0

VMware, Inc. provides virtualization software. VMware’s enterprise software hypervisors for servers—VMware ESX, Vmware ESXi, and VSphere—are bare-metal embedded hypervisors that run directly on server hardware without requiring an additional underlying operating system.

4.4.1 VMware on ESXi 5.0 Hypervisor

ESXi 5.0 is a "bare-metal" hypervisor, so it installs directly on top of the physical server and partitions it into multiple virtual machines that can run simultaneously, sharing the physical resources of the underlying server. VMware introduced ESXi in 2007 to deliver industry-leading performance and scalability while setting a new bar for reliability, security and hypervisor management efficiency.

Due to its ultra-thin architecture with less than 100MB of code-base disk footprint, ESXi delivers industry-leading performance and scalability plus:

- **Improved Reliability and Security —** with fewer lines of code and independence from general purpose OS, ESXi drastically reduces the risk of bugs or security vulnerabilities and makes it easier to secure your hypervisor layer.

- **Streamlined Deployment and Configuration —** ESXi has far fewer configuration items than ESX, greatly simplifying deployment and configuration and making it easier to maintain consistency.
- **Higher Management Efficiency —** The API-based, partner integration model of ESXi eliminates the need to install and manage third party management agents. You can automate routine tasks by leveraging remote command line scripting environments such as vCLI or PowerCLI.
- **Simplified Hypervisor Patching and Updating —** Due to its smaller size and fewer components, ESXi requires far fewer patches than ESX, shortening service windows and reducing security vulnerabilities.

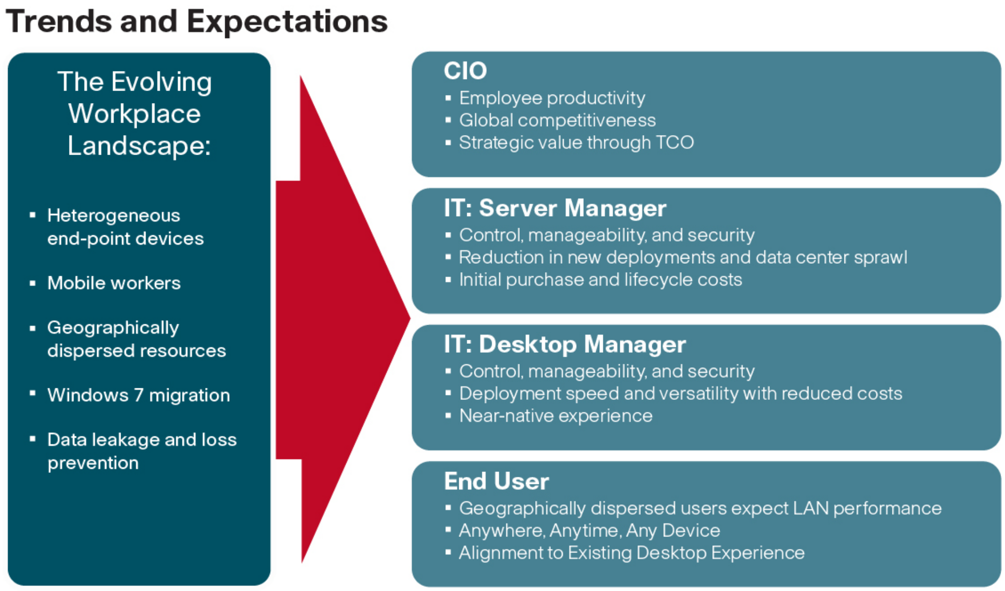
4.5 Modular Virtual Desktop Infrastructure Technical Overview

4.5.1 Modular Architecture

Today's IT departments are facing a rapidly-evolving workplace environment. The workforce is becoming increasingly diverse and geographically distributed and includes offshore contractors, distributed call center operations, knowledge and task workers, partners, consultants, and executives connecting from locations around the globe at all times.

An increasingly mobile workforce wants to use a growing array of client computing and mobile devices that they can choose based on personal preference. These trends are increasing pressure on IT to ensure protection of corporate data and to prevent data leakage or loss through any combination of user, endpoint device, and desktop access scenarios (Figure 6). These challenges are compounded by desktop refresh cycles to accommodate aging PCs and bounded local storage and migration to new operating systems, specifically Microsoft Windows 7.

Figure 6 The Evolving Workplace Landscape

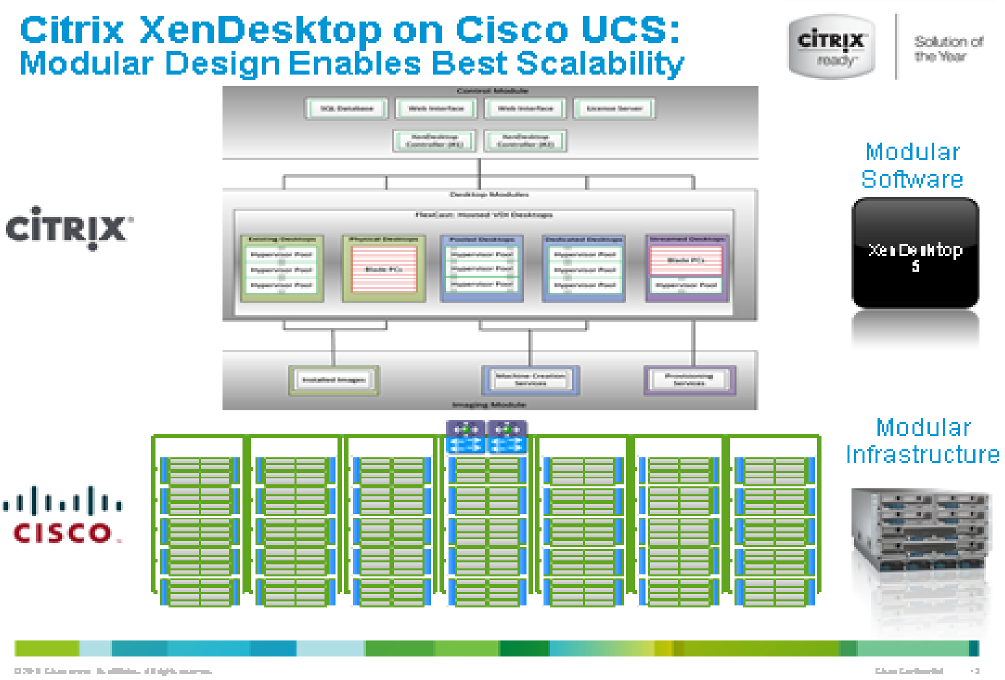

Trends and Expectations
The Evolving Workplace Landscape:
▪ Heterogeneous end-point devices
▪ Mobile workers
▪ Geographically dispersed resources
▪ Windows 7 migration
▪ Data leakage and loss prevention
CIO
▪ Employee productivity
▪ Global competitiveness
▪ Strategic value through TCO
IT: Server Manager
▪ Control, manageability, and security
▪ Reduction in new deployments and data center sprawl
▪ Initial purchase and lifecycle costs
IT: Desktop Manager
▪ Control, manageability, and security
▪ Deployment speed and versatility with reduced costs
▪ Near-native experience
End User
▪ Geographically dispersed users expect LAN performance
▪ Anywhere, Anytime, Any Device
▪ Alignment to Existing Desktop Experience

Some of the key drivers for desktop virtualization are increased data security and reduced TCO through increased control and reduced management costs.

4.5.1.1 Cisco Data Center Infrastructure for Desktop Virtualization

Cisco focuses on three key elements to deliver the best desktop virtualization data center infrastructure: simplification, security, and scalability. The software combined with platform modularity provides a simplified, secure, and scalable desktop virtualization platform (Figure 7).

Figure 7 Citirx XenDesktop on Cisco Unified Computing System



4.5.1.2 Simplified

Cisco UCS provides a radical new approach to industry standard computing and provides the heart of the data center infrastructure for desktop virtualization and the Cisco Virtualization Experience (VXI). Among the many features and benefits of Cisco UCS are the drastic reductions in the number of servers needed and number of cables per server and the ability to very quickly deploy or re-provision servers through Cisco UCS Service Profiles. With fewer servers and cables to manage and with streamlined server and virtual desktop provisioning, operations are significantly simplified. Thousands of desktops can be provisioned in minutes with Cisco Service Profiles and Cisco storage partners' storage-based cloning. This speeds time to productivity for end users, improves business agility, and allows IT resources to be allocated to other tasks.

IT tasks are further simplified through reduced management complexity, provided by the highly integrated Cisco UCS Manager, along with fewer servers, interfaces, and cables to manage and maintain. This is possible due to the industry-leading, highest virtual desktop density per blade of Cisco UCS along with the reduced cabling and port count due to the unified fabric and unified ports of Cisco UCS and desktop virtualization data center infrastructure.

Simplification also leads to improved and more rapid success of a desktop virtualization implementation. Cisco and its partners –Citrix (XenDesktop and Provisioning Server) and EMC – have developed integrated, validated architectures, including available pre-defined, validated infrastructure packages, known as Cisco Solutions for VSPEX.

4.5.1.3 Secure

While virtual desktops are inherently more secure than their physical world predecessors, they introduce new security considerations. Desktop virtualization significantly increases the need for virtual machine-level awareness of policy and security, especially given the dynamic and fluid nature of virtual machine mobility across an extended computing infrastructure. The ease with which new virtual desktops can proliferate magnifies the importance of a virtualization-aware network and security infrastructure. Cisco UCS and Nexus data center infrastructure for desktop virtualization provides stronger data center, network, and desktop security with comprehensive security from the desktop to the hypervisor. Security is enhanced with segmentation of virtual desktops, virtual machine-aware policies and administration, and network security across the LAN and WAN infrastructure.

4.5.1.4 Scalable

Growth of a desktop virtualization solution is all but inevitable and it is critical to have a solution that can scale predictably with that growth. The Cisco solution supports more virtual desktops per server and additional servers scale with near linear performance. Cisco data center infrastructure provides a flexible platform for growth and improves business agility. Cisco UCS Service Profiles allow for on-demand desktop provisioning, making it easy to deploy dozens or thousands of additional desktops.

Each additional Cisco UCS blad server provides near linear performance and utilizes Cisco's dense memory servers and unified fabric to avoid desktop virtualization bottlenecks. The high performance, low latency network supports high volumes of virtual desktop traffic, including high resolution video and communications.

Cisco Unified Computing System and Nexus data center infrastructure is an ideal platform for growth, with transparent scaling of server, network, and storage resources to support desktop virtualization.

4.5.1.5 Savings and Success

As demonstrated above, the simplified, secure, scalable Cisco data center infrastructure solution for desktop virtualization will save time and cost. There will be faster payback, better ROI, and lower TCO with the industry's highest virtual desktop density per server, meaning there will be fewer servers needed, reducing both capital expenditures (CapEx) and operating expenditures (OpEx). There will also be much lower network infrastructure costs, with fewer cables per server and fewer ports required, via the Cisco UCS architecture and unified fabric.

The simplified deployment of Cisco Unified Computing System for desktop virtualization speeds up time to productivity and enhances business agility. IT staff and end users are more productive more quickly and the business can react to new opportunities by simply deploying virtual desktops whenever and wherever they are needed. The high performance Cisco systems and network deliver a near-native end-user experience, allowing users to be productive anytime, anywhere.

4.5.2 Understanding Desktop User Groups

There must be a considerable effort within the enterprise to identify desktop user groups and their memberships. The most broadly recognized, high level user groups are:

- **Task Workers**?Groups of users working in highly specialized environments where the number of tasks performed by each worker is essentially identical. These users are typically located at a corporate facility (e.g., call center employees).

- **Knowledge/Office Workers**?Groups of users who use a relatively diverse set of applications that are Web-based and installed and whose data is regularly accessed. They typically have several applications running simultaneously throughout their workday and a requirement to utilize Flash video for business purposes. This is not a singular group within an organization. These workers are typically located at a corporate office (e.g., workers in accounting groups).
- **Power Users**?Groups of users who run high-end, memory, processor, disk IO, and/or graphic-intensive applications, often simultaneously. These users have high requirements for reliability, speed, and real-time data access (e.g., design engineers).
- **Mobile Workers**?Groups of users who may share common traits with Knowledge/Office Workers, with the added complexity of needing to access applications and data from wherever they are?whether at a remote corporate facility, customer location, at the airport, at a coffee shop, or at home?all in the same day (e.g., a company's outbound sales force).
- **Remote Workers**?Groups of users who could fall into the Task Worker or Knowledge/Office Worker groups but whose experience is from a remote site that is not corporate owned, most often from the user's home. This scenario introduces several challenges in terms of type, available bandwidth, and latency and reliability of the user's connectivity to the data center (for example, a work-from-home accounts payable representative).
- **Guest/Contract Workers**?Groups of users who need access to a limited number of carefully controlled enterprise applications and data and resources for short periods of time. These workers may need access from the corporate LAN or remote access (for example, a medical data transcriptionist).

There is good reason to search for and identify multiple sub-groups of the major groups listed above in the enterprise. Typically, each sub-group has different application and data requirements.

4.5.3 Understanding Applications and Data

When the desktop user groups and sub-groups have been identified, the next task is to catalog group application and data requirements. This can be one of the most time-consuming processes in the VDI planning exercise, but is essential for the VDI project's success. If the applications and data are not identified and co-located, performance will be negatively affected.

The process of analyzing the variety of application and data pairs for an organization will likely be complicated by the inclusion cloud applications, like SalesForce.com. This application and data analysis is beyond the scope of this Cisco Validated Design, but should not be omitted from the planning process. There are a variety of third party tools available to assist organizations with this crucial exercise.

4.5.4 Project Planning and Solution Sizing Sample Questions

Now that user groups, their applications and their data requirements are understood, some key project and solution sizing questions may be considered.

General project questions should be addressed at the outset, including:

- Has a VDI pilot plan been created based on the business analysis of the desktop groups, applications and data?
- Is there infrastructure and budget in place to run the pilot program?
- Are the required skill sets to execute the VDI project available? Can we hire or contract for them?
- Do we have end user experience performance metrics identified for each desktop sub-group?
- How will we measure success or failure?

- What is the future implication of success or failure?

Provided below is a short, non-exhaustive list of sizing questions that should be addressed for each user sub-group:

- What is the desktop OS planned? Windows 7 or Windows XP?
- 32 bit or 64 bit desktop OS?
- How many virtual desktops will be deployed in the pilot? In production? All Windows 7?
- How much memory per target desktop group desktop?
- Are there any rich media, Flash, or graphics-intensive workloads?
- What is the end point graphics processing capability?
- Will XenApp be used for Hosted Shared Server Desktops or exclusively XenDesktop?
- Are there XenApp hosted applications planned? Are they packaged or installed?
- Will Provisioning Server or Machine Creation Services be used for virtual desktop deployment?
- What is the hypervisor for the solution?
- What is the storage configuration in the existing environment?
- Are there sufficient IOPS available for the write-intensive VDI workload?
- Will there be storage dedicated and tuned for VDI service?
- Is there a voice component to the desktop?
- Is anti-virus a part of the image?
- Is user profile management (e.g., non-roaming profile based) part of the solution?
- What is the fault tolerance, failover, disaster recovery plan?
- Are there additional desktop sub-group specific questions?

4.5.5 Cisco Services

Cisco offers assistance for customers in the analysis, planning, implementation, and support phases of the VDI lifecycle. These services are provided by the Cisco Advanced Services group. Some examples of Cisco services include:

- Cisco VXI Unified Solution Support
- Cisco VXI Desktop Virtualization Strategy Service
- Cisco VXI Desktop Virtualization Planning and Design Service

4.5.6 The Solution: A Unified, Pre-Tested and Validated Infrastructure

To meet the challenges of designing and implementing a modular desktop infrastructure, Cisco, Citrix, EMC and VMware have collaborated to create the data center solution for virtual desktops outlined in this document.

Key elements of the solution include:

- A shared infrastructure that can scale easily
- A shared infrastructure that can accommodate a variety of virtual desktop workloads

4.6 Cisco Networking Infrastructure

This section describes the Cisco networking infrastructure components used in the configuration.

4.6.1 Cisco Nexus 5548UP Switch (Unmanaged FC Variant Only)

Two Cisco Nexus 5548UP access switches are 1RU 10 Gigabit Ethernet, Fibre Channel, and FCoE switch offering up to 960 Gbps of throughput and up to 48 ports. The switch has 32 unified ports and one expansion slot. The Cisco Nexus 5500 platform can be equipped with an expansion module that can be used to increase the number of 10 Gigabit Ethernet and FCoE ports or to connect to Fibre Channel SANs with 8/4/2/1-Gbps Fibre Channel switch ports, or both. (Not required for this study.)

The switch has a single serial console port and a single out-of-band 10/100/1000-Mbps Ethernet management port. Two N+1 redundant, hot-pluggable power supplies and five N+1 redundant, hot-pluggable fan modules provide highly reliable front-to-back cooling.

4.6.2 Cisco Nexus 2232PP Fabric Extender (Managed FC Variant Only)

The Cisco Nexus 2232PP 10G provides 32 10 Gb Ethernet and Fibre Channel Over Ethernet (FCoE) Small Form-Factor Pluggable Plus (SFP+) server ports and eight 10 Gb Ethernet and FCoE SFP+ uplink ports in a compact 1 rack unit (1RU) form factor.

Two Nexus 2232PP 10GE Fabric Extenders were deployed to provide cluster-mode single wire management to the Cisco UCS C220 M3 rack servers.

Four of eight available 10 GbE uplinks from each Nexus 2232 were utilized to provide 40 Gb of bandwidth between the UCS 6248UP Fabric Interconnects and the Cisco UCS C220 M3 rack servers.

5 Architecture and Design of XenDesktop 5.6 on Cisco Unified Computing System and EMC VNX Storage

5.1 Design Fundamentals

There are many reasons to consider a virtual desktop solution such as an ever growing and diverse base of user devices, complexity in management of traditional desktops, security, and even Bring Your Own Computer (BYOC) to work programs. The first step in designing a virtual desktop solution is to understand the user community and the type of tasks that are required to successfully execute their role. The following user classifications are provided:

- **Knowledge Workers** today do not just work in their offices all day – they attend meetings, visit branch offices, work from home, and even coffee shops. These anywhere workers expect access to all of their same applications and data wherever they are.
- **External Contractors** are increasingly part of your everyday business. They need access to certain portions of your applications and data, yet administrators still have little control over the devices they use and the locations they work from. Consequently, IT is stuck making trade-offs on the cost of providing these workers a device vs. the security risk of allowing them access from their own devices.

- **Task Workers** perform a set of well-defined tasks. These workers access a small set of applications and have limited requirements from their PCs. However, since these workers are interacting with your customers, partners, and employees, they have access to your most critical data.
- **Mobile Workers** need access to their virtual desktop from everywhere, regardless of their ability to connect to a network. In addition, these workers expect the ability to personalize their PCs, by installing their own applications and storing their own data, such as photos and music, on these devices.
- **Shared Workstation** users are often found in state-of-the-art university and business computer labs, conference rooms or training centers. Shared workstation environments have the constant requirement to re-provision desktops with the latest operating systems and applications as the needs of the organization change, tops the list.

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

- **Traditional PC:** A traditional PC is what ?typically? constituted a desktop environment: physical device with a locally installed operating system.
- **Hosted Shared Desktop:** A hosted, server-based desktop is a desktop where the user interacts through a delivery protocol. With hosted, server-based desktops, a single installed instance of a server operating system, such as Microsoft Windows Server 2008 R2, is shared by multiple users simultaneously. Each user receives a desktop "session" and works in an isolated memory space. Changes made by one user could impact the other users.
- **Hosted Virtual Desktop:** A hosted virtual desktop is a virtual desktop running either on virtualization layer (XenServer, Hyper-V or ESX) or on bare metal hardware. The user does not work with and sit in front of the desktop, but instead the user interacts through a delivery protocol.
- **Streamed Applications:** Streamed desktops and applications run entirely on the user‘s local client device and are sent from a server on demand. The user interacts with the application or desktop directly but the resources may only available while they are connected to the network.
- **Local Virtual Desktop:** A local virtual desktop is a desktop running entirely on the user‘s local device and continues to operate when disconnected from the network. In this case, the user’s local device is used as a type 1 hypervisor and is synced with the data center when the device is connected to the network.

For the purposes of the validation represented in this document only hosted virtual desktops were validated. Each of the sections provides some fundamental design decisions for this environment.

5.2 Hosted VDI Design Fundamentals

Citrix XenDesktop 5.6 can be used to deliver a variety of virtual desktop configurations. When evaluating a Hosted VDI deployment, consider the following:

5.2.1 Hypervisor Selection

Citrix XenDesktop is hypervisor agnostic, so any of the following three hypervisors can be used to hosted VDI-baseddesktops:

- Hyper-V: Microsoft Windows Server 2008 R2 Hyper-V builds on the architecture and functions of Windows Server 2008 Hyper-V by adding multiple new features that enhance product flexibility. Hyper-V is available in a Standard, Server Core and free Hyper-V Server 2008 R2 versions. More information on Hyper-V can be obtained at the company web site.
- vSphere: VMware vSphere consists of the management infrastructure or virtual center server software and the hypervisor software that virtualizes the hardware resources on the servers. It offers features like Distributed resource scheduler, vMotion, HA, Storage vMotion, VMFS, and a mutlipathing storage layer. More information on vSphere can be obtained at the company website.
- XenServer: Citrix® XenServer® is a complete, managed server virtualization platform built on the powerful Xen® hypervisor. Xen technology is widely acknowledged as the fastest and most secure virtualization software in the industry. XenServer is designed for efficient management of Windows® and Linux® virtual servers and delivers cost-effective server consolidation and business continuity. More information on Hyper-V can be obtained at the company website.

For this study, we utilized VMware ESXi 5.0 Update 1 and vCenter 5.0 Update 1.

5.2.2 XenDesktop 5.6 Desktop Broker

The Citrix XenDesktop 5.6 broker provides two methods of creating hosted virtual desktops:

- Citrix Provisioning Services
- Citrix Machine Creation Services

Citrix Machine Creation Services, which is integrated directly with the XenDesktop Studio console, was used for this study.

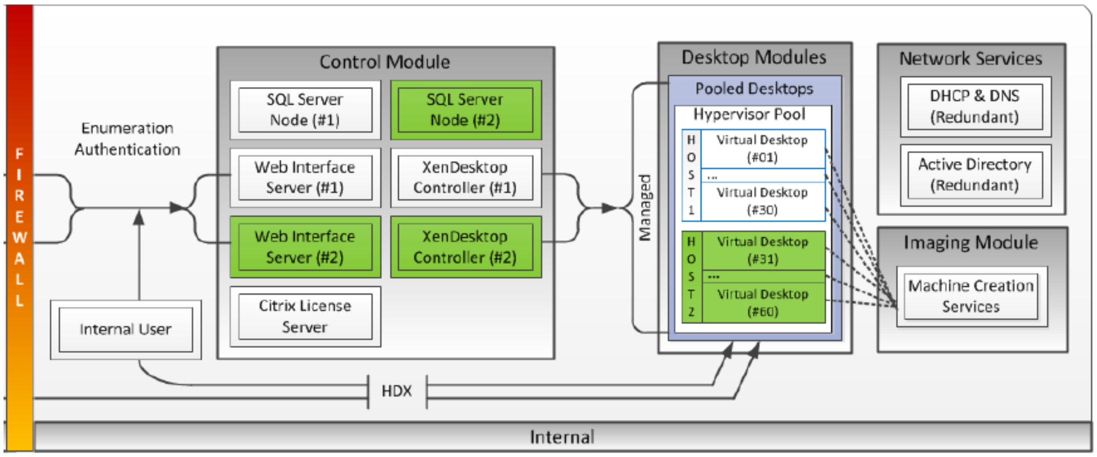
It provides the ability to create seven types of virtual machines with random or static (assigned) users:

- Pooled
- Pooled with personal vDisk
- Dedicated
- Existing
- Physical
- Streamed
- Streamed with personal vDisk

5.3 Designing a Citrix XenDesktop 5.6 Deployment

To implement our pooled desktop delivery model for this study, known as Hosted VDI Pooled Desktops, we followed the Citrix Reference Architecture for local desktop delivery.

Figure 8 Pooled Desktop Infrastructure



To read about Citrix's XenDesktop Reference Architecture – Pooled Desktops (Local and Remote) go to the following link:

http://support.citrix.com/article/CTX131049

To learn more about XenDesktop 5.6 Planning and Design go to the following link:

http://support.citrix.com/product/xd/v5.5/consulting/

5.4 Storage Architecture Design

Designing for this workload involves the deployment of many disks to handle brief periods of extreme I/O pressure, which is expensive to implement. This solution uses EMC VNX FAST Cache to reduce the number of disks required.

VNX multi-protocol support enables use of either Fibre Channel SAN-connected block storage or 10-gigabit Ethernet (GbE) connected NFS for flexible, cost effective, and easily deployable storage for VMware-based desktop virtualization.

The storage architecture use in this study was validated to support 600 hosted virtual desktops using Citrix Machine Creation Services for virtual machine provisioning and management.

Section 6.5 EMC VNX5300 Storage Configuration provides details on the storage architecture used for this solution.

6 Solution Validation

This section details the configuration and tuning that was performed on the individual components to produce a complete, validated solution.

6.1 Configuration Topology for Scalable Citrix XenDesktop 5.6 Virtual Desktop Infrastructure on Cisco Unified Computing System and EMC Storage

There are two variants of the configuration topology for this solution:

- Managed Fibre Channel Variant
- Unmanaged NFS Variant

Diagrams for each variant are shown in the following sections.

Figure 9 Architecture Block Diagram-Single Wire Managed Fibre Channel Variant

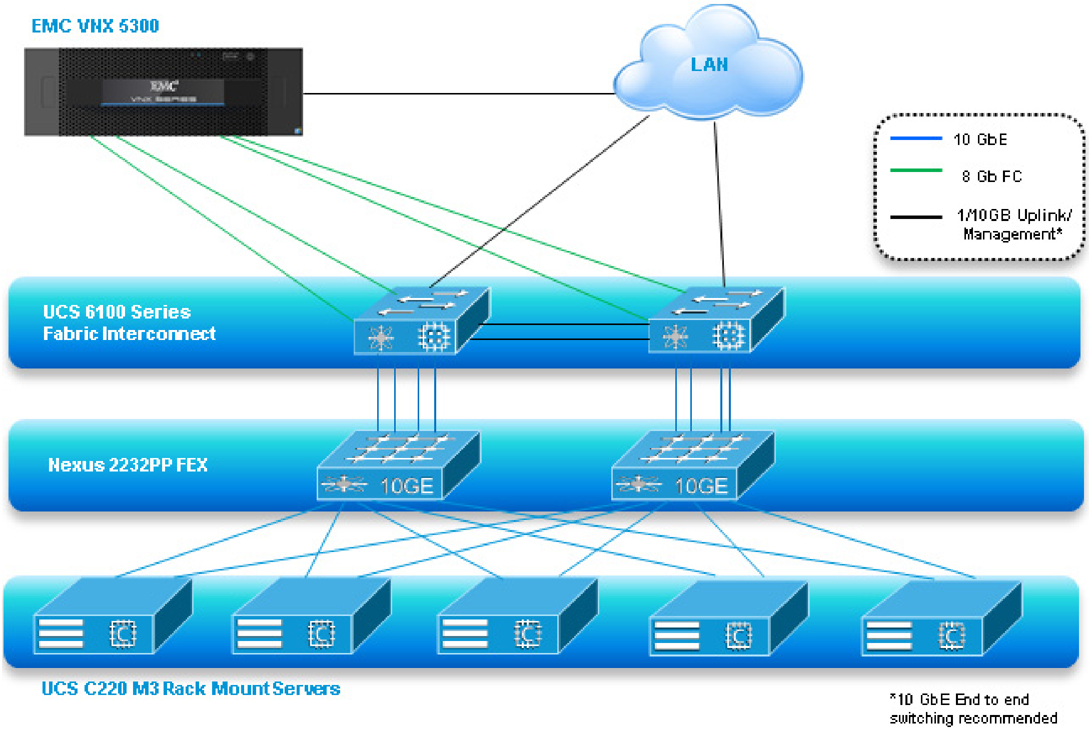
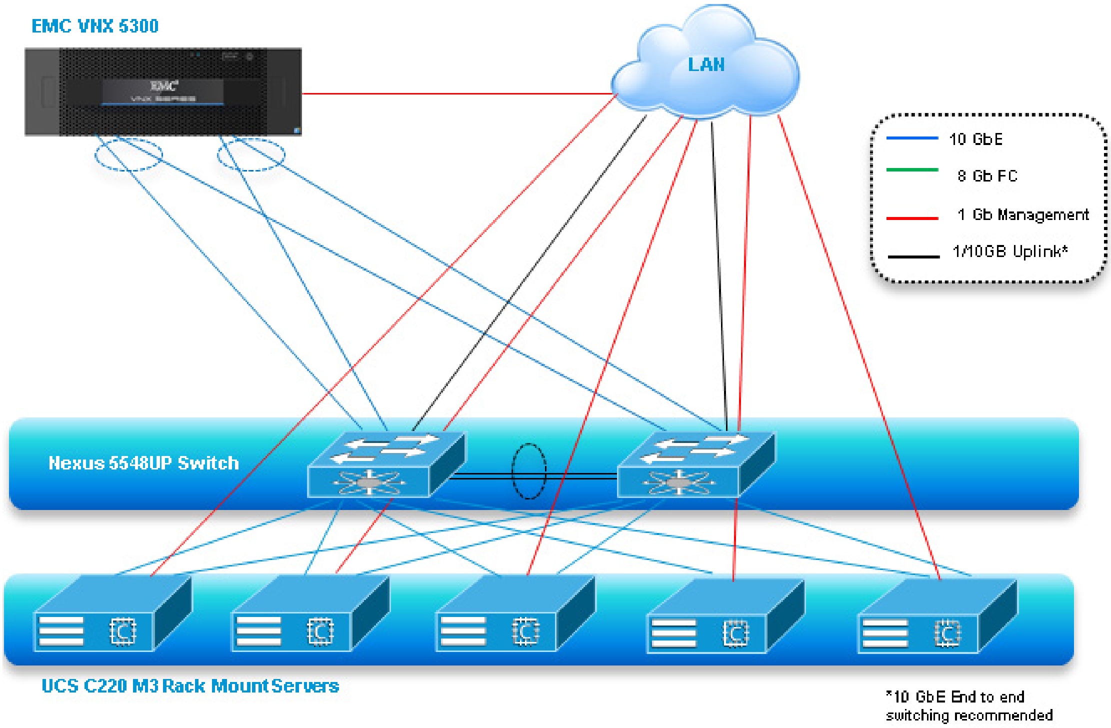

EMC VNX 5300
LAN
10 GbE
8 Gb FC
1/10GB Uplink/ Management*
UCS 6100 Series Fabric Interconnect
Nexus 2232PP FEX
10GE
10GE
UCS C220 M3 Rack Mount Servers
*10 GbE End to end switching recommended

Figure 10 Architecture Block Diagram-Unmanaged NFS Variant



The figures above capture the architectural diagram for the purpose of this study. The architecture is divided into four distinct layers:

- Cisco UCS Compute Platform
- The Virtual Desktop Infrastructure that runs on Cisco UCS blade hypervisor hosts
- Network Access layer and LAN
- Storage Access Network (SAN) and EMC VNX Storage array

The following figure details the physical configuration of the 500-600 seat XenDesktop 5.6 environment.

Figure 11 Detailed Architecture of the Configuration for the Single Wire Managed Fibre Channel Variant

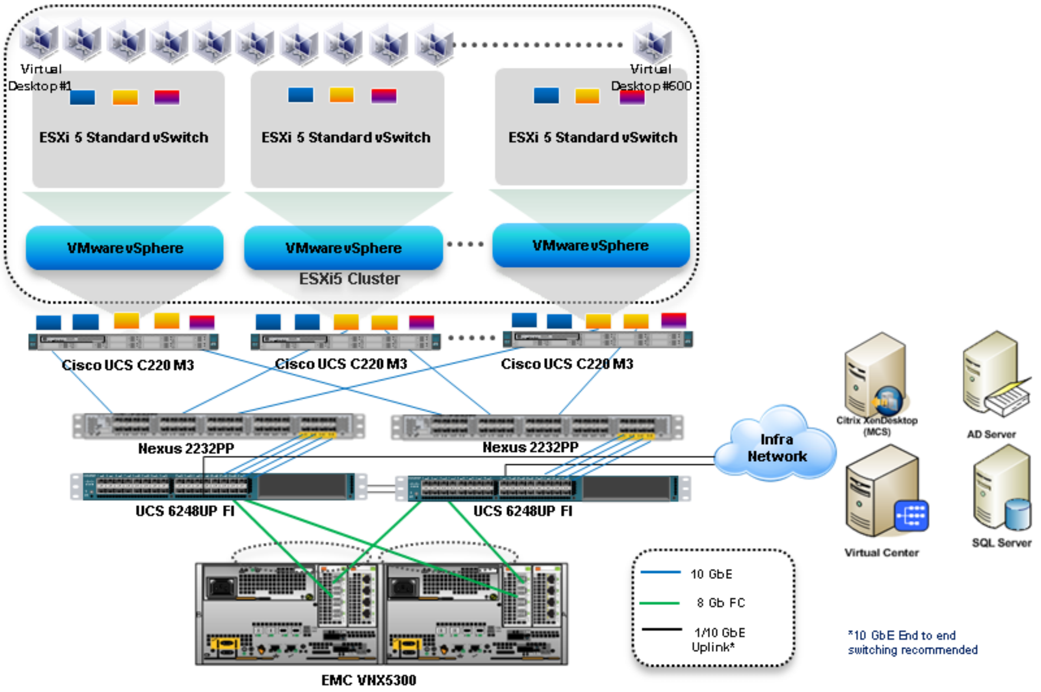
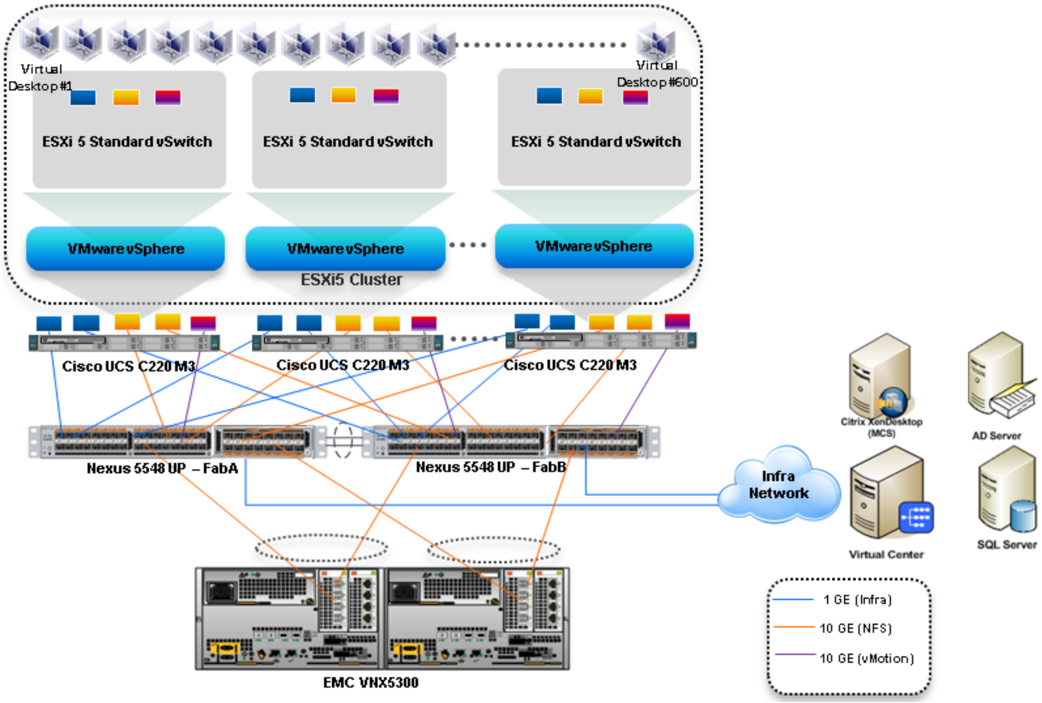


Figure 12 Detailed Architecture of the Configuration for the Unmanaged NFS Variant



Note The figure above does not include the 1 x 1Gb management connection from each unmanaged Cisco UCS C220 M3 to the Infrastructure Network.

6.2 Cisco Unified Computing System Configuration (Managed FC Variant Only)

This section talks about the Cisco UCS configuration that was done as part of the infrastructure build out. The racking, power and installation of the chassis are described in the install guide (see http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/ucs5108_install.html) and it is beyond the scope of this document. More details on each step can be found in the following documents:

- Cisco UCS CLI Configuration guide http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.1/b_UCSM_CLI_Configuration_Guide_2_1.pdf
- Cisco UCS Manager GUI Configuration guide http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/gui/config/guide/2.1/b_UCSM_GUI_Configuration_Guide_2_1.html

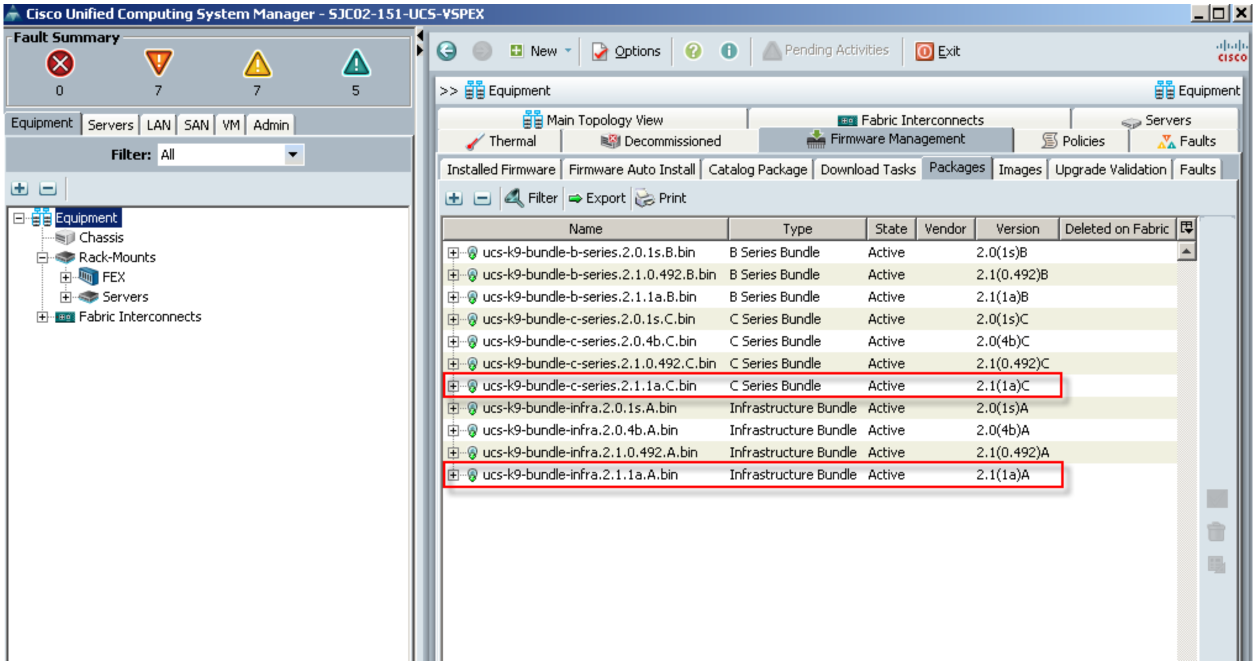
6.2.1 Base Cisco UCS System Configuration

To configure the Cisco Unified Computing System, perform the following steps:

1 Bring up the Fabric interconnect and from a Serial Console connection set the IP address, gateway, and the hostname of the primary fabric interconnect. Now bring up the second fabric interconnect after connecting the dual cables between them. The second fabric interconnect automatically recognizes the primary and ask if you want to be part of the cluster, answer yes and set the IP address, gateway and the hostname. Once this is done all access to the FI can be done remotely. You will also configure the virtual IP address to connect to the FI, you need a total of three IP address to bring it online. You can also wire up the chassis to the FI, using either 1, 2 or 4 links per IO Module, depending on your application bandwidth requirement. We connected all the four links to each module.

2 Now connect using your favorite browser to the Virtual IP and launch the Cisco UCS-Manager. The Java based Cisco UCS Manager will let you do everything that you could do from the CLI. We will highlight the GUI methodology here.

3 First check the firmware on the system and see if it is current. Visit http://software.cisco.com/download/release.html?mdfid=283612660&softwareid=283655658&release=2.0(4d)&relind=AVAILABLE&rellifecycle=&reltype=latest to download the most current UCS Infrastructure and UCS Manager software. Use the UCS Manager Equipment tab in the left pane, then the Firmware Management tab in the right pane and Packages sub-tab to view the packages on the system. Use the Download Tasks tab to download needed software to the FI. The firmware release used in this paper is 2.1(1a).

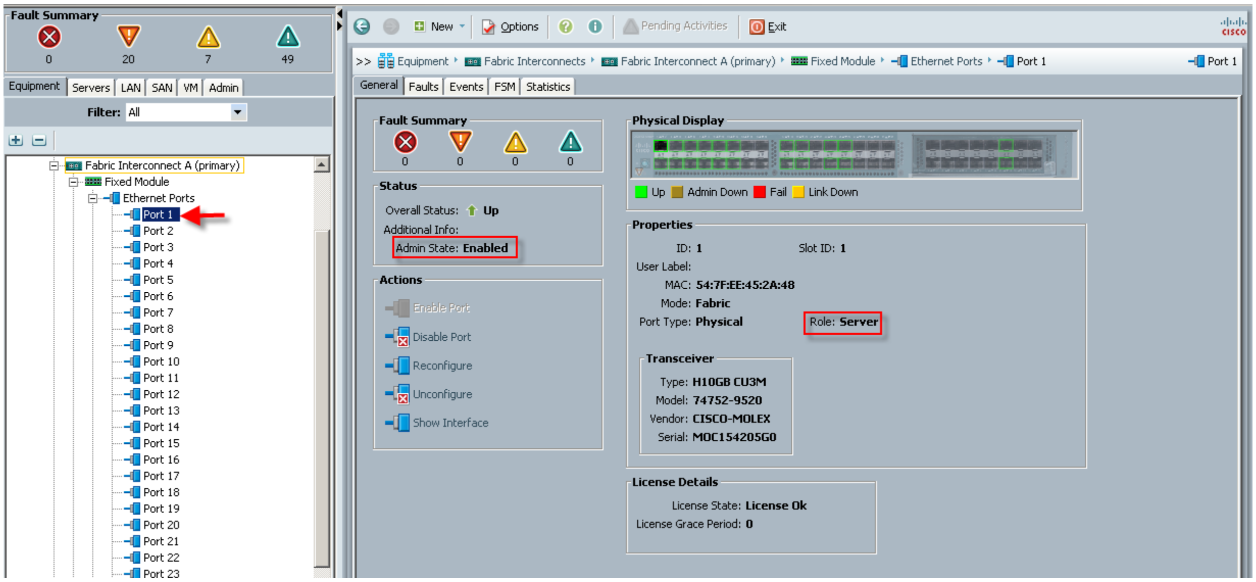


Name	Type	State	Vendor	Version	Deleted on Fabric
ucs-k9-bundle-b-series.2.0.1s.B.bin	B Series Bundle	Active		2.0(1s)B	
ucs-k9-bundle-b-series.2.1.0.492.B.bin	B Series Bundle	Active		2.1(0.492)B	
ucs-k9-bundle-b-series.2.1.1a.B.bin	B Series Bundle	Active		2.1(1a)B	
ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active		2.0(1s)C	
ucs-k9-bundle-c-series.2.0.4b.C.bin	C Series Bundle	Active		2.0(4b)C	
ucs-k9-bundle-c-series.2.1.0.492.C.bin	C Series Bundle	Active		2.1(0.492)C	
ucs-k9-bundle-c-series.2.1.1a.C.bin	C Series Bundle	Active		2.1(1a)C	
ucs-k9-bundle-infra.2.0.1s.A.bin	Infrastructure Bundle	Active		2.0(1s)A	
ucs-k9-bundle-infra.2.0.4b.A.bin	Infrastructure Bundle	Active		2.0(4b)A	
ucs-k9-bundle-infra.2.1.0.492.A.bin	Infrastructure Bundle	Active		2.1(0.492)A	
ucs-k9-bundle-infra.2.1.1a.A.bin	Infrastructure Bundle	Active		2.1(1a)A	

If the firmware is not current, follow the installation and upgrade guide to upgrade the Cisco UCS Manager firmware. We will use UCS Policy in Service Profiles later in this document to update all Cisco UCS components in the solution.

Note: The Bios and Board Controller version numbers do not track the IO Module, Adapter, nor CIMC controller version numbers in the packages.

4 Configure and enable the server ports on the FI. These are the ports that will connect the chassis to the FIs.



Status

Overall Status: Up

Additional Info:

Admin State: Enabled

Properties

ID: 1 Slot ID: 1

User Label:

MAC: 54:7F:EE:45:2A:48

Mode: Fabric

Port Type: Physical Role: Server

Transceiver

Type: H10GB CU3M

Model: 74752-9520

Vendor: CISCO-MOLEX

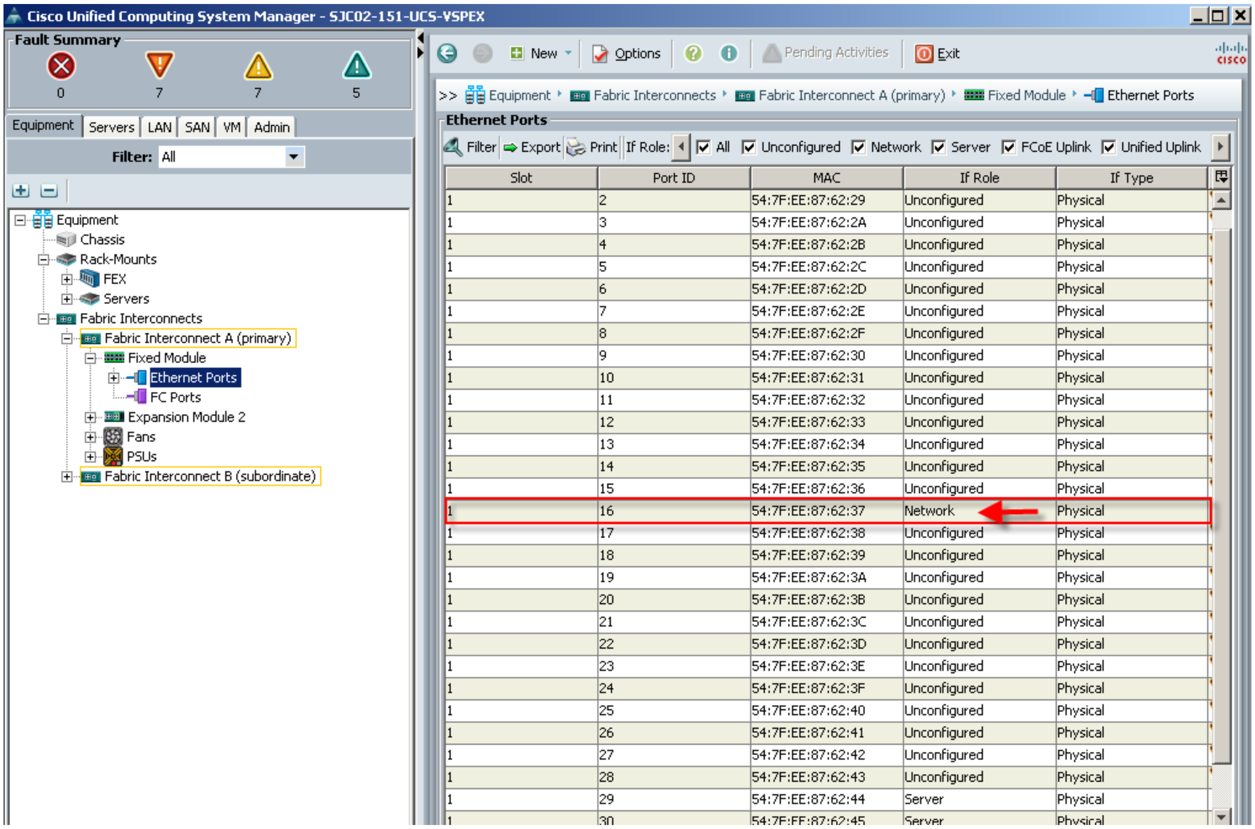
Serial: MOC154205G0

License Details

License State: License Ok

License Grace Period: 0

5 Configure and enable at least one uplink Ethernet ports to connect the Cisco Unified Computing System to your LAN:



Ethernet Ports

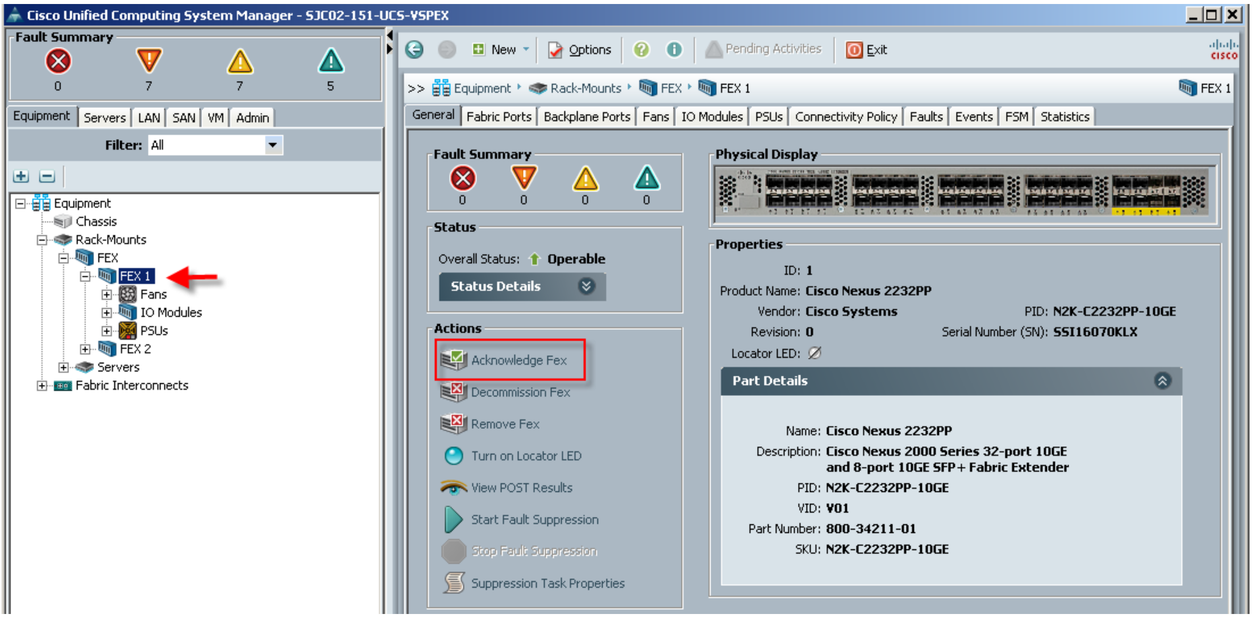
If Role: ☑ All ☑ Unconfigured ☑ Network ☑ Server ☑ FCoE Uplink ☑ Unified Uplink

Slot	Port ID	MAC	If Role	If Type
1	2	54:7F:EE:87:62:29	Unconfigured	Physical
1	3	54:7F:EE:87:62:2A	Unconfigured	Physical
1	4	54:7F:EE:87:62:2B	Unconfigured	Physical
1	5	54:7F:EE:87:62:2C	Unconfigured	Physical
1	6	54:7F:EE:87:62:2D	Unconfigured	Physical
1	7	54:7F:EE:87:62:2E	Unconfigured	Physical
1	8	54:7F:EE:87:62:2F	Unconfigured	Physical
1	9	54:7F:EE:87:62:30	Unconfigured	Physical
1	10	54:7F:EE:87:62:31	Unconfigured	Physical
1	11	54:7F:EE:87:62:32	Unconfigured	Physical
1	12	54:7F:EE:87:62:33	Unconfigured	Physical
1	13	54:7F:EE:87:62:34	Unconfigured	Physical
1	14	54:7F:EE:87:62:35	Unconfigured	Physical
1	15	54:7F:EE:87:62:36	Unconfigured	Physical
1	16	54:7F:EE:87:62:37	Network	Physical
1	17	54:7F:EE:87:62:38	Unconfigured	Physical
1	18	54:7F:EE:87:62:39	Unconfigured	Physical
1	19	54:7F:EE:87:62:3A	Unconfigured	Physical
1	20	54:7F:EE:87:62:3B	Unconfigured	Physical
1	21	54:7F:EE:87:62:3C	Unconfigured	Physical
1	22	54:7F:EE:87:62:3D	Unconfigured	Physical
1	23	54:7F:EE:87:62:3E	Unconfigured	Physical
1	24	54:7F:EE:87:62:3F	Unconfigured	Physical
1	25	54:7F:EE:87:62:40	Unconfigured	Physical
1	26	54:7F:EE:87:62:41	Unconfigured	Physical
1	27	54:7F:EE:87:62:42	Unconfigured	Physical
1	28	54:7F:EE:87:62:43	Unconfigured	Physical
1	29	54:7F:EE:87:62:44	Server	Physical
1	30	54:7F:EE:87:62:45	Server	Physical

From the Equipment tab with one of the two Fabric Interconnects highlighted in the navigation pane, use the Configure Unified Ports in the Actions panel on the General tab, to configure FC Storage ports. **Note**: In this example, we configured four FC Storage ports, two of which are in use. Ports to the left of the slider shown above are Ethernet ports. Ports to the right of the slider are Fibre Channel ports.

5a Connect four uplink ports on each of the Nexus 2232PP Fabric Extenders to four server ports on one of the Cisco UCS Fabric Interconnects. (All four to one Fabric Interconnect.) Power the Nexus 2232PPs on.

6 Expand the Rack-Mounts, FEX node in the left pane of the UCS Manager console, the click on each FEX in the left pane, then click Acknowledge FEX in the right pane to bring the FEX online and enable server discovery.



Cisco Unified Computing System Manager - SJC02-151-UCS-VSPEX

Overall Status: Operable

ID: 1
Product Name: Cisco Nexus 2232PP
Vendor: Cisco Systems
PID: N2K-C2232PP-10GE
Revision: 0
Serial Number (SN): SSI16070KLX
Locator LED: ∅

Name: Cisco Nexus 2232PP
Description: Cisco Nexus 2000 Series 32-port 10GE and 8-port 10GE SFP+ Fabric Extender
PID: N2K-C2232PP-10GE
VID: V01
Part Number: 800-34211-01
SKU: N2K-C2232PP-10GE

7 Repeat the procedure for FEX2.

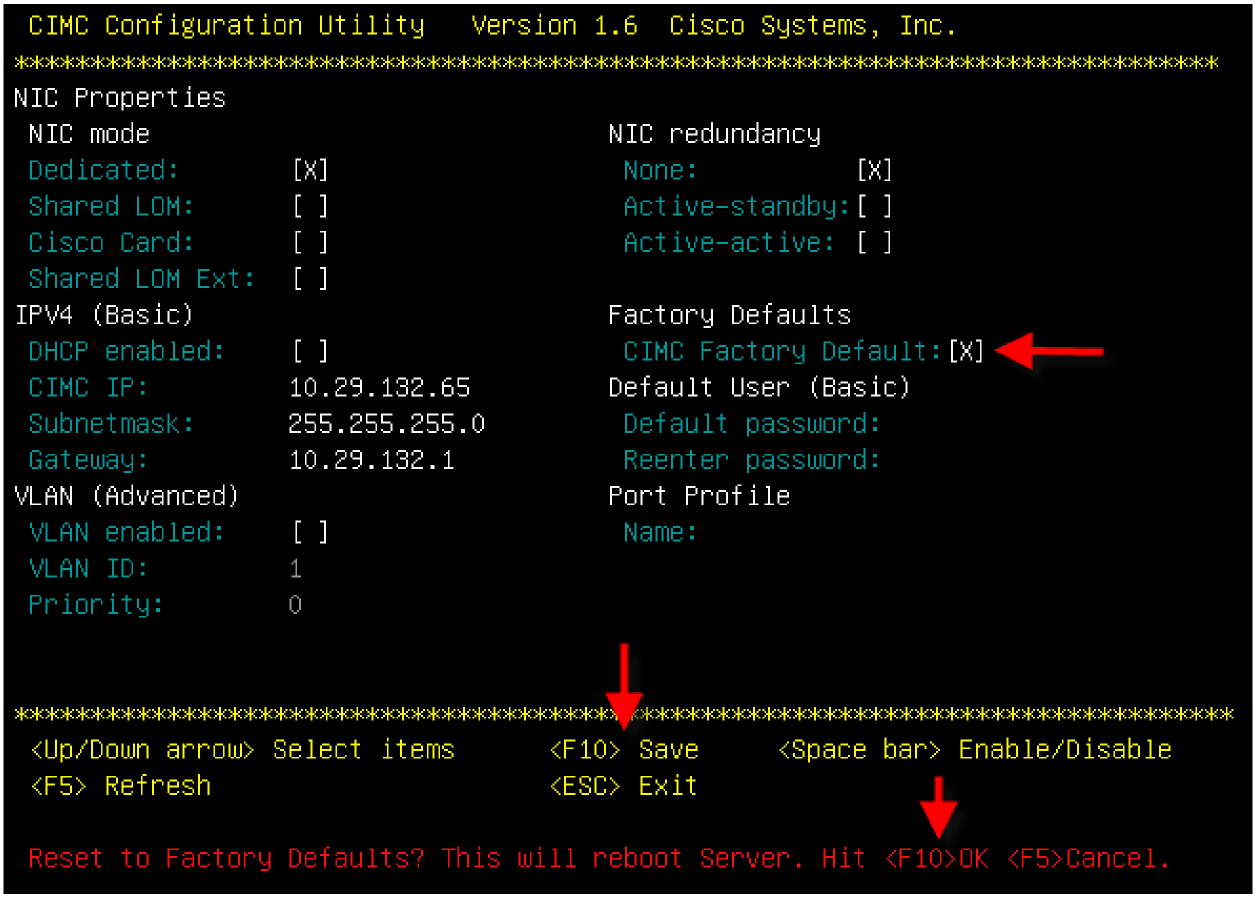
8 Download the UCS C220 M3 Rack Server Software version 1.4.(7a) or later from:

http://software.cisco.com/download/release.html?mdfid=284296253&flowid=31742&softwareid=283850974&release=1.4(7a)1&relind=null&rellifecycle=null&reltype=null&i=rb

8.1 Burn the software to a CD.

8.2 Insert the CD into each UCS C220 M3, restart the server, press F6 during the post process to view the boot menu, select the CD Rom for the boot device and update all components via the menu.

8.3 After the server firmware and CIMC have been updated, during the restart, press F8 to access the server CIMC.



```
 CIMC Configuration Utility   Version 1.6  Cisco Systems, Inc.
********************************************************************************
NIC Properties
 NIC mode                              NIC redundancy
 Dedicated:        [X]                  None:           [X]
 Shared LOM:       [ ]                  Active-standby:[ ]
 Cisco Card:       [ ]                  Active-active: [ ]
 Shared LOM Ext:   [ ]
IPV4 (Basic)                           Factory Defaults
 DHCP enabled:     [ ]                  CIMC Factory Default:[X]
 CIMC IP:          10.29.132.65        Default User (Basic)
 Subnetmask:       255.255.255.0        Default password:
 Gateway:          10.29.132.1          Reenter password:
VLAN (Advanced)                        Port Profile
 VLAN enabled:     [ ]                  Name:
 VLAN ID:          1
 Priority:         0


********************************************************************************
 <Up/Down arrow> Select items      <F10> Save     <Space bar> Enable/Disable
 <F5> Refresh                      <ESC> Exit

 Reset to Factory Defaults? This will reboot Server. Hit <F10>OK <F5>Cancel.
```

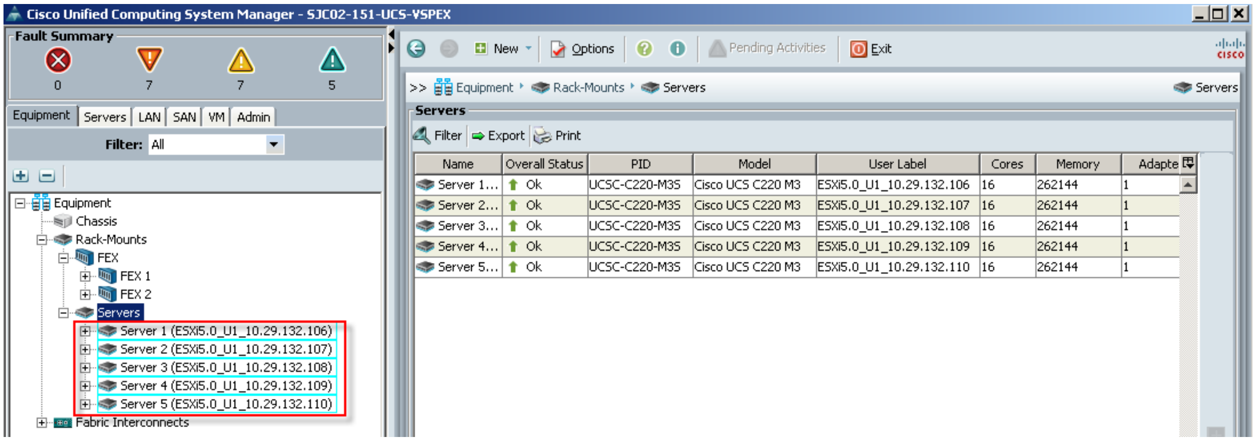
8.4 Select CIMC Factory Default with spacebar, press F10, then F10 again to confirm factory defaults. This step prepares the server for management through the Nexus 2232PP FEX by Cisco UCS Manager on the Fabric Interconnects.

8.5 Connect one port of the VIC1225 from each Cisco UCS C220 M3 server to one Nexus 2232PP Fabric Extender. Connect the second VIC1225 port to the other Nexus 2232PP Fabric Extender. Repeat for all servers.

8.6 Reboot all of the Cisco UCS C220 M3 servers.

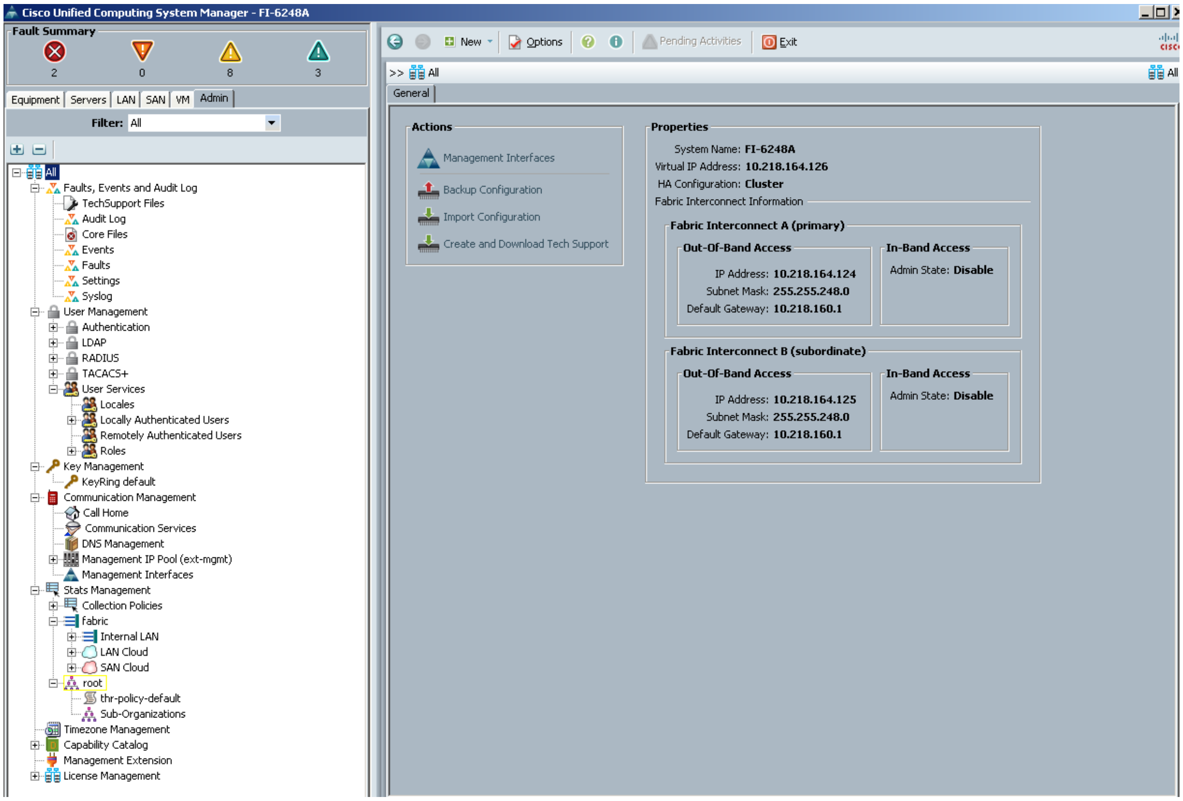
8.7 From the Equipment tab in UCS Manager, navigate to Rack-Mounts, Servers. The five UCS C220 M3 servers should be visible.

If the servers do not appear under the server node, repeat step 6, Acknowledge FEX for each FEX.


Cisco Unified Computing System Manager - SJC02-151-UCS-VSPEX
Fault Summary
0
7
7
5
Equipment
Servers
LAN
SAN
VM
Admin
Filter: All
Equipment
Chassis
Rack-Mounts
FEX
FEX 1
FEX 2
Servers
Server 1 (ESXi5.0_U1_10.29.132.106)
Server 2 (ESXi5.0_U1_10.29.132.107)
Server 3 (ESXi5.0_U1_10.29.132.108)
Server 4 (ESXi5.0_U1_10.29.132.109)
Server 5 (ESXi5.0_U1_10.29.132.110)
Fabric Interconnects
New
Options
Pending Activities
Exit
>> Equipment ▸ Rack-Mounts ▸ Servers
Servers
Servers
Filter
Export
Print

Name	Overall Status	PID	Model	User Label	Cores	Memory	Adapte
Server 1...	Ok	UCSC-C220-M3S	Cisco UCS C220 M3	ESXi5.0_U1_10.29.132.106	16	262144	1
Server 2...	Ok	UCSC-C220-M3S	Cisco UCS C220 M3	ESXi5.0_U1_10.29.132.107	16	262144	1
Server 3...	Ok	UCSC-C220-M3S	Cisco UCS C220 M3	ESXi5.0_U1_10.29.132.108	16	262144	1
Server 4...	Ok	UCSC-C220-M3S	Cisco UCS C220 M3	ESXi5.0_U1_10.29.132.109	16	262144	1
Server 5...	Ok	UCSC-C220-M3S	Cisco UCS C220 M3	ESXi5.0_U1_10.29.132.110	16	262144	1

9 Use the Admin tab in the left pane, to configure logging, users and authentication, key management, communications, statistics, time zone and NTP services, and Licensing. Configuring your Management IP Pool (which provides IP based access to the KVM of each Cisco UCS Blade Server,) Time zone Management (including NTP time source(s)) and uploading your license files are critical steps in the process.



Properties

System Name: **FI-6248A**
Virtual IP Address: **10.218.164.126**
HA Configuration: **Cluster**

Fabric Interconnect Information

Fabric Interconnect A (primary)

Out-Of-Band Access
IP Address: **10.218.164.124**
Subnet Mask: **255.255.248.0**
Default Gateway: **10.218.160.1**

In-Band Access
Admin State: **Disable**

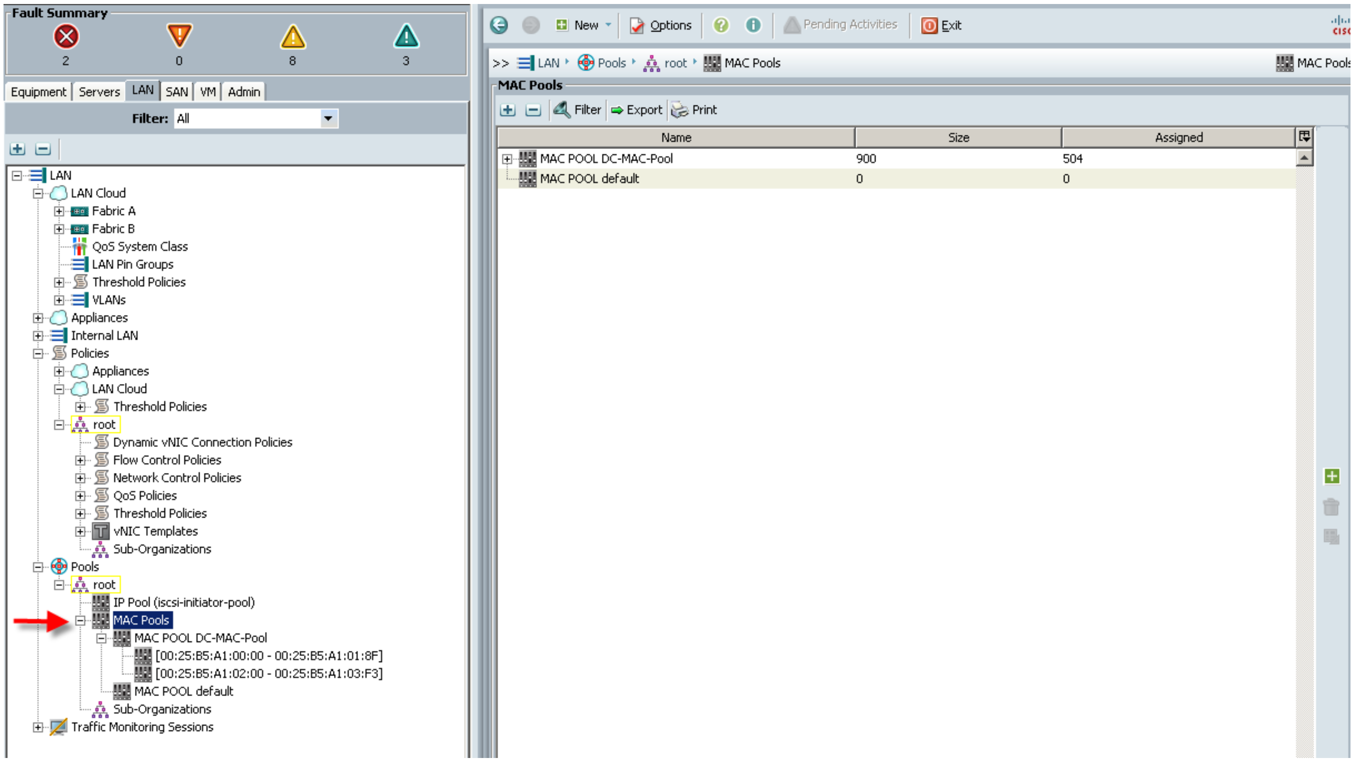
Fabric Interconnect B (subordinate)

Out-Of-Band Access
IP Address: **10.218.164.125**
Subnet Mask: **255.255.248.0**
Default Gateway: **10.218.160.1**

In-Band Access
Admin State: **Disable**

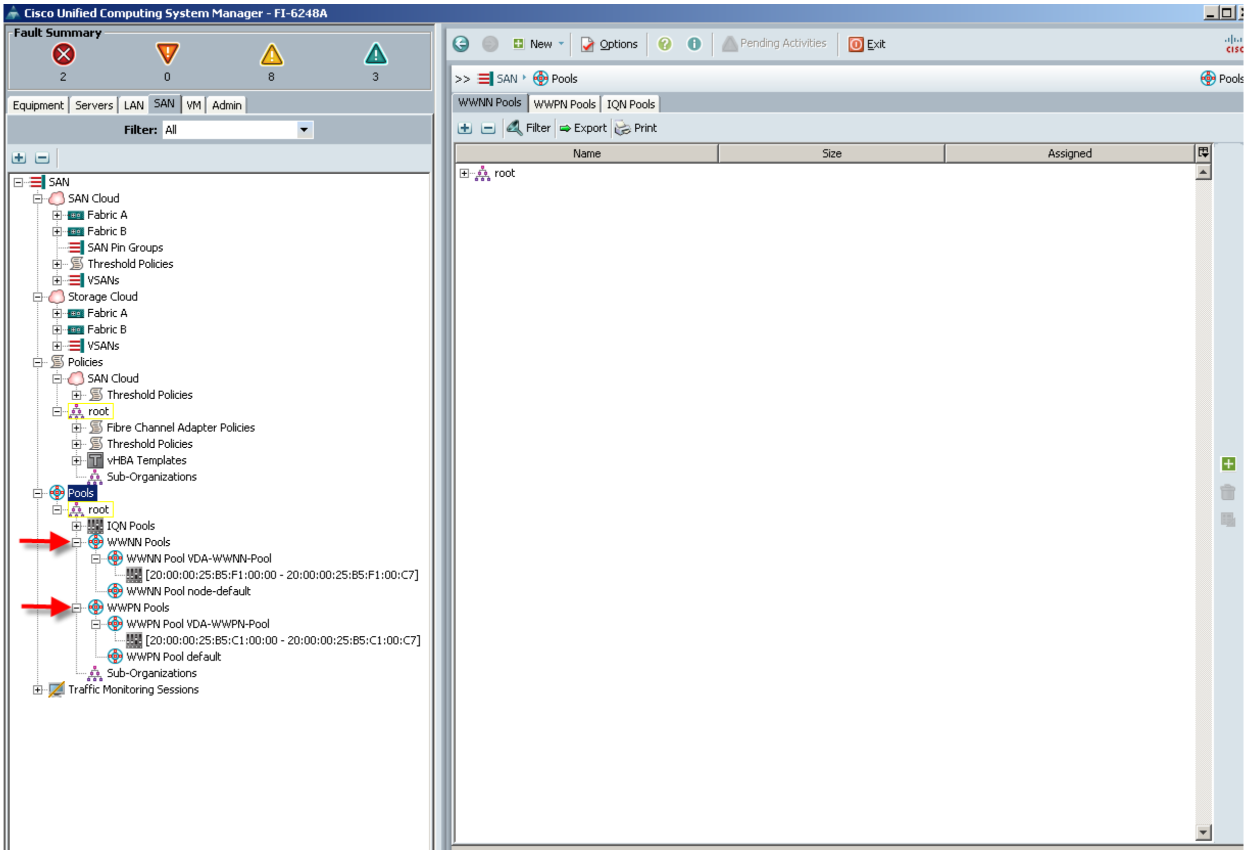
10 Create all the pools: MAC pool, WWPN pool, WWNN pool, UUID pool, Server pool.

11 From the LAN tab in the navigator, under the Pools node, we created a MAC address pool of sufficient size for the environment. In this project, we created a single pool with two address ranges for expandability.

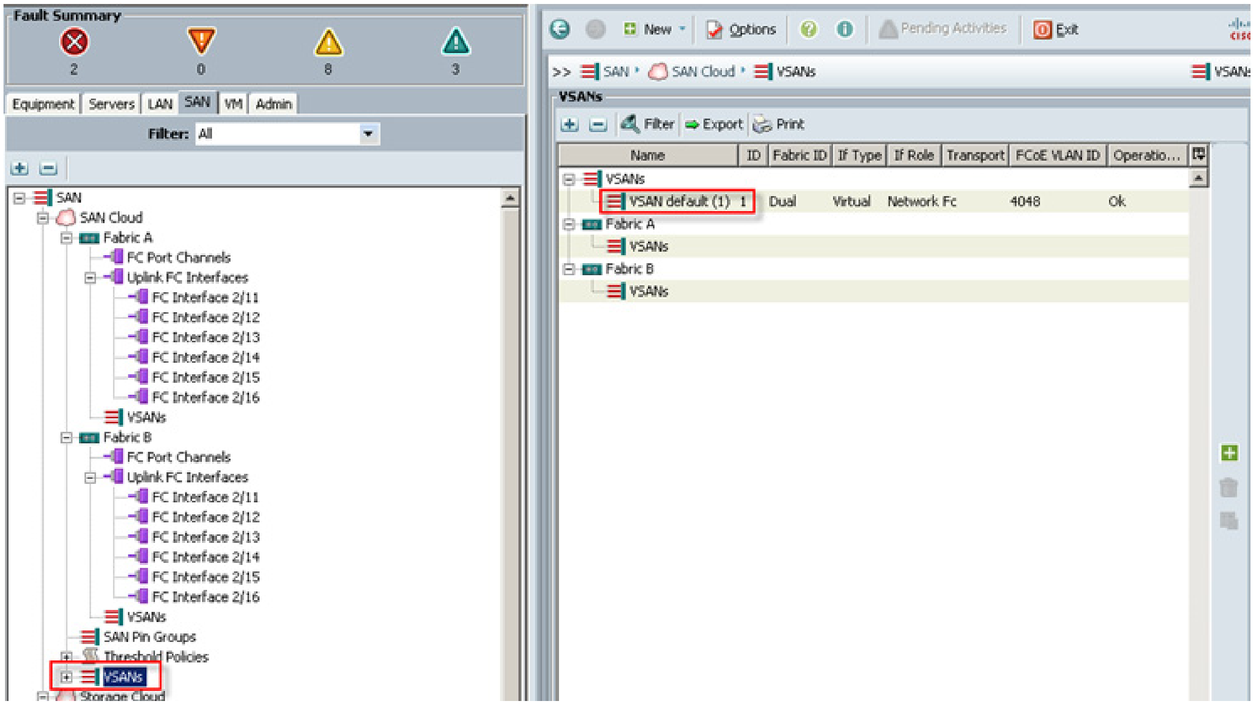


Name	Size	Assigned
MAC POOL DC-MAC-Pool	900	504
MAC POOL default	0	0

12 For Fiber Channel connectivity, WWNN and WWPN pools must be created from the SAN tab in the navigator pane, in the Pools node:

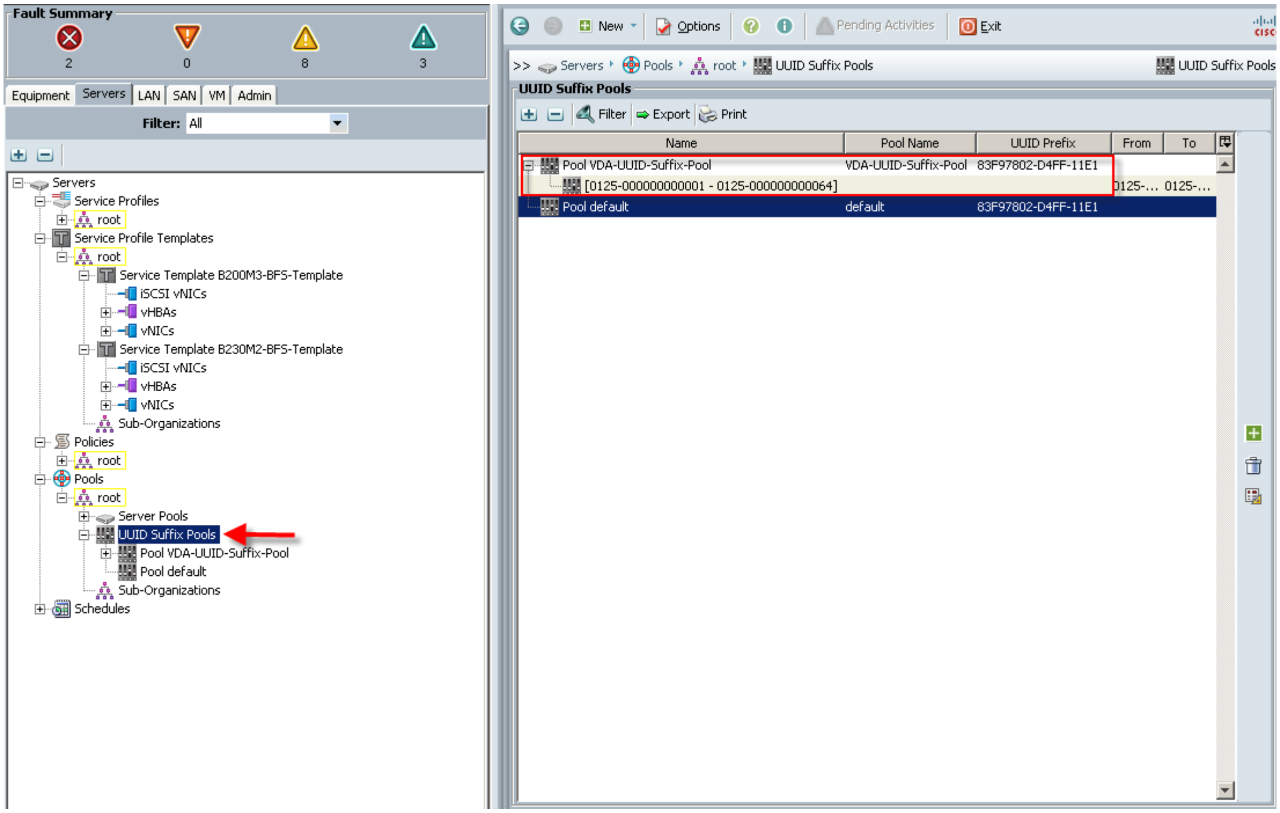


13 For this project, we used a single VSAN, the default VSAN with ID 1:



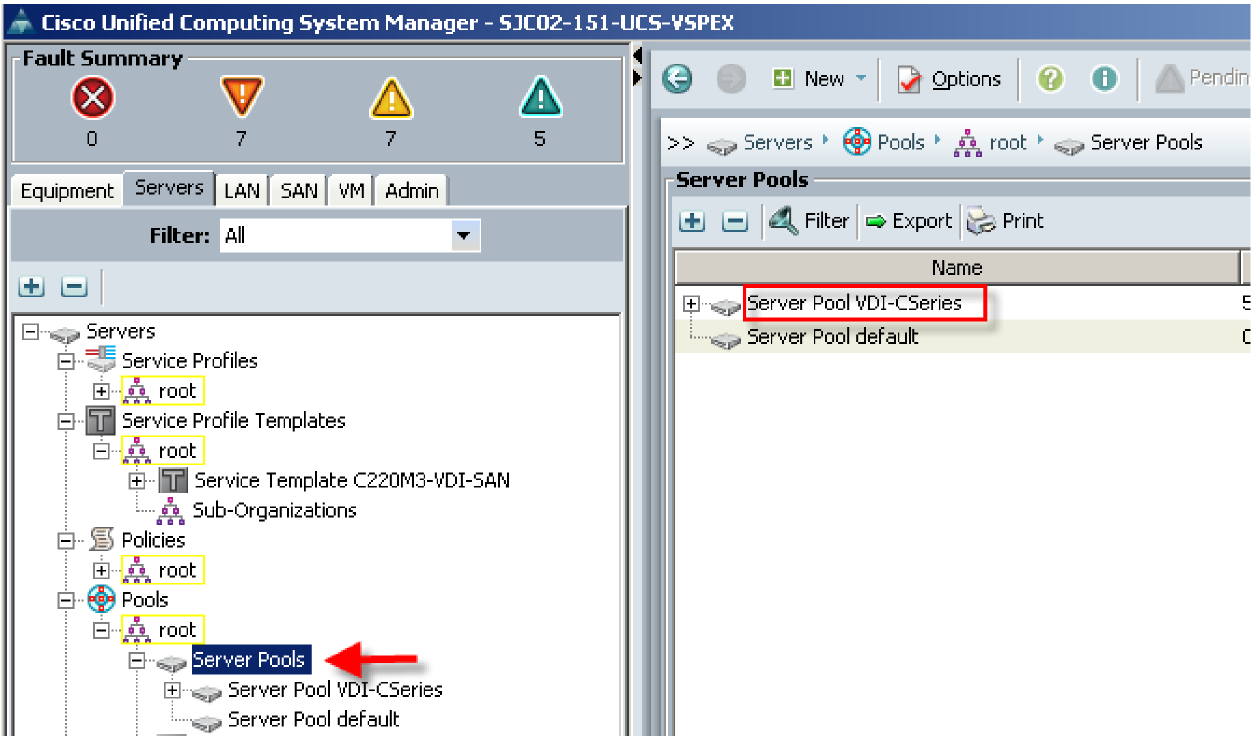
Name	ID	Fabric ID	If Type	If Role	Transport	FCoE VLAN ID	Operatio...
VSANs							
VSAN default (1)	1	Dual	Virtual	Network	Fc	4048	Ok
Fabric A							
VSANs							
Fabric B							
VSANs							

14 The next pool we created is the Server UUID pool. On the Servers tab in the Navigator page under the Pools node we created a single UUID Pool for the test environment. Each UCS Blade Server requires a unique UUID to be assigned by its Service profile.

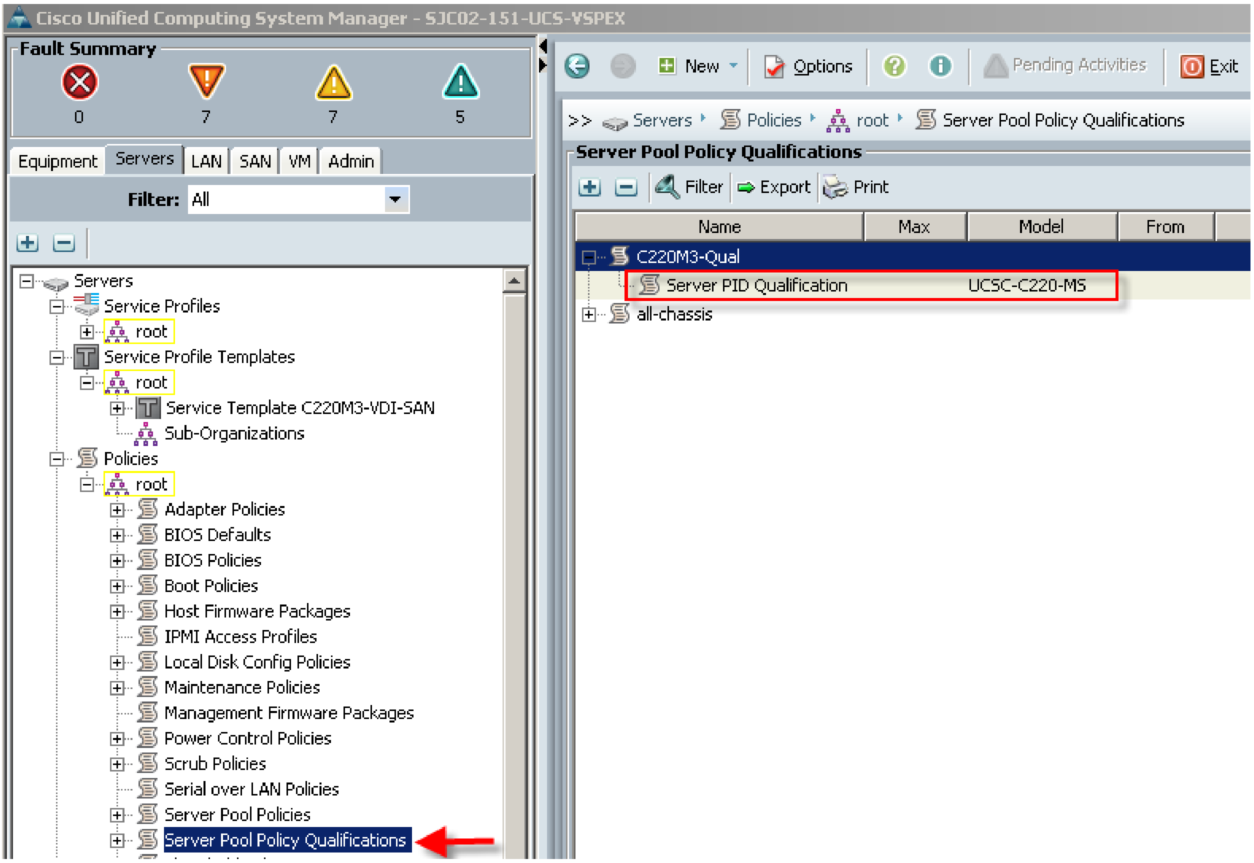


Name	Pool Name	UUID Prefix	From	To
Pool VDA-UUID-Suffix-Pool	VDA-UUID-Suffix-Pool	83F97802-D4FF-11E1		
[0125-000000000001 - 0125-000000000064]			0125-...	0125-...
Pool default	default	83F97802-D4FF-11E1		

15 We created one Server Pool for use in our Service Profile Templates as selection criteria for automated profile association. The Server Pool were created on the Servers tab in the navigation page under the Pools node. Only the pool name was created, no servers were added:



16 We created one Server Pool Policy Qualification to identify the UCS C220 M3 rack-mount server model for placement into the correct Server pool using the Service Profile Template. In this case we used the C220 M3 Product ID (PID) to select the servers. (This would be helpful if the deployment grew and different UCS C-Series Rack-Mount models were incorporated later.)



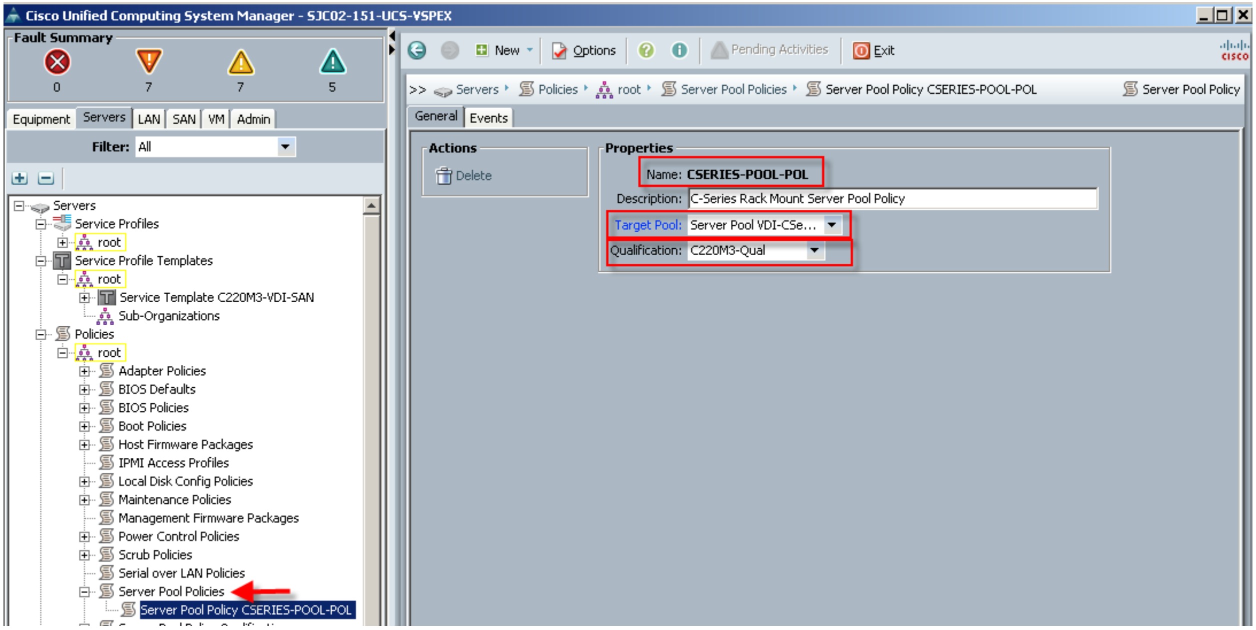
Cisco Unified Computing System Manager - SJC02-151-UCS-VSPEX

>> Servers ▸ Policies ▸ root ▸ Server Pool Policy Qualifications

Server Pool Policy Qualifications

Name	Max	Model	From
C220M3-Qual			
Server PID Qualification		UCSC-C220-M3	
all-chassis			

17 The next step in automating the server selection process is to create corresponding Server Pool Policy for each UCS C-Series server model, utilizing the Server Pool and Server Pool Policy Qualification created earlier.



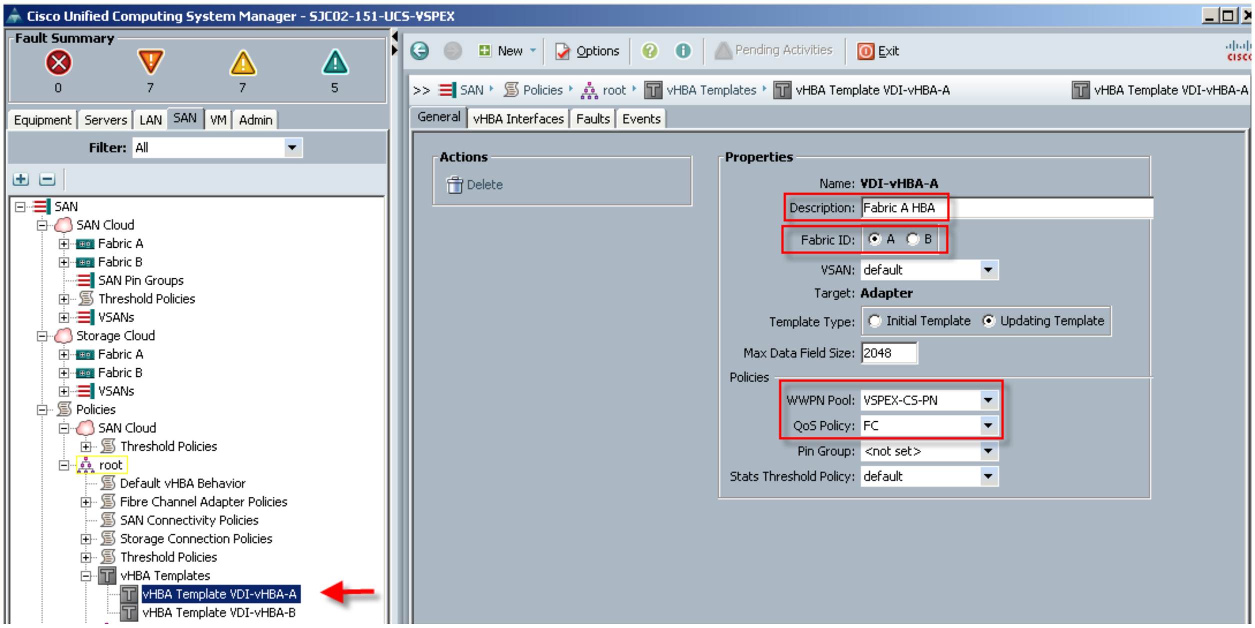
Name: **CSERIES-POOL-POL**

Description: C-Series Rack Mount Server Pool Policy

Target Pool: Server Pool VDI-CSe...

Qualification: C220M3-Qual

18 Virtual Host Bus Adapter updating templates were created for FC SAN connectivity from the SAN tab under the Polices node, utilizing the WWPN pool created earlier and the default FC QoS policy, one template for each fabric:



Name: **VDI-vHBA-A**

Description: Fabric A HBA

Fabric ID: ● A ○ B

VSAN: default

Target: **Adapter**

Template Type: ○ Initial Template ● Updating Template

Max Data Field Size: 2048

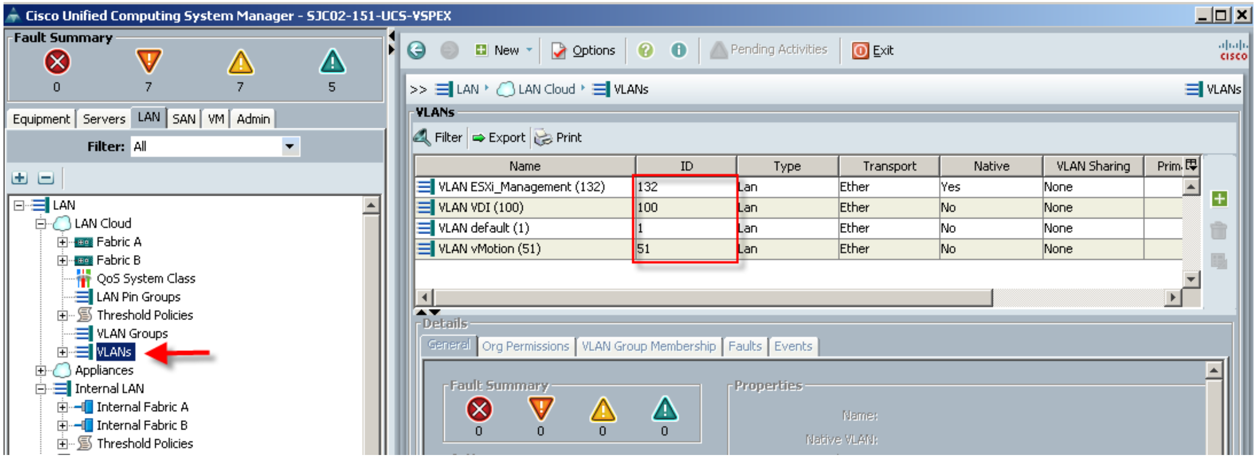
WWPN Pool: VSPEX-CS-PN

QoS Policy: FC

Pin Group: <not set>

Stats Threshold Policy: default

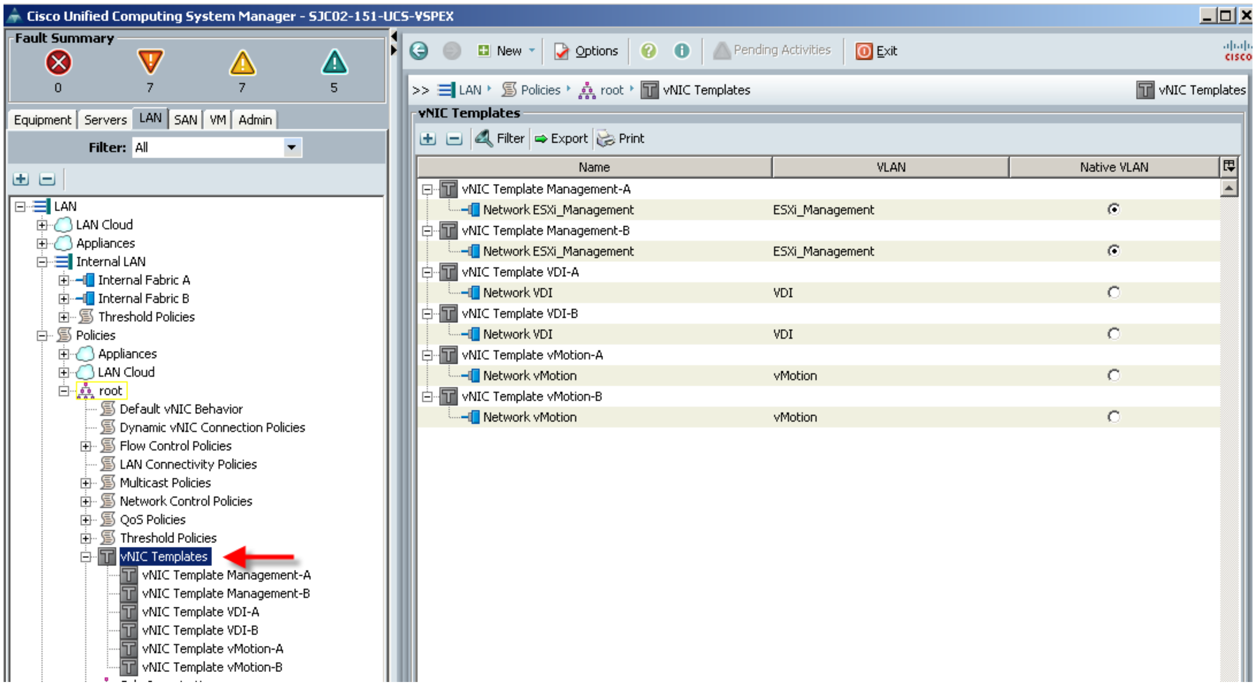
10 On the LAN tab in the navigator pane, configure the VLANs for the environment:



Name	ID	Type	Transport	Native	VLAN Sharing	Prim
VLAN ESXi_Management (132)	132	Lan	Ether	Yes	None	
VLAN VDI (100)	100	Lan	Ether	No	None	
VLAN default (1)	1	Lan	Ether	No	None	
VLAN vMotion (51)	51	Lan	Ether	No	None	

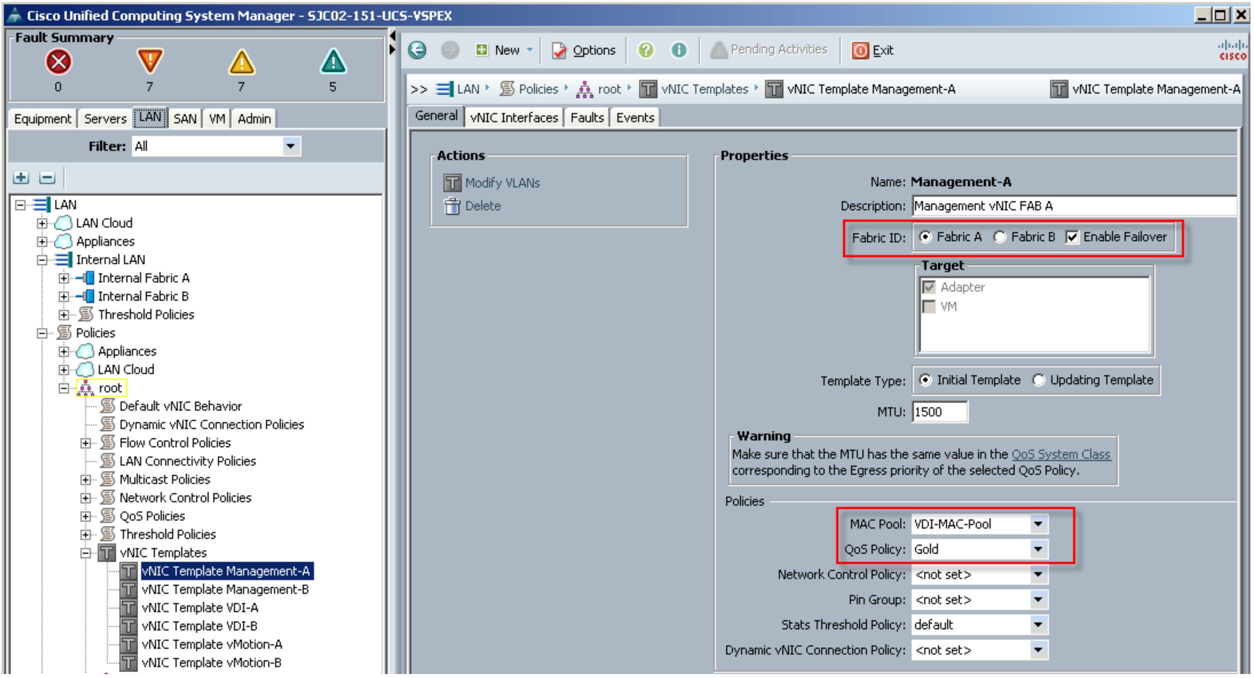
In this project we utilized three VLANs for the Managed FC variant to accommodate our three ethernet system classes. Infrastructure services shared VLAN 132.

11 On the LAN tab in the navigator pane, under the policies node configure the vNIC templates that will be used in the Service Profiles. In this project, we utilize six virtual NICs per host, three pairs, with one member of each pair connected to one of the two Fabric Interconnects for resiliency.



Name	VLAN	Native VLAN
vNIC Template Management-A		
Network ESXi_Management	ESXi_Management	●
vNIC Template Management-B		
Network ESXi_Management	ESXi_Management	●
vNIC Template VDI-A		
Network VDI	VDI	○
vNIC Template VDI-B		
Network VDI	VDI	○
vNIC Template vMotion-A		
Network vMotion	vMotion	○
vNIC Template vMotion-B		
Network vMotion	vMotion	○

11a Create vNIC templates for both fabrics, check Enable Failover, select VLANs supported on adapter (optional,) set the MTU size if necessary, select the MAC Pool and QoS Policy, then click OK



Properties

Name: **Management-A**

Description: Management vNIC FAB A

Fabric ID: ● Fabric A ○ Fabric B ☑ Enable Failover

Target

☑ Adapter

□ VM

Template Type: ● Initial Template ○ Updating Template

MTU: 1500

Warning

Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.

Policies

MAC Pool: VDI-MAC-Pool

QoS Policy: Gold

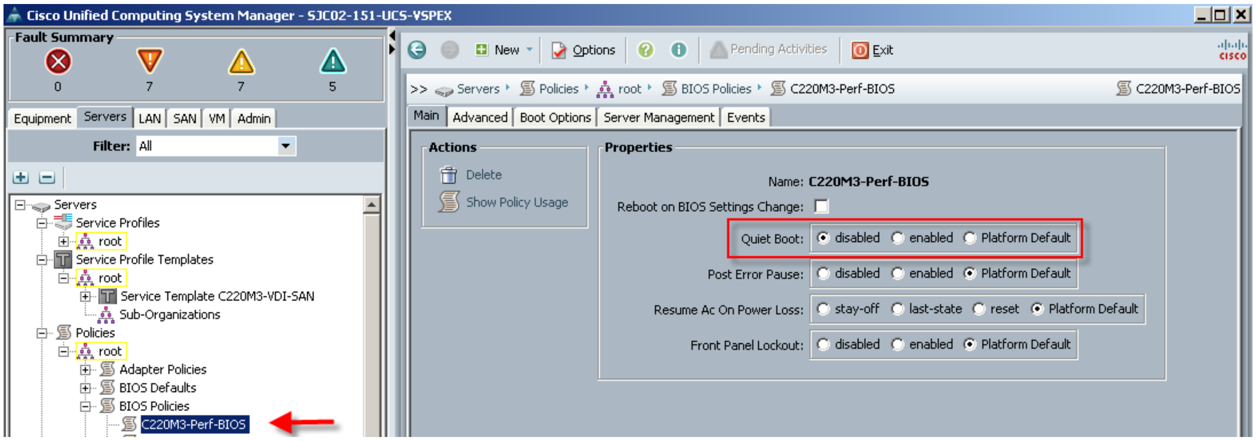
Network Control Policy: <not set>

Pin Group: <not set>

Stats Threshold Policy: default

Dynamic vNIC Connection Policy: <not set>

12 Create a performance BIOS Policy for the C220 M3 server to insure optimal performance. The following screen captures show the settings for the UCS C220 M3 servers used in this study:



Name: **C220M3-Perf-BIOS**

Reboot on BIOS Settings Change: □

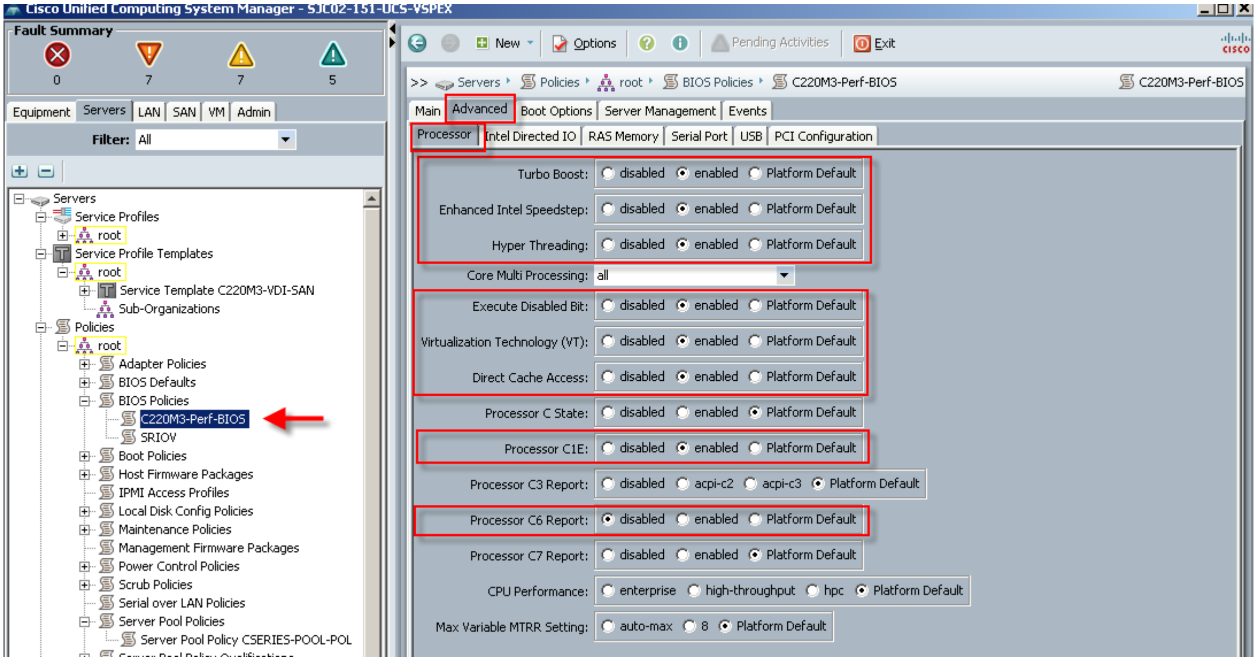
Quiet Boot: ● disabled ○ enabled ○ Platform Default

Post Error Pause: ○ disabled ○ enabled ● Platform Default

Resume Ac On Power Loss: ○ stay-off ○ last-state ○ reset ● Platform Default

Front Panel Lockout: ○ disabled ○ enabled ● Platform Default

Advanced tab, Processor settings



Turbo Boost: ○ disabled ● enabled ○ Platform Default

Enhanced Intel Speedstep: ○ disabled ● enabled ○ Platform Default

Hyper Threading: ○ disabled ● enabled ○ Platform Default

Core Multi Processing: all

Execute Disabled Bit: ○ disabled ● enabled ○ Platform Default

Virtualization Technology (VT): ○ disabled ● enabled ○ Platform Default

Direct Cache Access: ○ disabled ● enabled ○ Platform Default

Processor C State: ○ disabled ○ enabled ● Platform Default

Processor C1E: ○ disabled ● enabled ○ Platform Default

Processor C3 Report: ○ disabled ○ acpi-c2 ○ acpi-c3 ● Platform Default

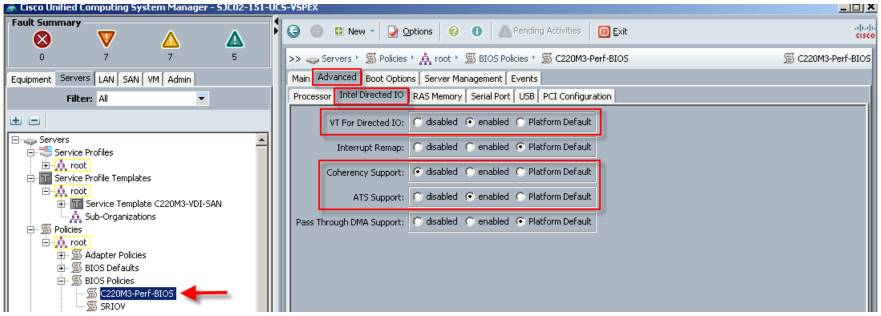
Processor C6 Report: ● disabled ○ enabled ○ Platform Default

Processor C7 Report: ○ disabled ○ enabled ● Platform Default

CPU Performance: ○ enterprise ○ high-throughput ○ hpc ● Platform Default

Max Variable MTRR Setting: ○ auto-max ○ 8 ● Platform Default

Advanced Tab, Intel Directed IO settings



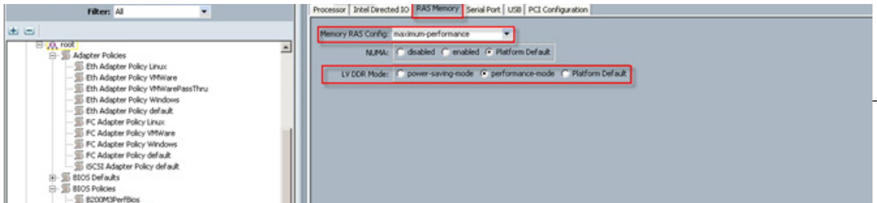
VT For Directed IO: ○ disabled ● enabled ○ Platform Default

Interrupt Remap: ○ disabled ○ enabled ● Platform Default

Coherency Support: ● disabled ○ enabled ○ Platform Default

ATS Support: ○ disabled ● enabled ○ Platform Default

Pass Through DMA Support: ○ disabled ○ enabled ● Platform Default



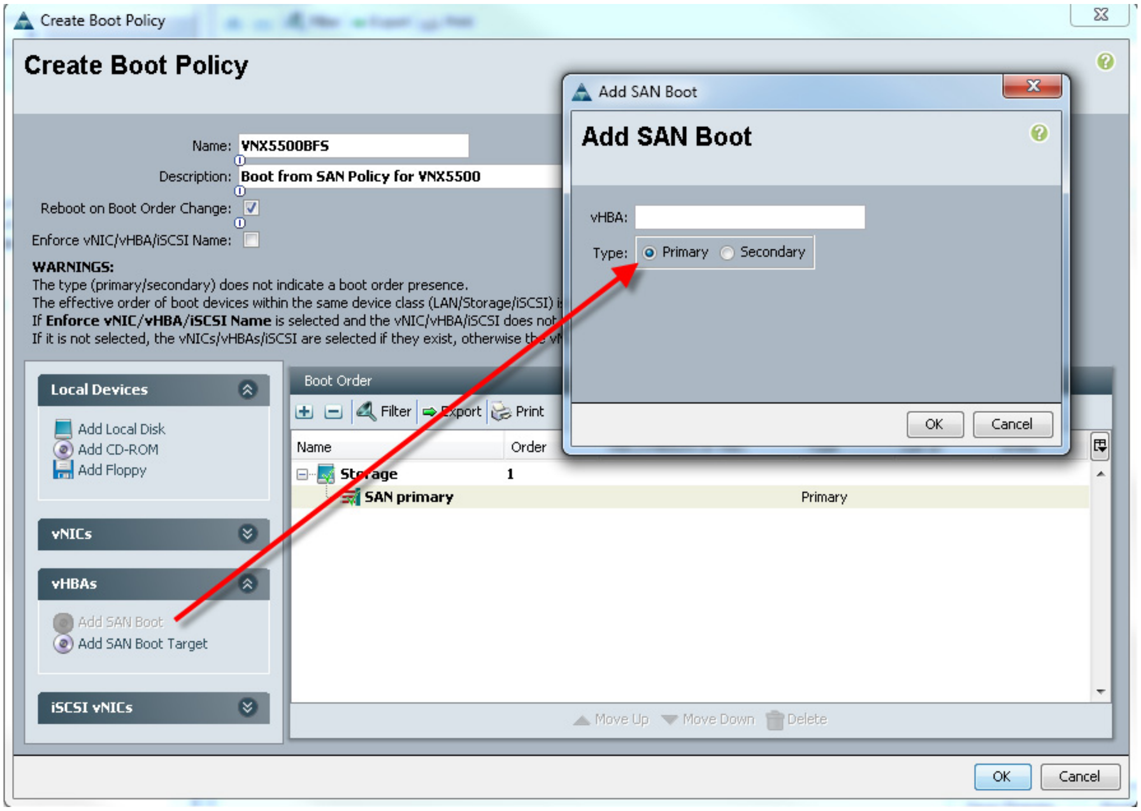
Memory RAS Config: maximum-performance

NUMA: ○ disabled ○ enabled ● Platform Default

LV DDR Mode: ○ power-saving-mode ● performance-mode ○ Platform Default

13 To enable Boot from SAN on the UCS Manager 2.0 (UCS-M) series, create a Boot from SAN policy:

1. Add SAN Boot for primary to the new policy. The vHBA name is optional, it could be left blank and we don’t have to enforce the vHBA name. Click OK.



Create Boot Policy

Name: VNX5500BFS

Description: Boot from SAN Policy for VNX5500

Reboot on Boot Order Change: ☑

Enforce vNIC/vHBA/iSCSI Name: □

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) i
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not
If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the v

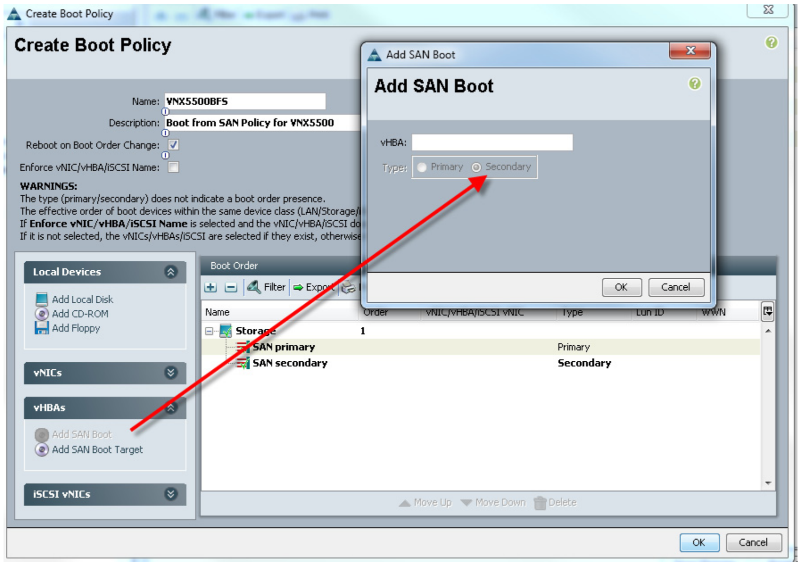
Add SAN Boot

vHBA:

Type: ● Primary ○ Secondary

Name	Order		
Storage	1		
SAN primary			Primary

2. Add SAN boot for SAN Secondary, Click OK. Again, we left the optional vHBA name blank



Create Boot Policy

Name: VNX5500BFS

Description: Boot from SAN Policy for VNX5500

Reboot on Boot Order Change: ☑

Enforce vNIC/vHBA/iSCSI Name: □

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/i
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI do
If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise

Add SAN Boot

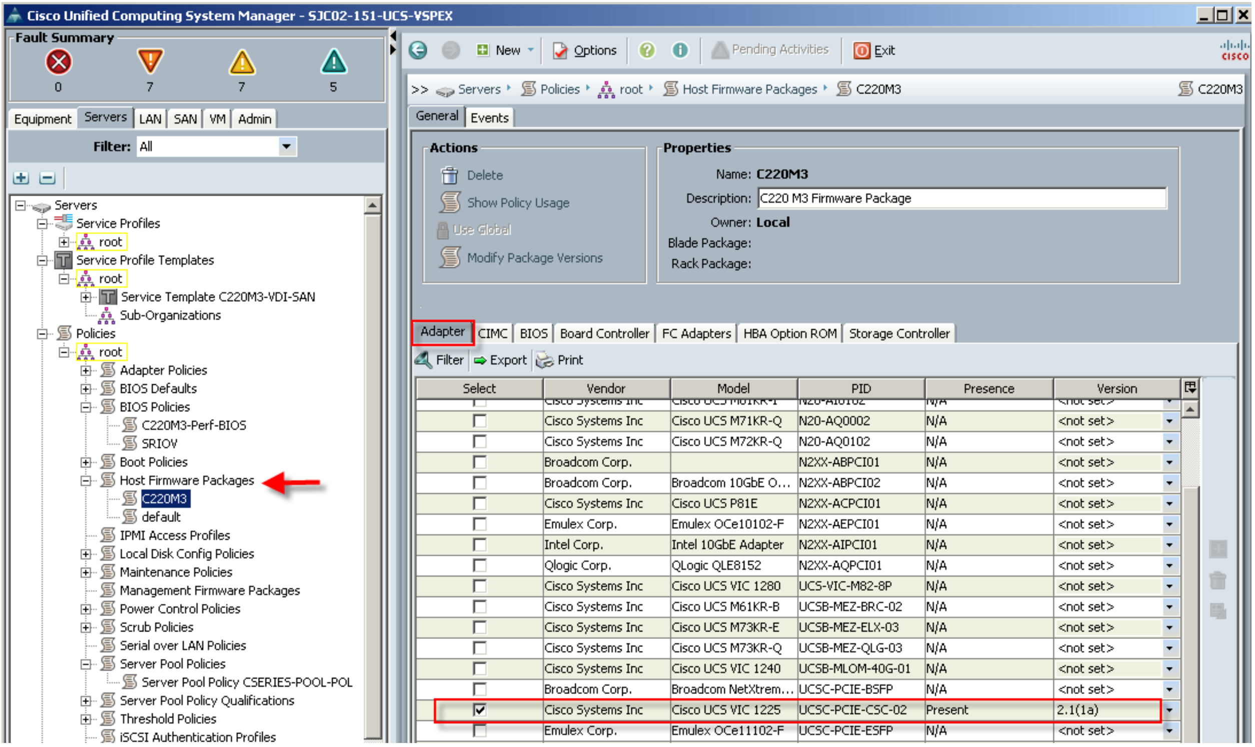
vHBA:

Type: ○ Primary ● Secondary

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN
Storage	1				
SAN primary			Primary		
SAN secondary			Secondary		

3. Now add Boot target WWPN to the SAN Primary, make sure this is exactly matches the EMC VNX pwwn. To avoid any typos, copy and paste from UCS 6248UP command as follows from each

14 The UCS C220 M3 Host Firmware Package polices were set for Adapter, CIMC and BIOS:



Properties

Name: **C220M3**

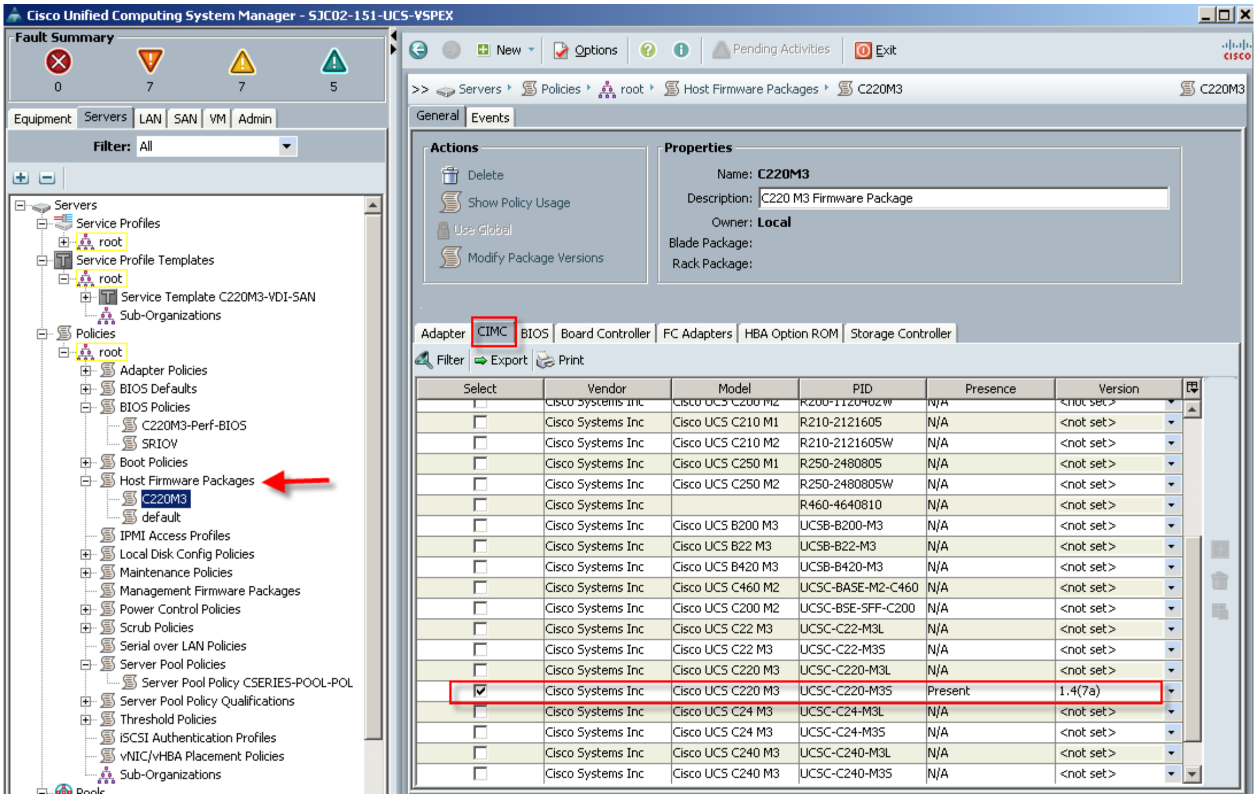
Description: C220 M3 Firmware Package

Owner: **Local**

Blade Package:

Rack Package:

Select	Vendor	Model	PID	Presence	Version
□	Cisco Systems Inc	Cisco UCS M81KR-I	N20-AI0102	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS M71KR-Q	N20-AQ0002	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS M72KR-Q	N20-AQ0102	N/A	<not set>
□	Broadcom Corp.		N2XX-ABPCI01	N/A	<not set>
□	Broadcom Corp.	Broadcom 10GbE O...	N2XX-ABPCI02	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS P81E	N2XX-ACPCI01	N/A	<not set>
□	Emulex Corp.	Emulex OCe10102-F	N2XX-AEPCI01	N/A	<not set>
□	Intel Corp.	Intel 10GbE Adapter	N2XX-AIPCI01	N/A	<not set>
□	Qlogic Corp.	QLogic QLE8152	N2XX-AQPCI01	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS VIC 1280	UCS-VIC-M82-8P	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS M61KR-B	UCSB-MEZ-BRC-02	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS M73KR-E	UCSB-MEZ-ELX-03	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS M73KR-Q	UCSB-MEZ-QLG-03	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS VIC 1240	UCSB-MLOM-40G-01	N/A	<not set>
□	Broadcom Corp.	Broadcom NetXtrem...	UCSC-PCIE-BSFP	N/A	<not set>
☑	Cisco Systems Inc	Cisco UCS VIC 1225	UCSC-PCIE-CSC-02	Present	2.1(1a)
□	Emulex Corp.	Emulex OCe11102-F	UCSC-PCIE-ESFP	N/A	<not set>



Properties

Name: **C220M3**

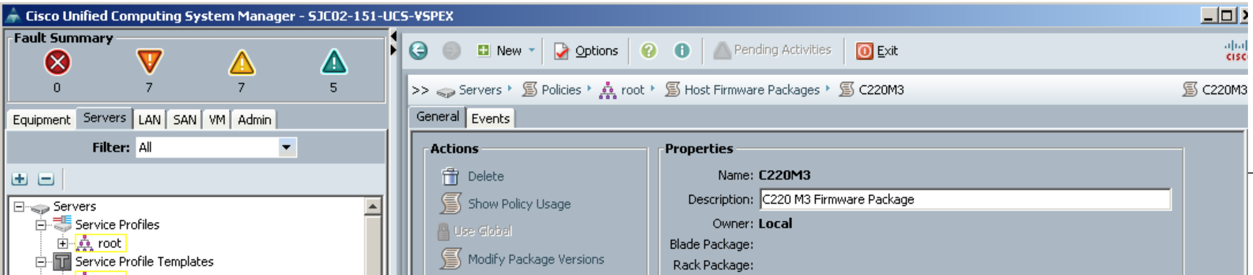
Description: C220 M3 Firmware Package

Owner: **Local**

Blade Package:

Rack Package:

Select	Vendor	Model	PID	Presence	Version
□	Cisco Systems Inc	Cisco UCS C200 M2	R200-1120402W	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C210 M1	R210-2121605	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C210 M2	R210-2121605W	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C250 M1	R250-2480805	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C250 M2	R250-2480805W	N/A	<not set>
□	Cisco Systems Inc		R460-4640810	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS B200 M3	UCSB-B200-M3	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS B22 M3	UCSB-B22-M3	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS B420 M3	UCSB-B420-M3	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C460 M2	UCSC-BASE-M2-C460	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C200 M2	UCSC-BSE-SFF-C200	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C22 M3	UCSC-C22-M3L	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C22 M3	UCSC-C22-M3S	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C220 M3	UCSC-C220-M3L	N/A	<not set>
☑	Cisco Systems Inc	Cisco UCS C220 M3	UCSC-C220-M3S	Present	1.4(7a)
□	Cisco Systems Inc	Cisco UCS C24 M3	UCSC-C24-M3L	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C24 M3	UCSC-C24-M3S	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C240 M3	UCSC-C240-M3L	N/A	<not set>
□	Cisco Systems Inc	Cisco UCS C240 M3	UCSC-C240-M3S	N/A	<not set>



Properties

Name: **C220M3**

Description: C220 M3 Firmware Package

Owner: **Local**

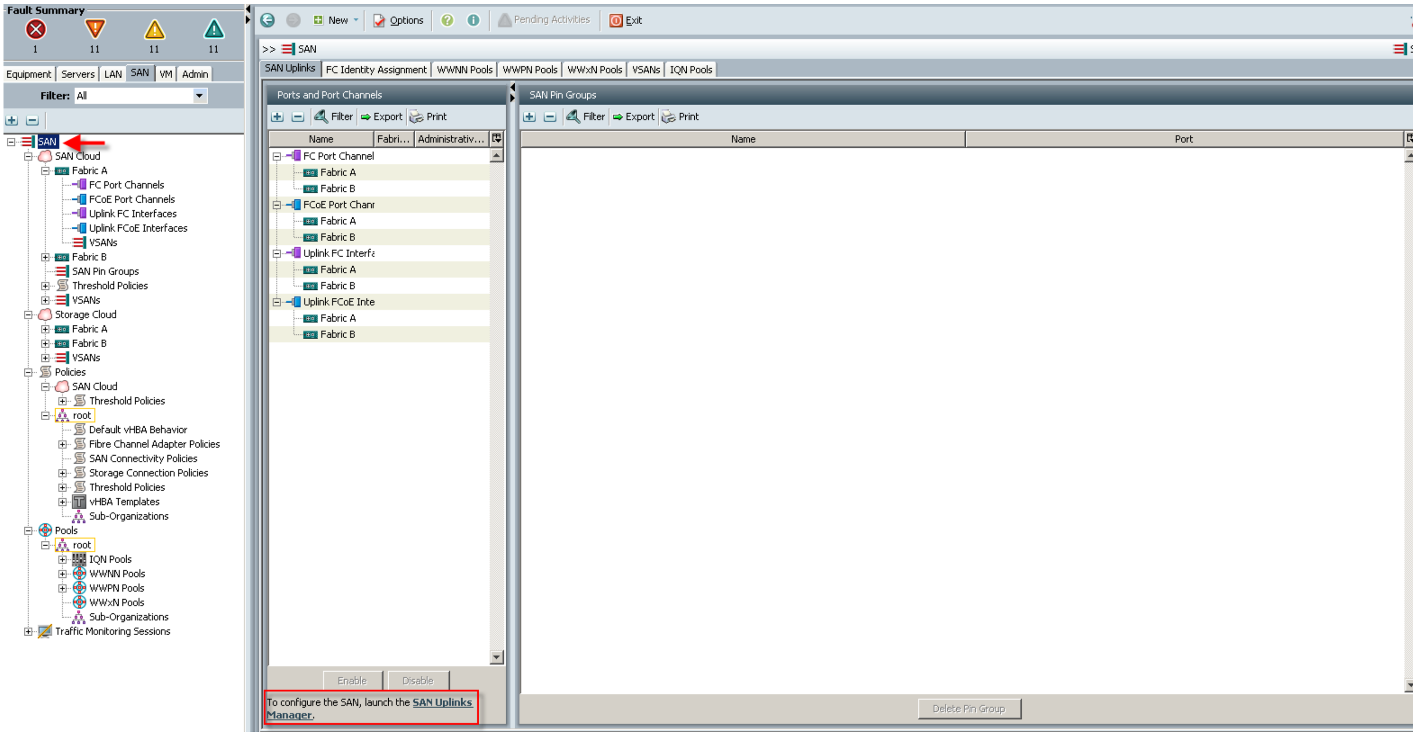
Blade Package:

Rack Package:

15 Set FC Switching Mode on the Fabric Interconnects to enable UCS Local Zoning feature.

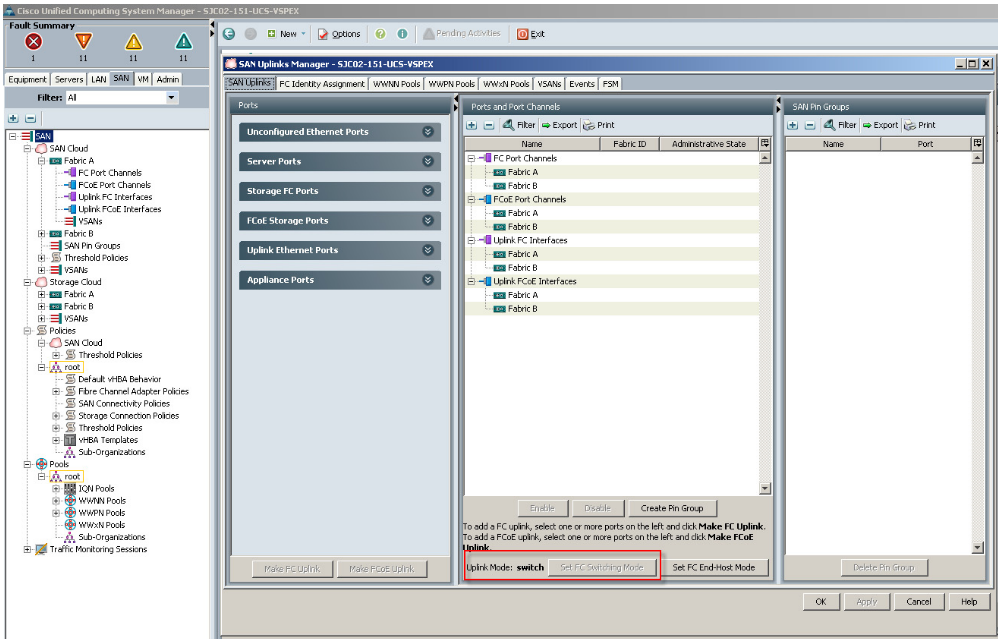
15a In UCSM, navigate to the “SAN Tab” in the navigation pane, Select top level “SAN” tab in the navigation tree. In the Main window, select the “SAN Uplinks Tab” which will display the “Port and Port Channels” and “SAN Pin Groups” windows.

Click the “SAN Uplinks Manager” in the Main window.



To configure the SAN, launch the SAN Uplinks Manager.

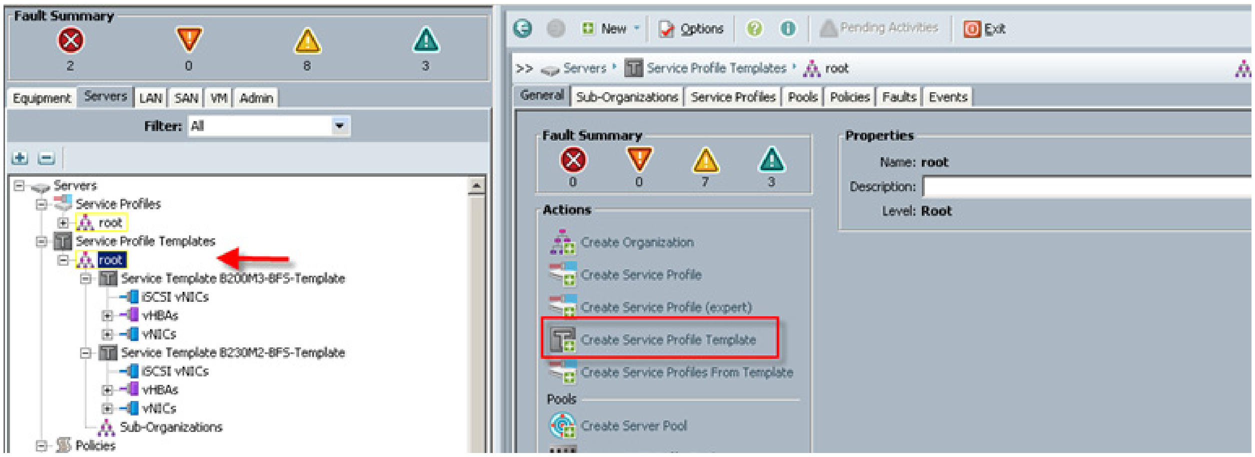
The SAN Uplinks Manager windows will appear:



To add a FC uplink, select one or more ports on the left and click **Make FC Uplink**.
To add a FCoE uplink, select one or more ports on the left and click **Make FCoE Uplink**.

Uplink Mode: **switch**

16 Create a service profile template using the pools, templates, and policies configured above.



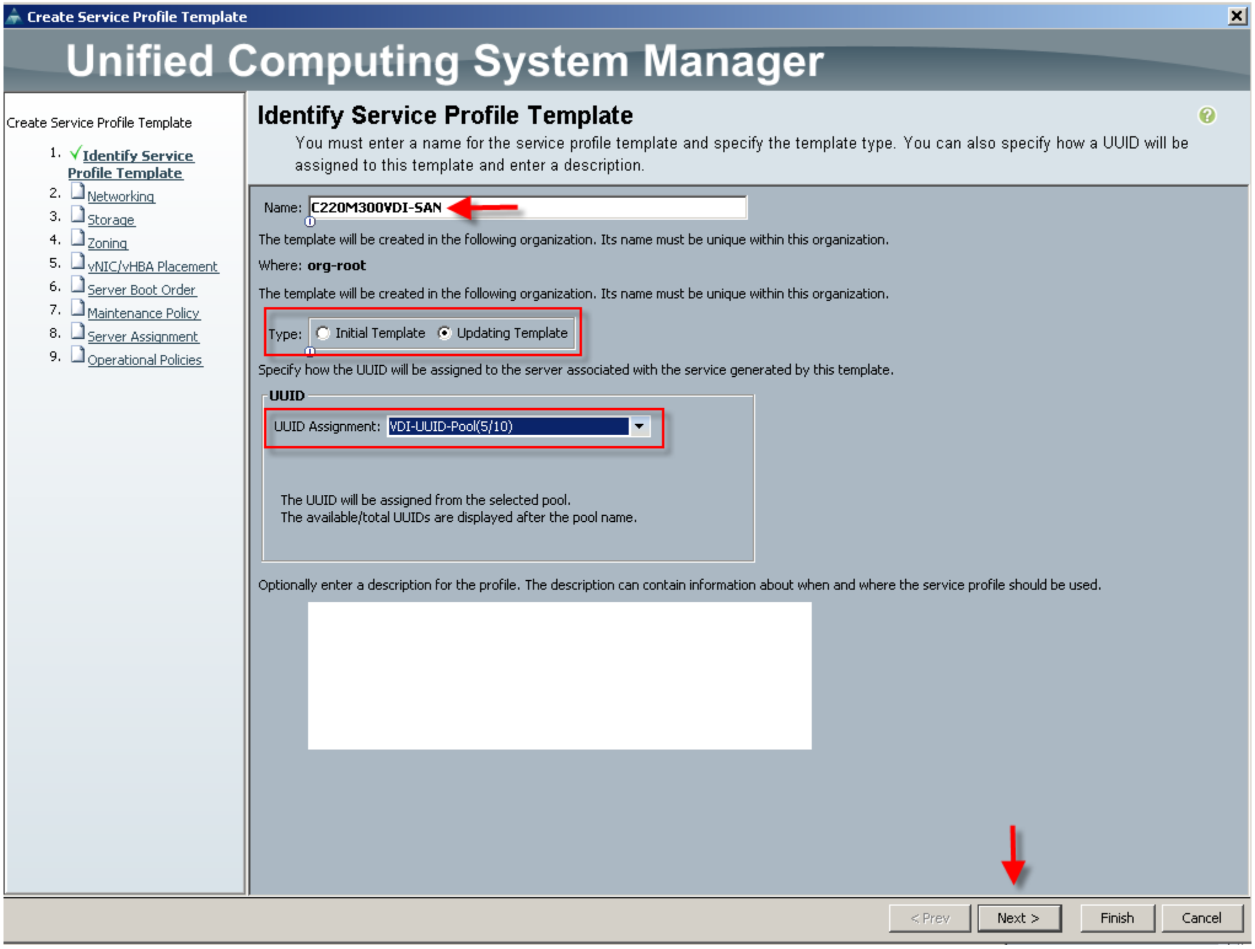
In this project, we created one template for the UCS C220 M3 Rack-Mount server model used.

Follow through each section, utilizing the policies and objects you created earlier, then click Finish.

Note: On the Operational Policies screen, select the appropriate performance BIOS policy you created earlier to insure maximum LV DIMM performance.

Note: For automatic deployment of service profiles from your template(s), you must associate a server pool that contains servers with the template.

16a On the Create Service Profile Template wizard, we entered a unique name, selected the type as updating, and selected the VDI-UUID-Pool created earlier, then clicked Next.



Identify Service Profile Template

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

Name: C220M300VDI-SAN

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

Where: **org-root**

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

Type: ○ Initial Template ● Updating Template

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

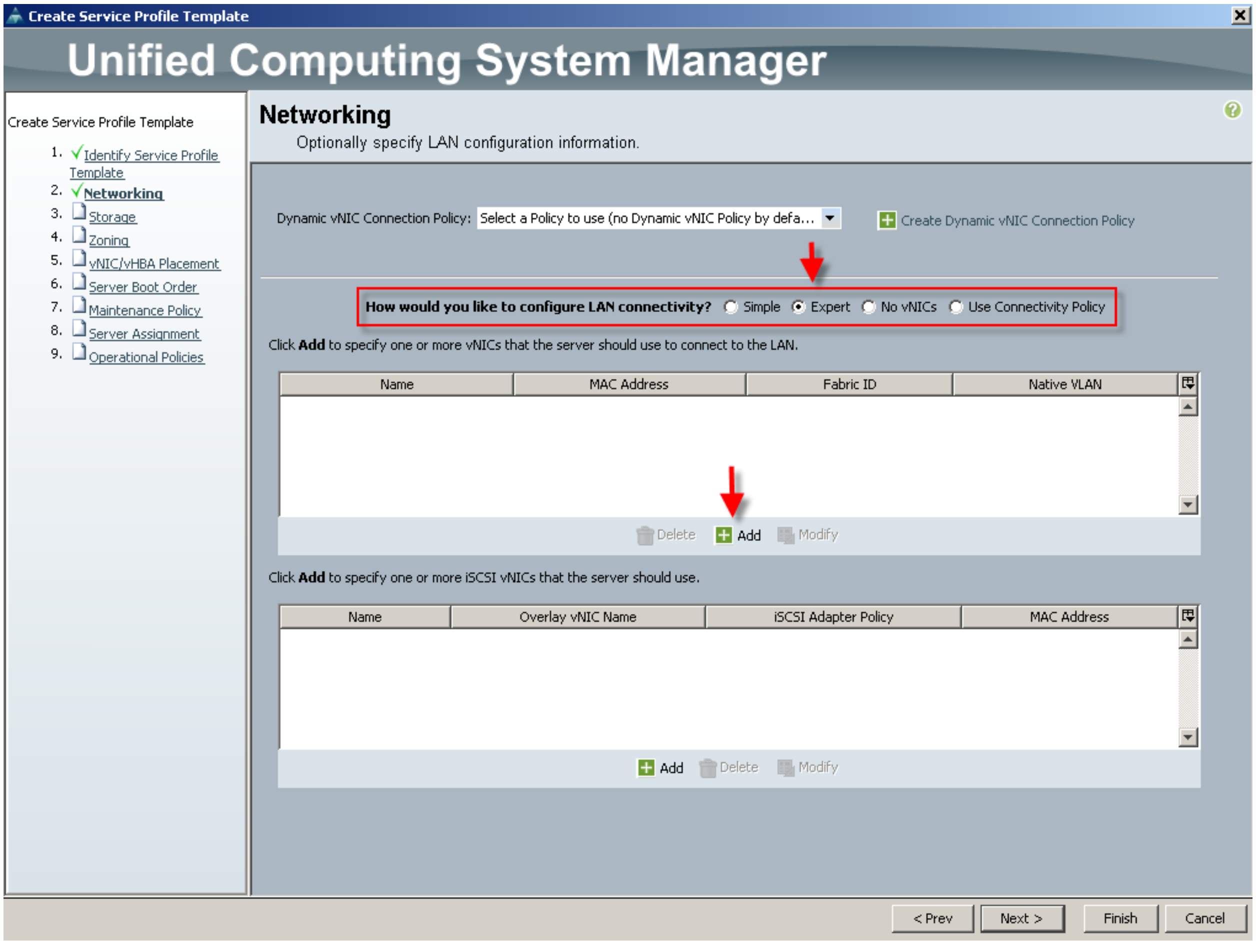
UUID

UUID Assignment: VDI-UUID-Pool(5/10)

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

16b On the Network page, we select Expert mode, we click Add to create virtual NICs.



Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

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

Networking

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by defa... ▾

How would you like to configure LAN connectivity? ○ Simple ● Expert ○ No vNICs ○ Use Connectivity Policy

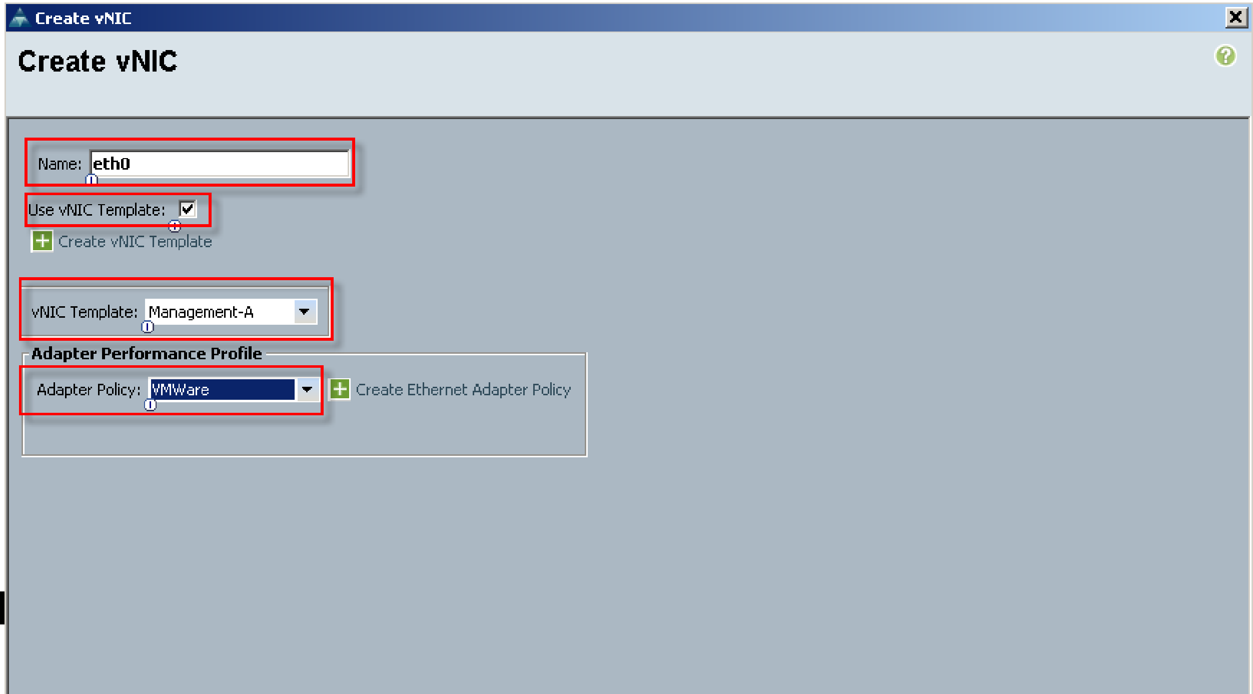
Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Fabric ID	Native VLAN

Click **Add** to specify one or more iSCSI vNICs that the server should use.

Name	Overlay vNIC Name	iSCSI Adapter Policy	MAC Address

On the Create vNIC page, provide a name, typically eth0, eth1, eth2, etc. Check the Use vNIC Template checkbox. Use the drop-down to select one of the vNIC templates created earlier. Use the drop-down list to choose the VMware Adapter Policy



Create vNIC

Create vNIC

Name: eth0

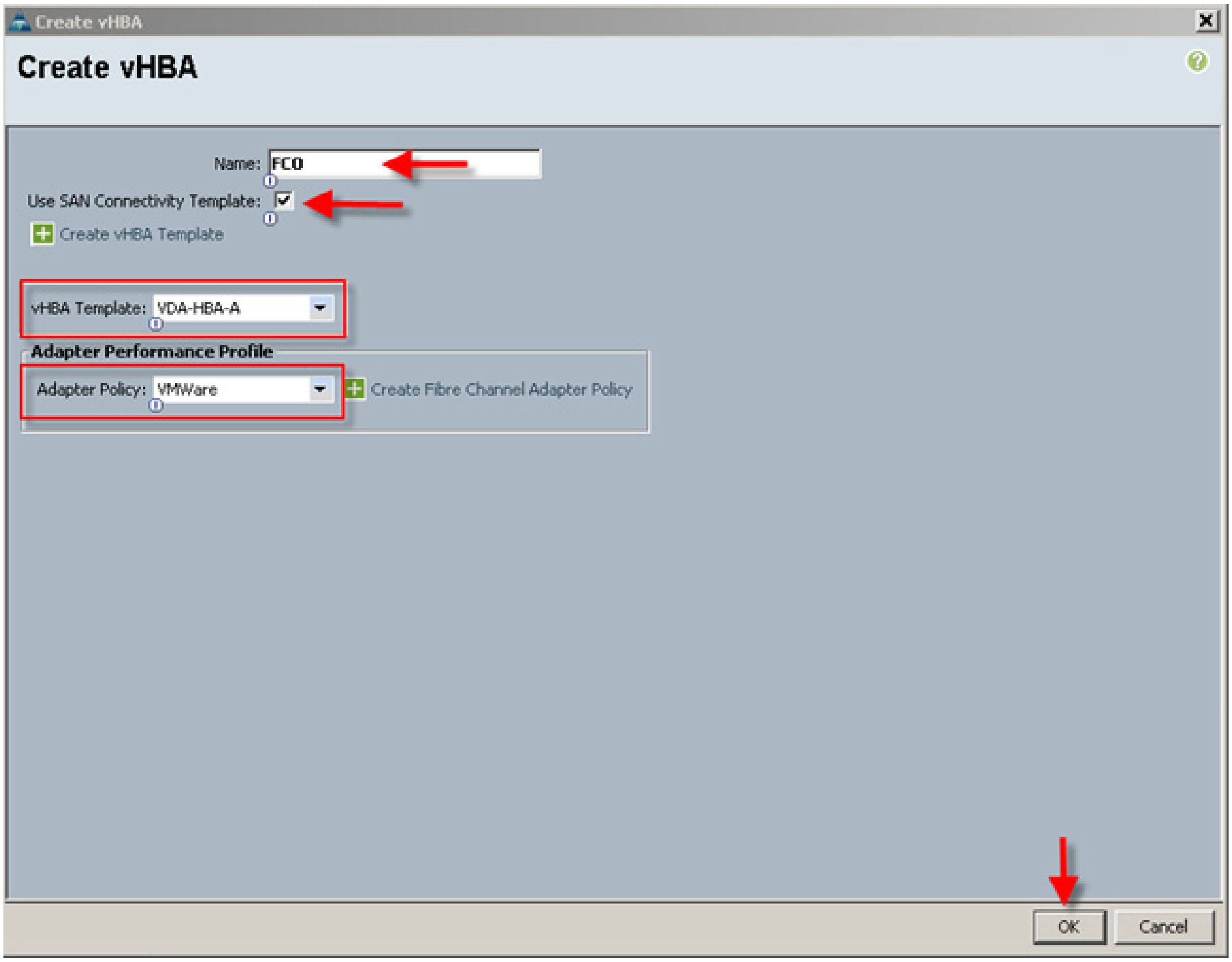
Use vNIC Template: ☑

vNIC Template: Management-A ▾

Adapter Performance Profile

Adapter Policy: VMWare ▾

16f On the Create HBA page, we entered a name (FC0) and checked Use SAN Connectivity Template, which changed the display to the following:



Create vHBA

Create vHBA

Name: FC0

Use SAN Connectivity Template: ☑

Create vHBA Template

vHBA Template: VDA-HBA-A

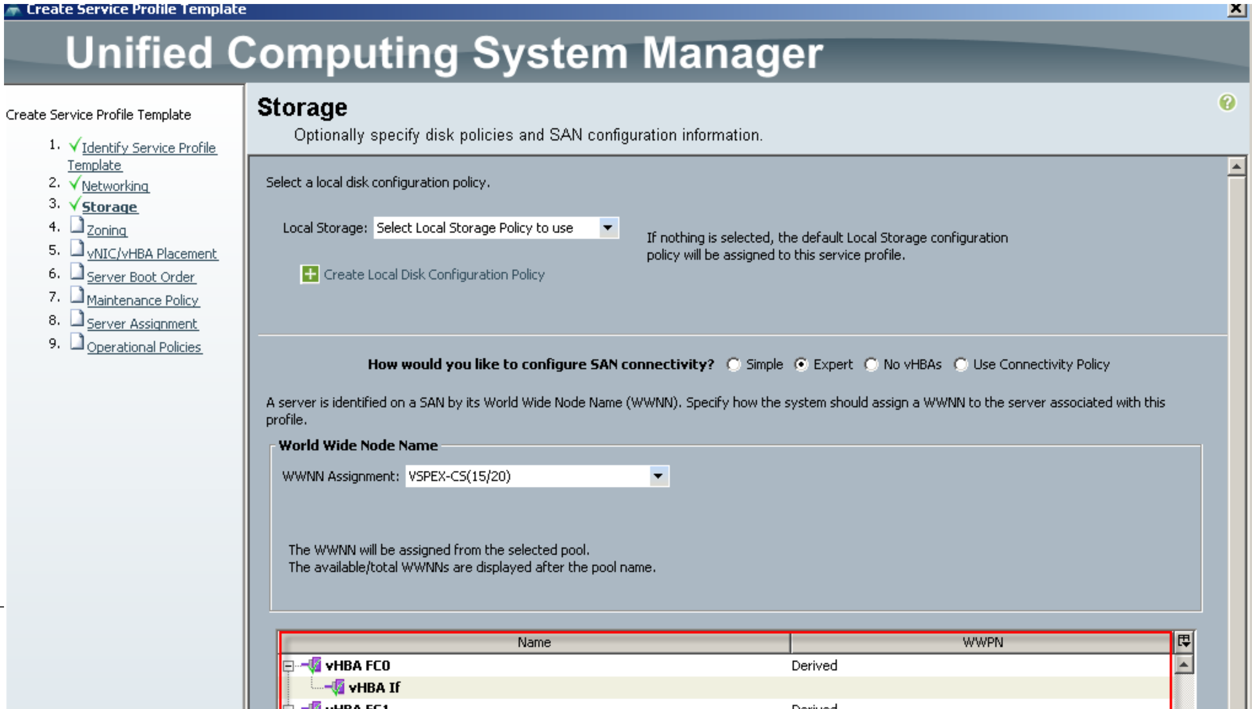
Adapter Performance Profile

Adapter Policy: VMWare

Create Fibre Channel Adapter Policy

We selected the vHBA template for Fabric Interconnect A and the VMware Adapter Policy from the drop downs, then clicked OK.

We repeated the process for FC1, choosing VDA-HBA-B for Fabric Interconnect B. The result is the Storage page that appears as follows:



Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

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

Storage

Optionally specify disk policies and SAN configuration information.

Select a local disk configuration policy.

Local Storage: Select Local Storage Policy to use

If nothing is selected, the default Local Storage configuration policy will be assigned to this service profile.

Create Local Disk Configuration Policy

How would you like to configure SAN connectivity? ○ Simple ● Expert ○ No vHBAs ○ Use Connectivity Policy

A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

World Wide Node Name

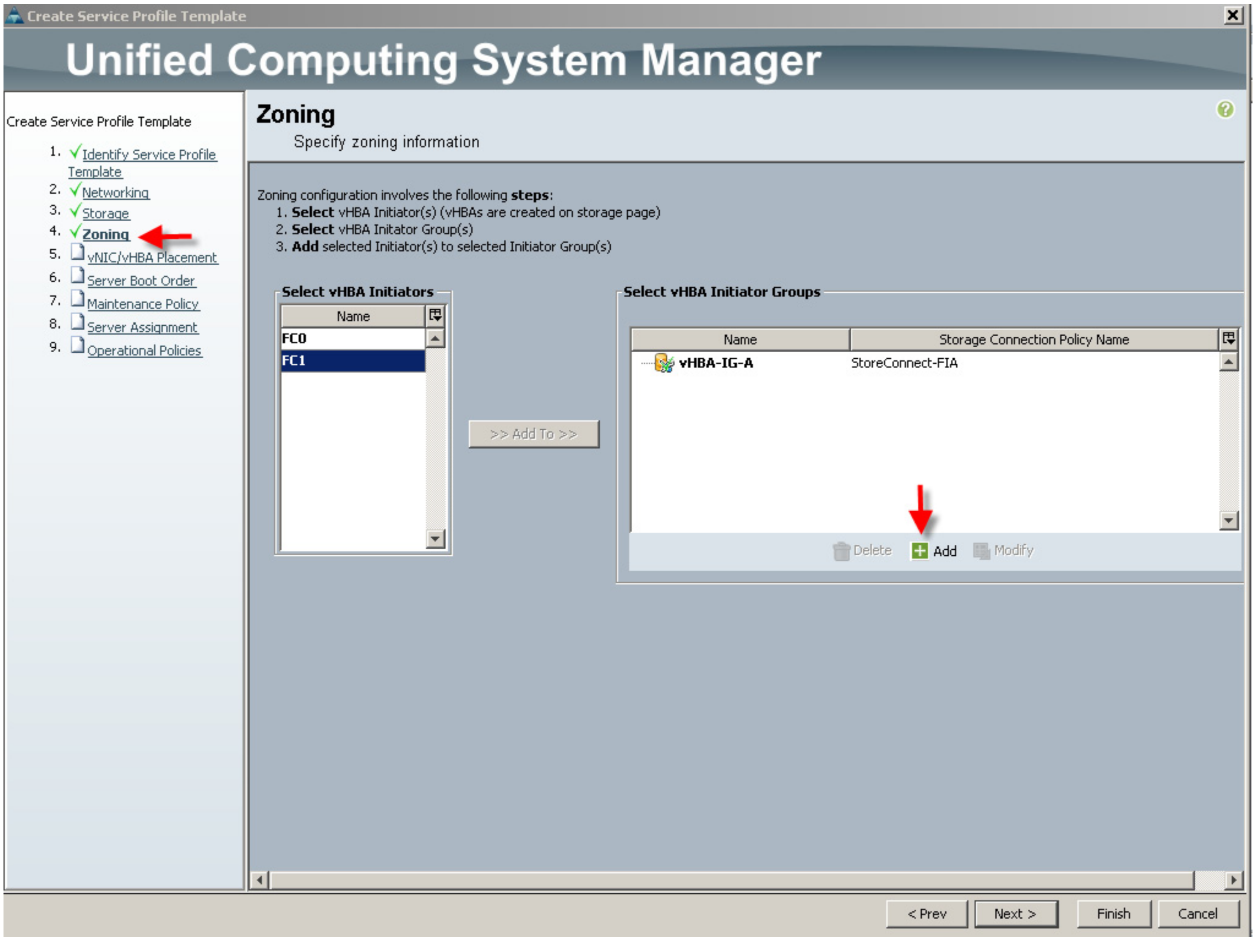
WWNN Assignment: VSPEX-CS(15/20)

The WWNN will be assigned from the selected pool.
The available/total WWNNs are displayed after the pool name.

Name	WWPN
vHBA FC0	Derived
vHBA If	
vHBA FC1	Derived

16g Part of the process for creating a Service Profile Template in UCS Manager 2.1 is to perform FC Zoning tasks. When you reach this task in the wizard, the vHBA Initiators added in step 3 appear in the Select vHBA Initiators section of the right pane. Before you can proceed, you must add vHBA Initiator Groups created previously or you can create them here.

Click the Add option in the Select vHBA Initiator Groups section in the right pane:



Create Service Profile Template

Unified Computing System Manager

Zoning

Specify zoning information

Zoning configuration involves the following **steps**:

1. **Select** vHBA Initiator(s) (vHBAs are created on storage page)
2. **Select** vHBA Initator Group(s)
3. **Add** selected Initiator(s) to selected Initiator Group(s)

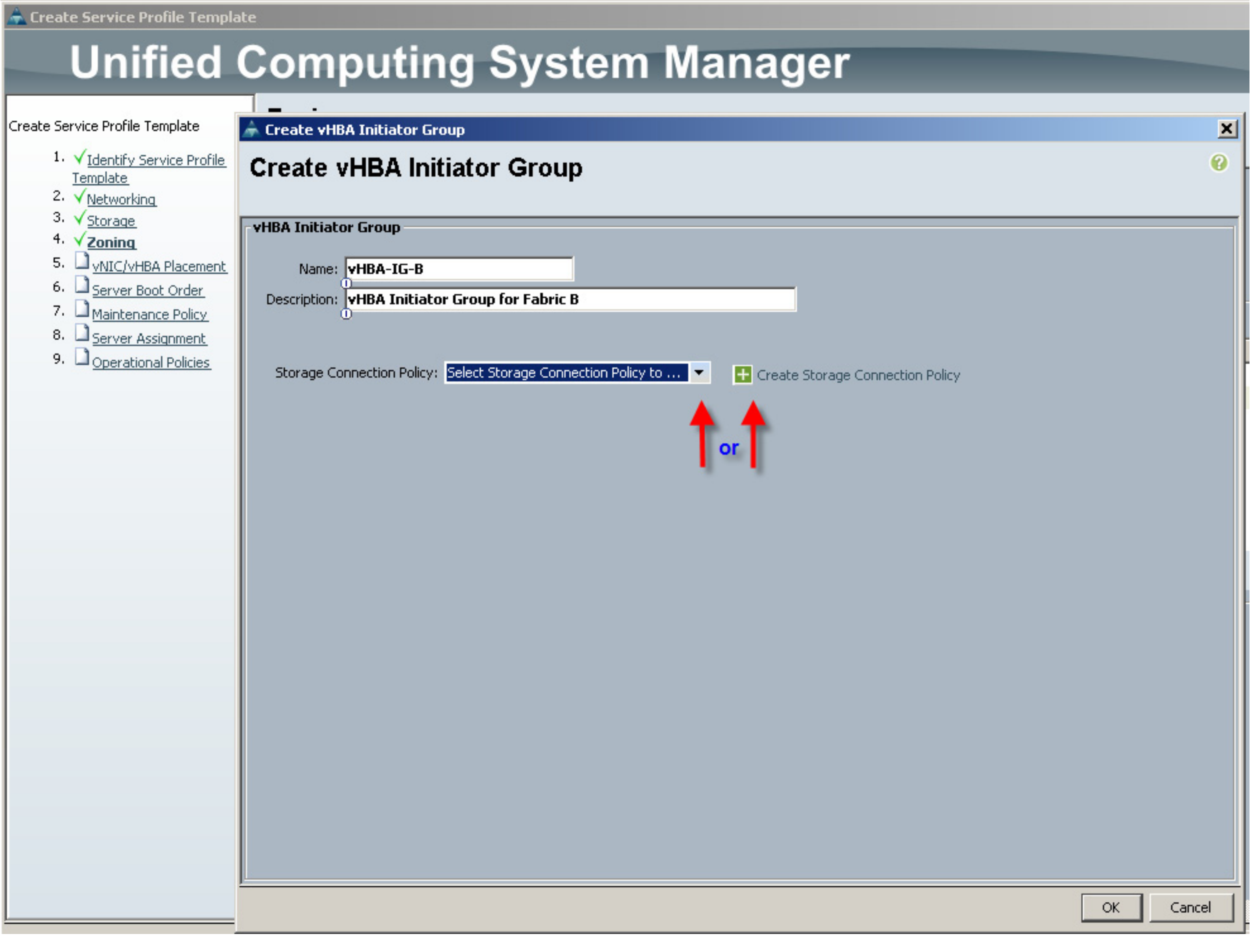
Select vHBA Initiators

Name
FC0
FC1

Select vHBA Initiator Groups

Name	Storage Connection Policy Name
vHBA-IG-A	StoreConnect-FIA

16h On the Create vHBA Initiator Group window, provide a unique name, optional description and then select a previously created Storage Connection Policy or click the +Create Storage Connection Policy control.



Create vHBA Initiator Group

vHBA Initiator Group

Name: vHBA-IG-B

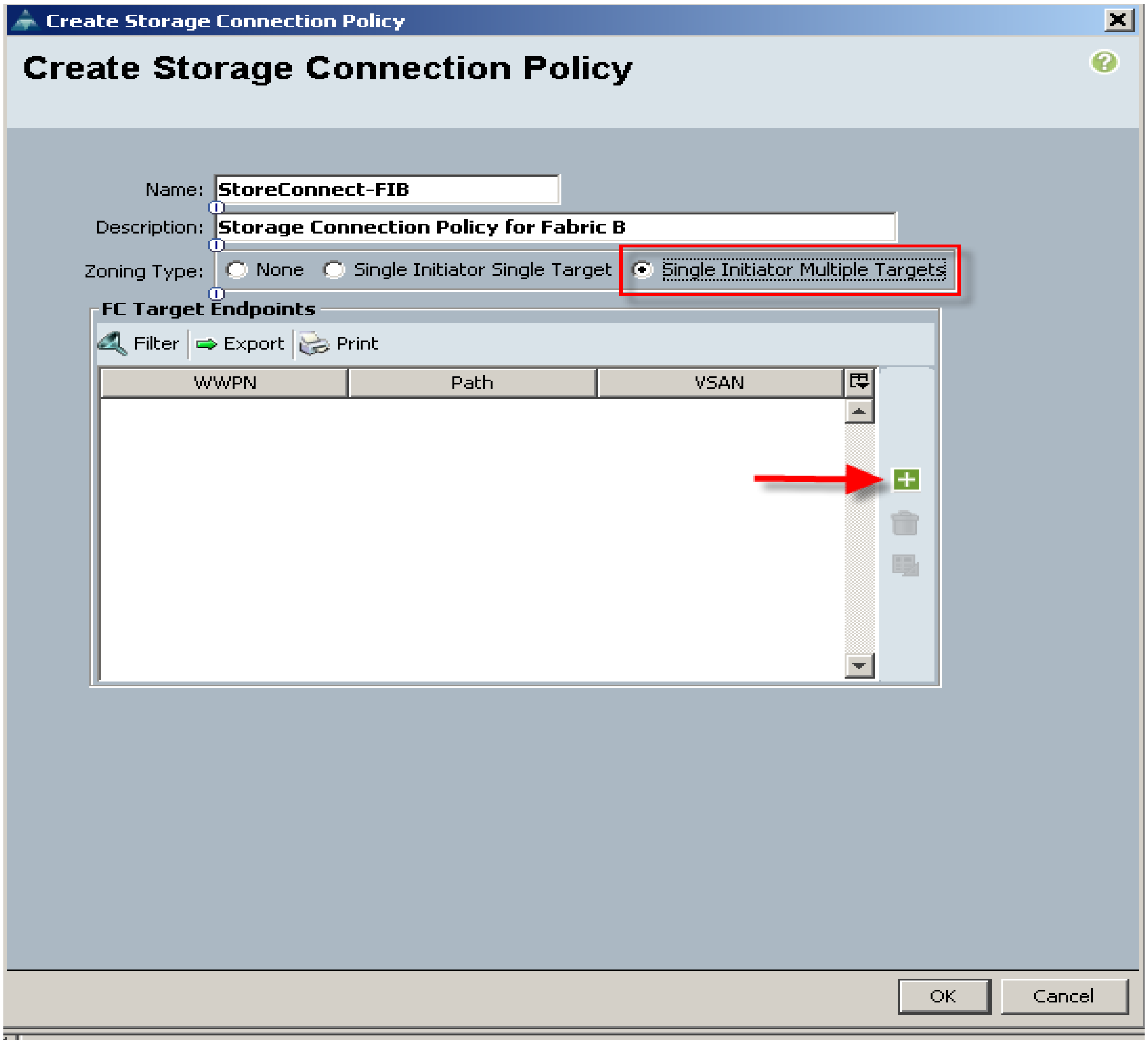
Description: vHBA Initiator Group for Fabric B

Storage Connection Policy: Select Storage Connection Policy to ...

Create Service Profile Template
Unified Computing System Manager
Create Service Profile Template
1. Identify Service Profile Template
2. Networking
3. Storage
4. Zoning
5. vNIC/vHBA Placement
6. Server Boot Order
7. Maintenance Policy
8. Server Assignment
9. Operational Policies
Create vHBA Initiator Group
Create Storage Connection Policy
or
OK
Cancel

16i In this case, we click the + Create Storage Connection Policy to demonstrate creating a new policy for Fabric B:

In the Create Storage Connection Policy window, provide a unique policy name, an optional description, select the Single Initiator Multiple Targets radio button when you have physically provisioned paths to multiple FC targets on each Fabric Interconnect (recommended,) and then click the + (Add) control on the right edge of the FC Target Endpoints area:



Create Storage Connection Policy

Name: StoreConnect-FIB

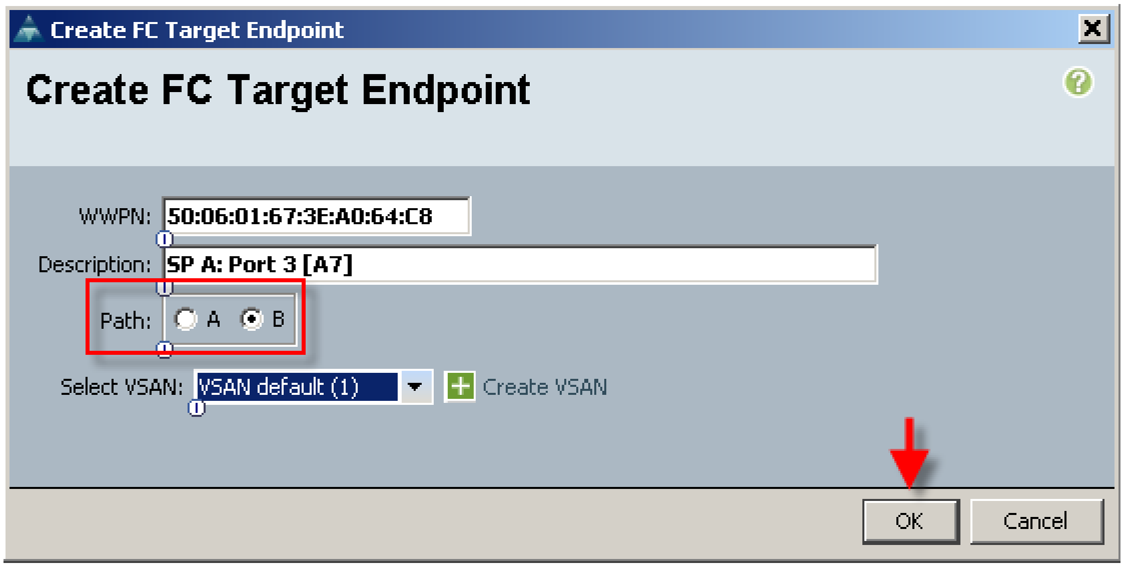
Description: Storage Connection Policy for Fabric B

Zoning Type: ○ None ○ Single Initiator Single Target ● Single Initiator Multiple Targets

FC Target Endpoints

WWPN	Path	VSAN

16j Input the World Wide Port Name value from the FC storage controllers that are connected to fabric B in our example case below, provide and optional description, select the B radio button in the path section, and select an existing VSAN or create a new one corresponding to a VSAN on your SAN controller.



Create FC Target Endpoint

WWPN: 50:06:01:67:3E:A0:64:C8

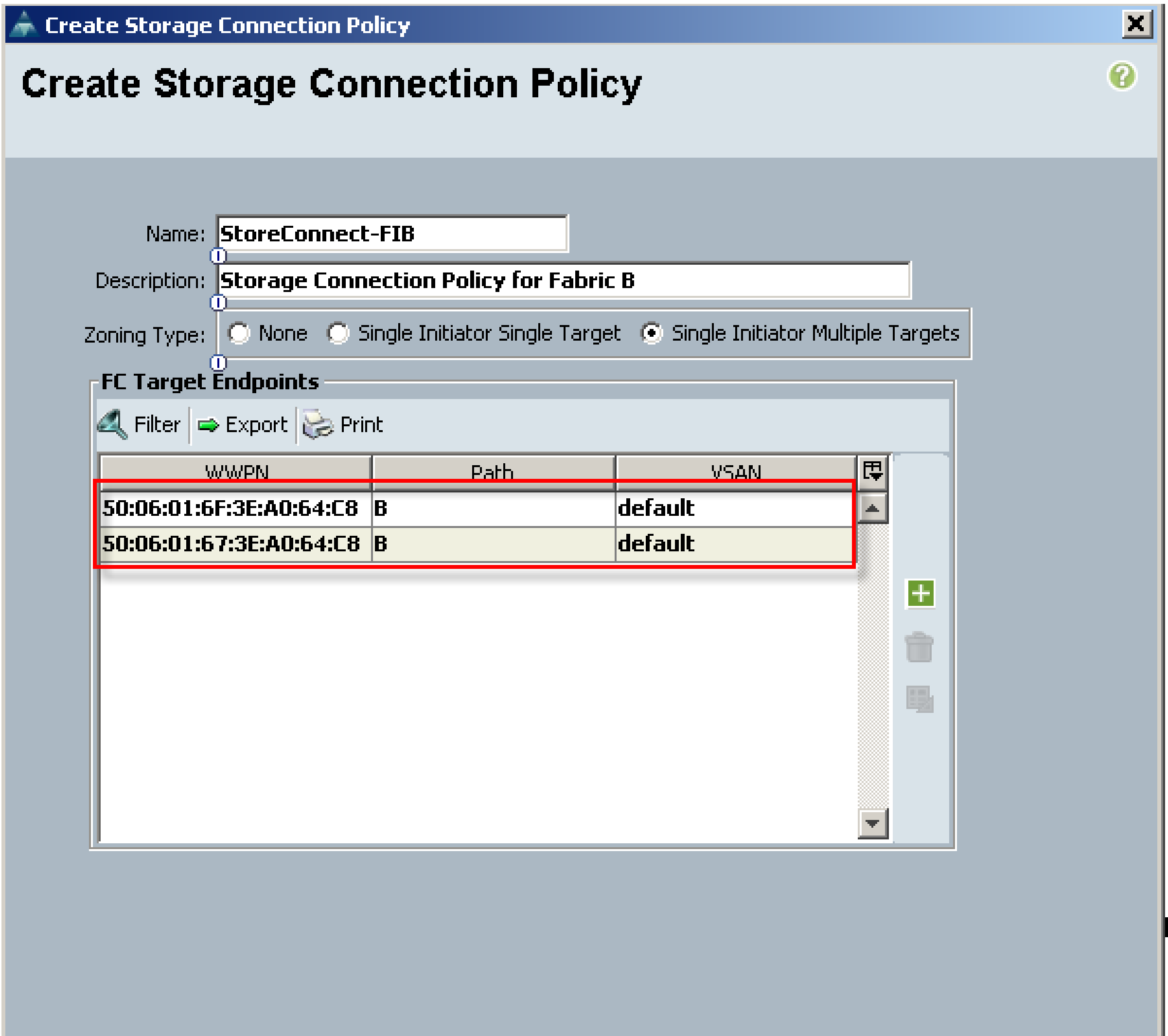
Description: SP A: Port 3 [A7]

Path: ○ A ● B

Select VSAN: VSAN default (1)

Repeat the process to add the second port to the SAN Controller.

Now click OK to add the Storage Connection Policy:



Create Storage Connection Policy

Name: StoreConnect-FIB

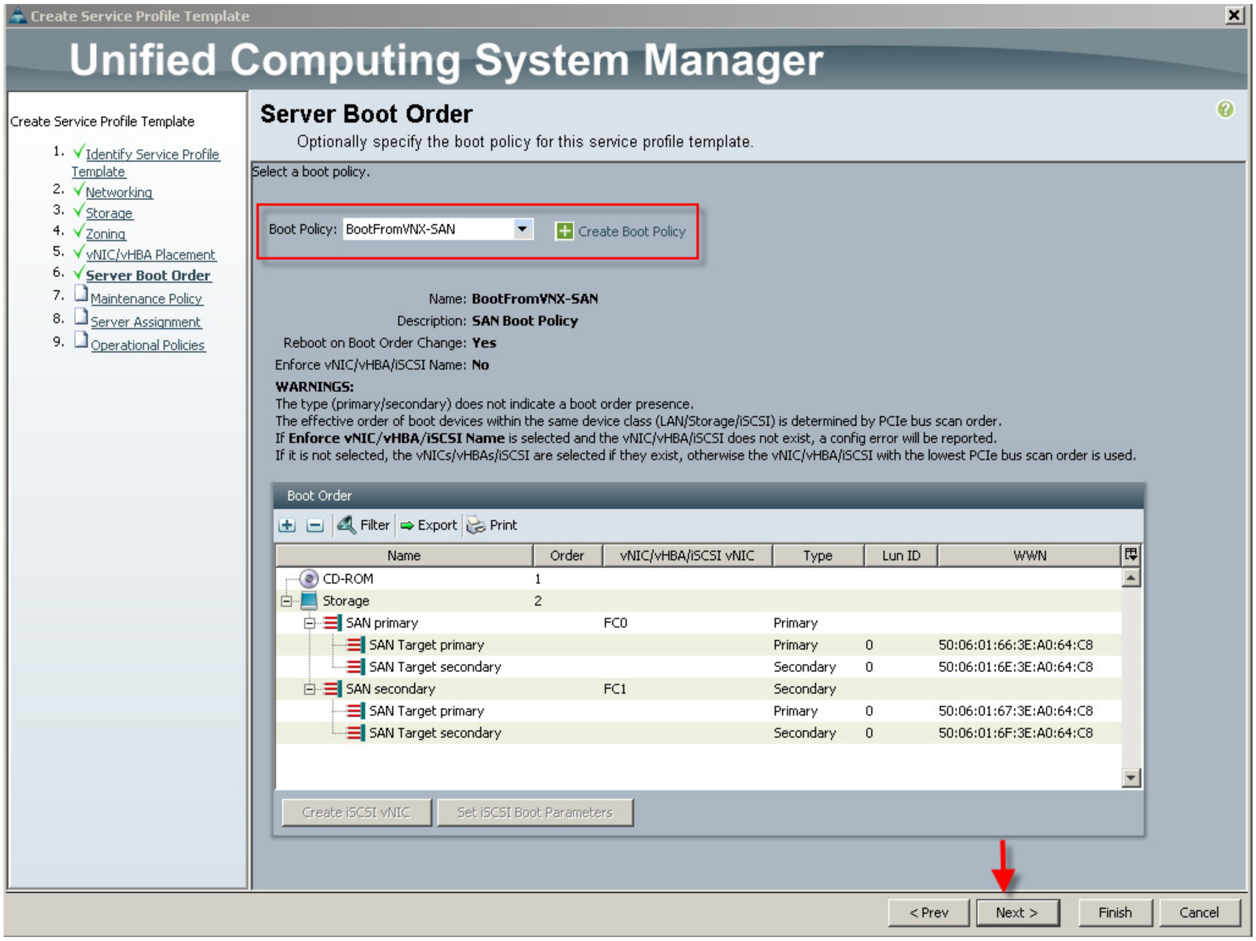
Description: Storage Connection Policy for Fabric B

Zoning Type: ○ None ○ Single Initiator Single Target ● Single Initiator Multiple Targets

FC Target Endpoints

WWPN	Path	VSAN
50:06:01:6F:3E:A0:64:C8	B	default
50:06:01:67:3E:A0:64:C8	B	default

16o Next, select the Boot Policy created earlier, use an existing default boot policy, or Create Boot Policy by clicking the + control. In our case, we selected the Boot from SAN policy created earlier. Once selected, the details of the policy are displayed in the lower portion of the window.



Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

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

Server Boot Order

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: BootFromVNX-SAN ▾ Create Boot Policy

Name: **BootFromVNX-SAN**
Description: **SAN Boot Policy**
Reboot on Boot Order Change: **Yes**
Enforce vNIC/vHBA/iSCSI Name: **No**

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

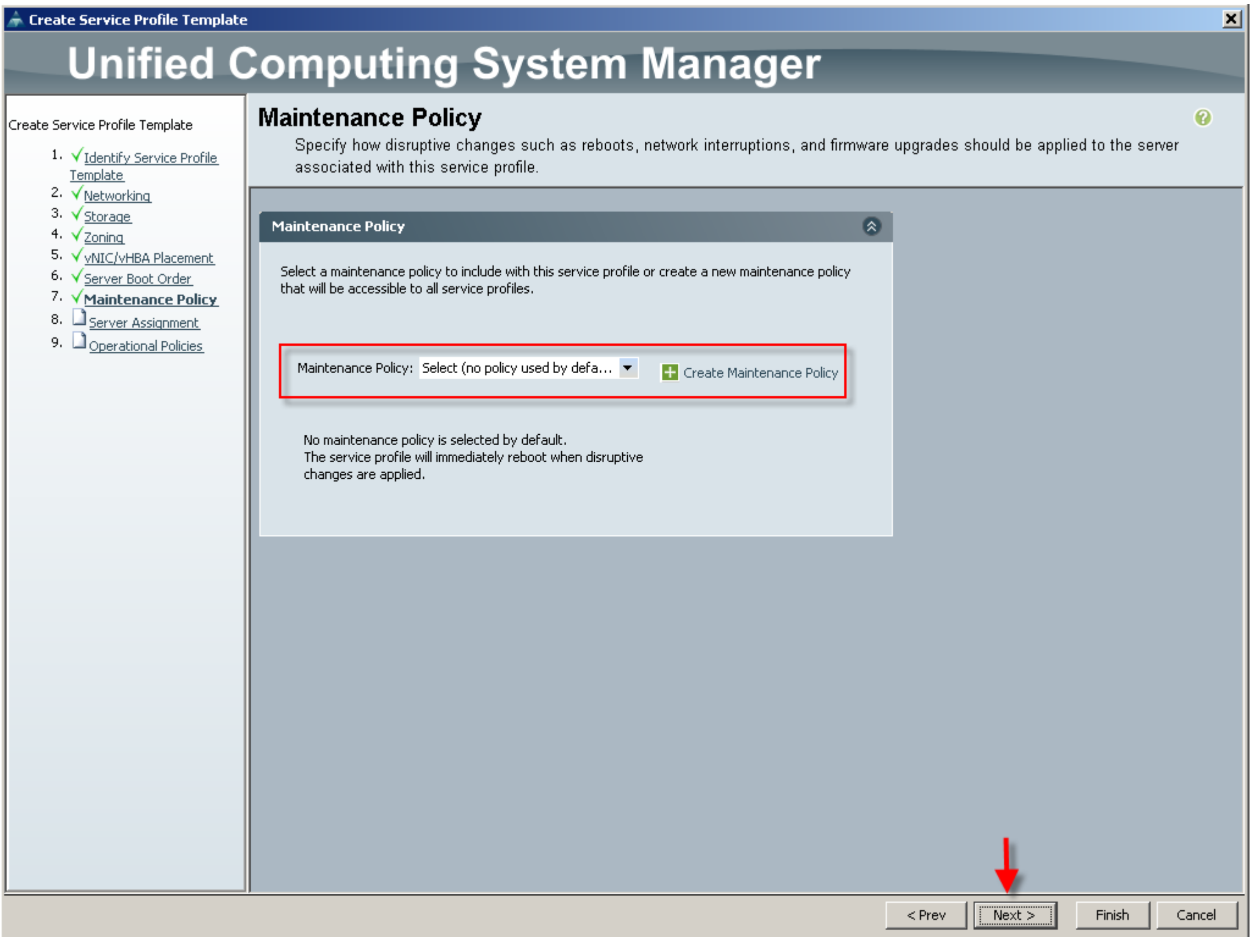
Boot Order

Filter Export Print

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN
CD-ROM	1				
Storage	2				
SAN primary		FC0	Primary		
SAN Target primary			Primary	0	50:06:01:66:3E:A0:64:C8
SAN Target secondary			Secondary	0	50:06:01:6E:3E:A0:64:C8
SAN secondary		FC1	Secondary		
SAN Target primary			Primary	0	50:06:01:67:3E:A0:64:C8
SAN Target secondary			Secondary	0	50:06:01:6F:3E:A0:64:C8

Click Next to continue

16p On the Maintenance Policy page, you can select the Maintenance Policy previously created, if any, or Create Maintenance Policy by clicking the + control. In this study, no maintenance policy was created nor used.



Maintenance Policy

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

Maintenance Policy

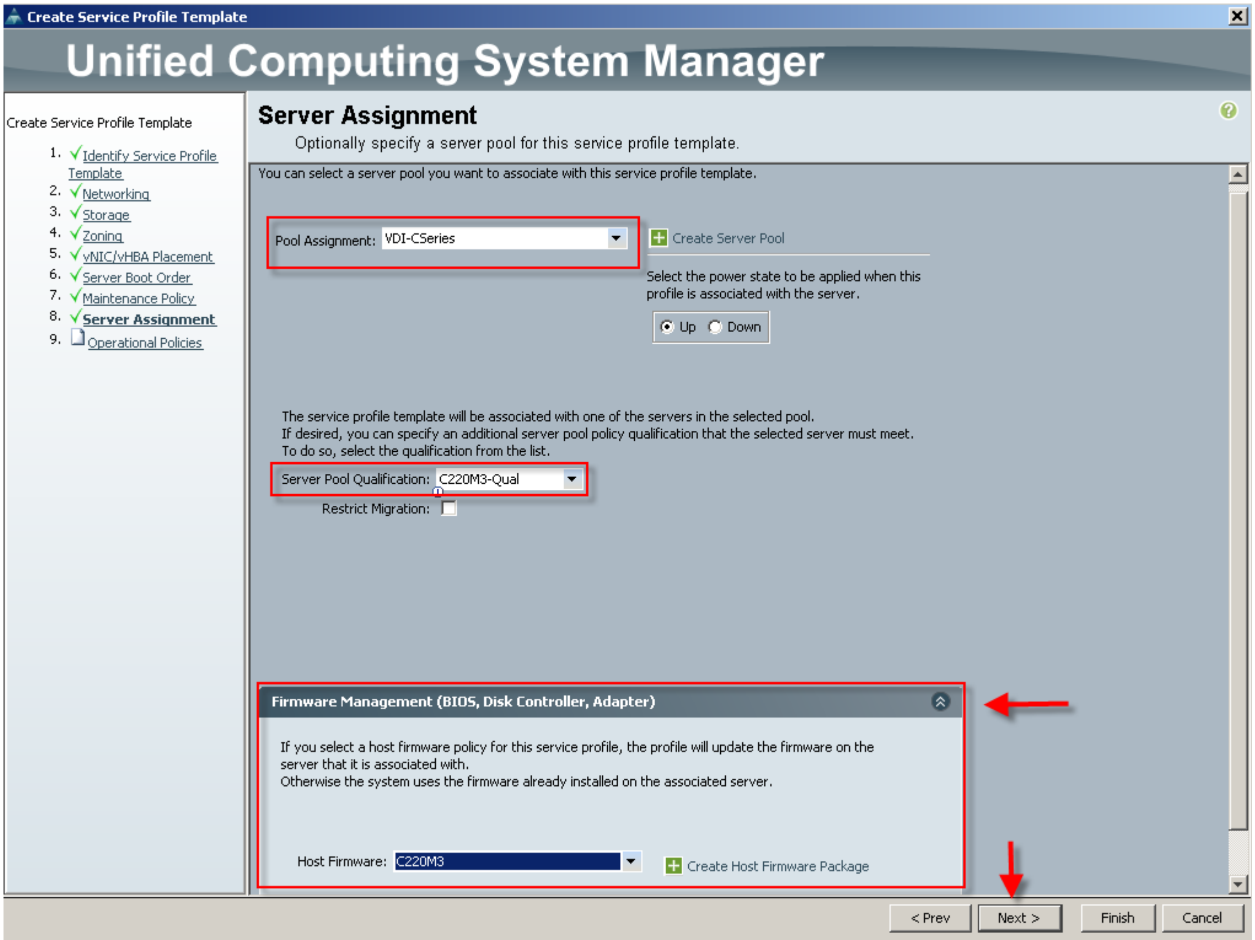
Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: Select (no policy used by defa... + Create Maintenance Policy

No maintenance policy is selected by default.
The service profile will immediately reboot when disruptive changes are applied.

Click Next to continue

16q On the Server Assignment page, utilize the Server Pool and Server Pool Qualification from the drop downs. You can create a Server Pool from the wizard, but you cannot create a Server Pool Qualification policy from here. In our study, we utilized the Server Pool and Server Pool Qualification policy we created earlier. We expanded the Firmware Management node near the bottom of the page and selected the policy we created earlier.



Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

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

Server Assignment

Optionally specify a server pool for this service profile template.

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

Pool Assignment: VDI-CSeries

Create Server Pool

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

● Up ○ Down

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

Server Pool Qualification: C220M3-Qual

Restrict Migration: □

Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with.
Otherwise the system uses the firmware already installed on the associated server.

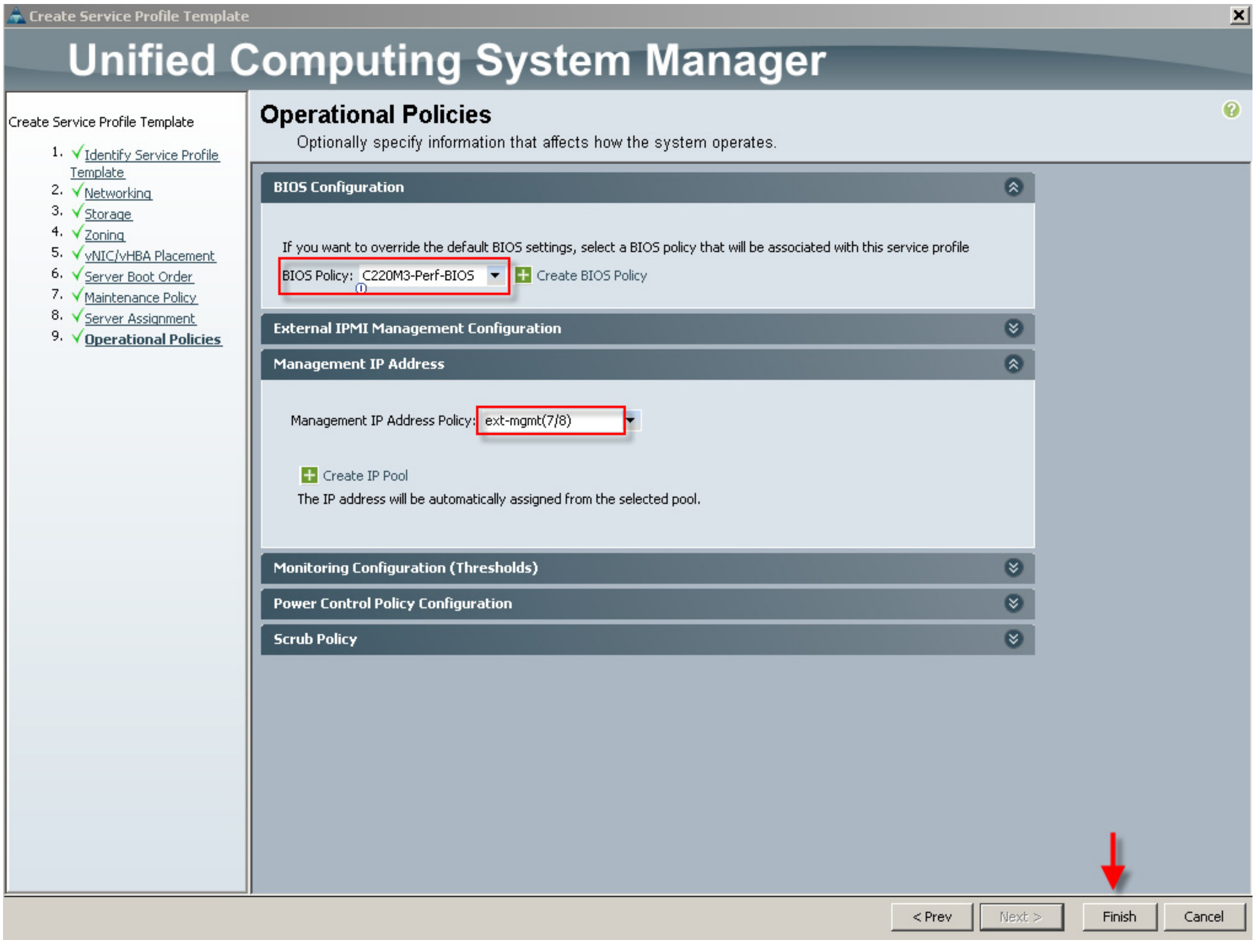
Host Firmware: C220M3

Create Host Firmware Package

Click Next to continue.

16r On the Operational Policy page, you can configure BIOS, External IPMI Management, Management IP Address, Monitoring, Power Control and Scrub configuration and policies for the UCS Servers the template will be applied to.

In our study, we configured a BIOS Policy and created a Management IP Address pool which we applied to the template. Note that you can create policies and pools from within this wizard.



Create Service Profile Template
Unified Computing System Manager
Create Service Profile Template
1. Identify Service Profile Template
2. Networking
3. Storage
4. Zoning
5. vNIC/vHBA Placement
6. Server Boot Order
7. Maintenance Policy
8. Server Assignment
9. Operational Policies
Operational Policies
Optionally specify information that affects how the system operates.
BIOS Configuration
External IPMI Management Configuration
Management IP Address
Create BIOS Policy
Create IP Pool
Monitoring Configuration (Thresholds)
Power Control Policy Configuration
Scrub Policy
< Prev
Next >
Finish
Cancel

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy: C220M3-Perf-BIOS

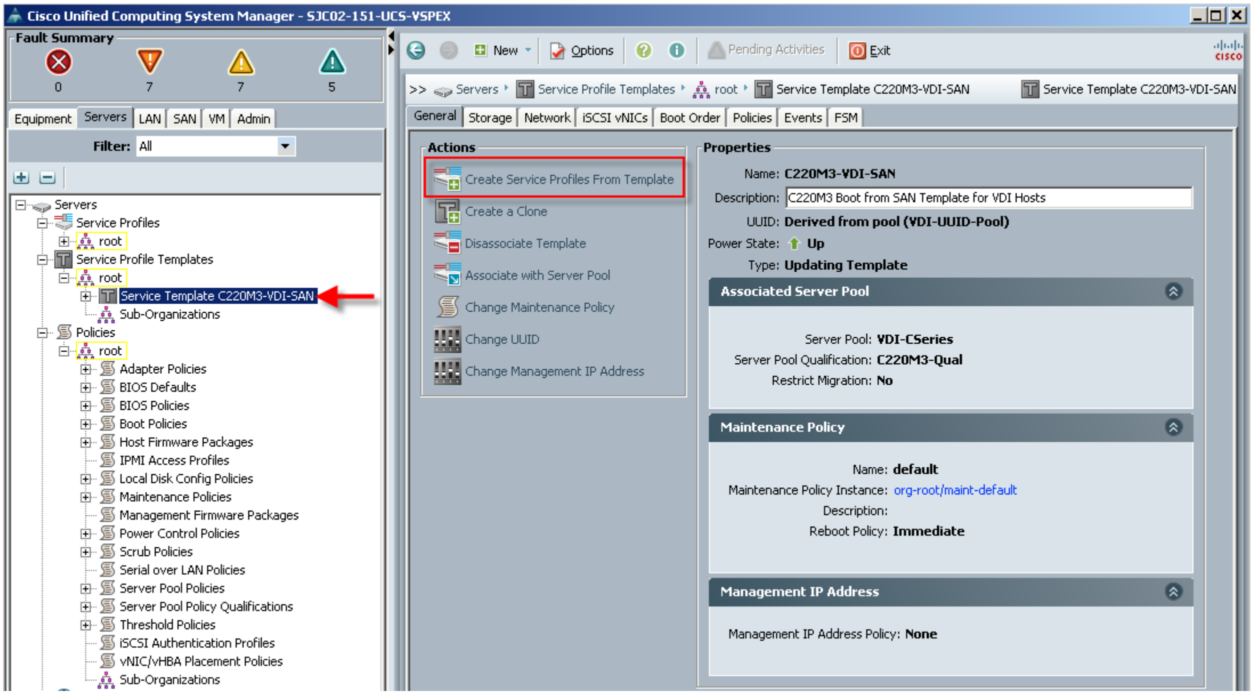
Management IP Address Policy: ext-mgmt(7/8)

The IP address will be automatically assigned from the selected pool.

Click Finish to complete the wizard.

Click OK to acknowledge successful creation.

17 Now that we had created the Service Profile Templates for each UCS Blade Server model used in the project, we used them to create the appropriate number of Service Profiles. To do so, in the Servers tab in the navigation page, in the Service Profile Templates node, we expanded the root and selected Service Template B200 M3, then clicked on Create Service Profiles from Template in the right pane, Actions area:



Cisco Unified Computing System Manager - SJC02-151-UCS-VSPEX

Fault Summary: 0, 7, 7, 5

Servers
- Service Profiles
  - root
- Service Profile Templates
  - root
    - Service Template C220M3-VDI-SAN
    - Sub-Organizations
- Policies
  - root
    - Adapter Policies
    - BIOS Defaults
    - BIOS Policies
    - Boot Policies
    - Host Firmware Packages
    - IPMI Access Profiles
    - Local Disk Config Policies
    - Maintenance Policies
    - Management Firmware Packages
    - Power Control Policies
    - Scrub Policies
    - Serial over LAN Policies
    - Server Pool Policies
    - Server Pool Policy Qualifications
    - Threshold Policies
    - iSCSI Authentication Profiles
    - vNIC/vHBA Placement Policies
    - Sub-Organizations

>> Servers > Service Profile Templates > root > Service Template C220M3-VDI-SAN

Actions
- Create Service Profiles From Template
- Create a Clone
- Disassociate Template
- Associate with Server Pool
- Change Maintenance Policy
- Change UUID
- Change Management IP Address

Properties

Name: C220M3-VDI-SAN
Description: C220M3 Boot from SAN Template for VDI Hosts
UUID: Derived from pool (VDI-UUID-Pool)
Power State: Up
Type: Updating Template

Associated Server Pool

Server Pool: VDI-CSeries
Server Pool Qualification: C220M3-Qual
Restrict Migration: No

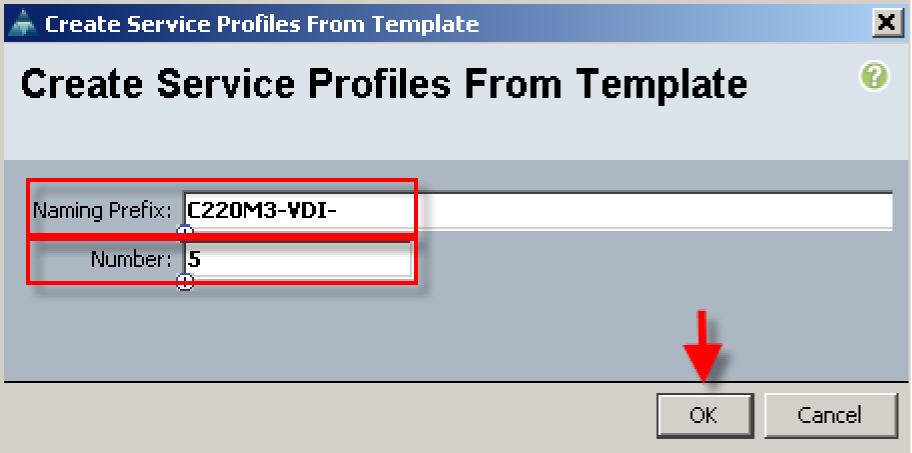
Maintenance Policy

Name: default
Maintenance Policy Instance: org-root/maint-default
Description:
Reboot Policy: Immediate

Management IP Address

Management IP Address Policy: None

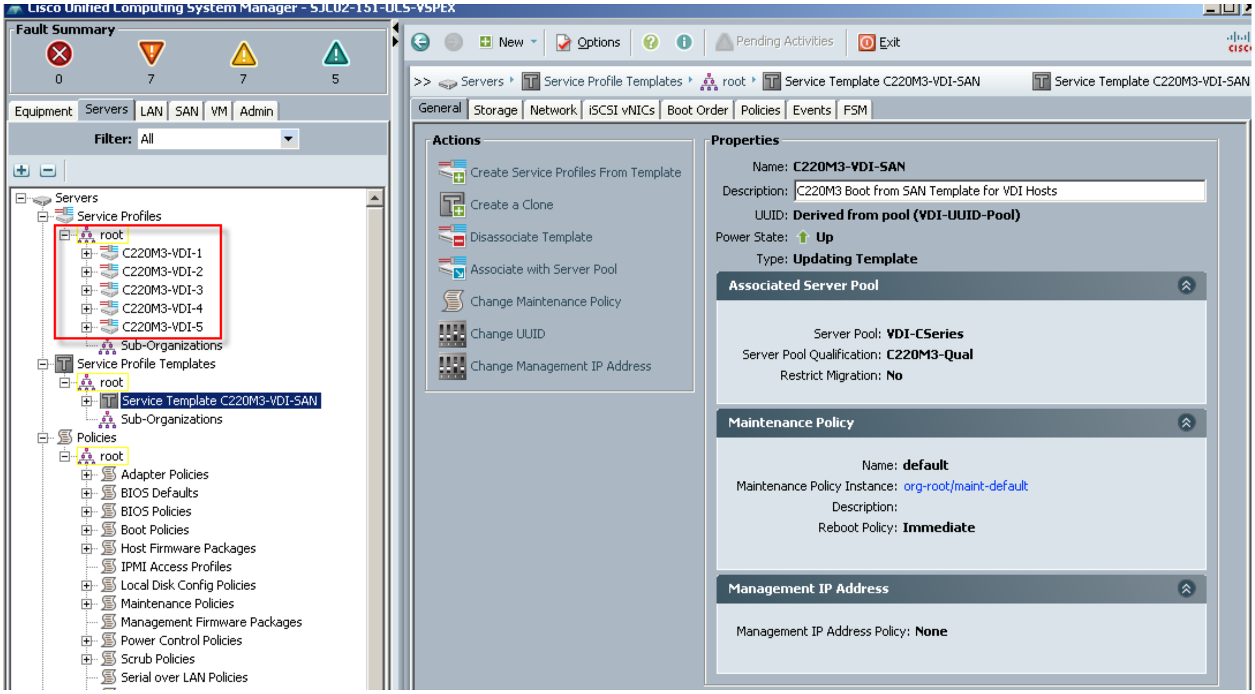
17a We provided the naming prefix and the number of Service Profiles to create and clicked OK



Create Service Profiles From Template

Naming Prefix: C220M3-VDI-
Number: 5

17b Cisco UCS Manager created the requisite number of profiles and because of the Associated Server Pool and Server Pool Qualification policy, the B200 M3 blades in the test environment began automatically associating with the proper Service Profile.



Properties

Name: C220M3-VDI-SAN
Description: C220M3 Boot from SAN Template for VDI Hosts
UUID: Derived from pool (VDI-UUID-Pool)
Power State: Up
Type: Updating Template

Associated Server Pool

Server Pool: VDI-CSeries
Server Pool Qualification: C220M3-Qual
Restrict Migration: No

Maintenance Policy

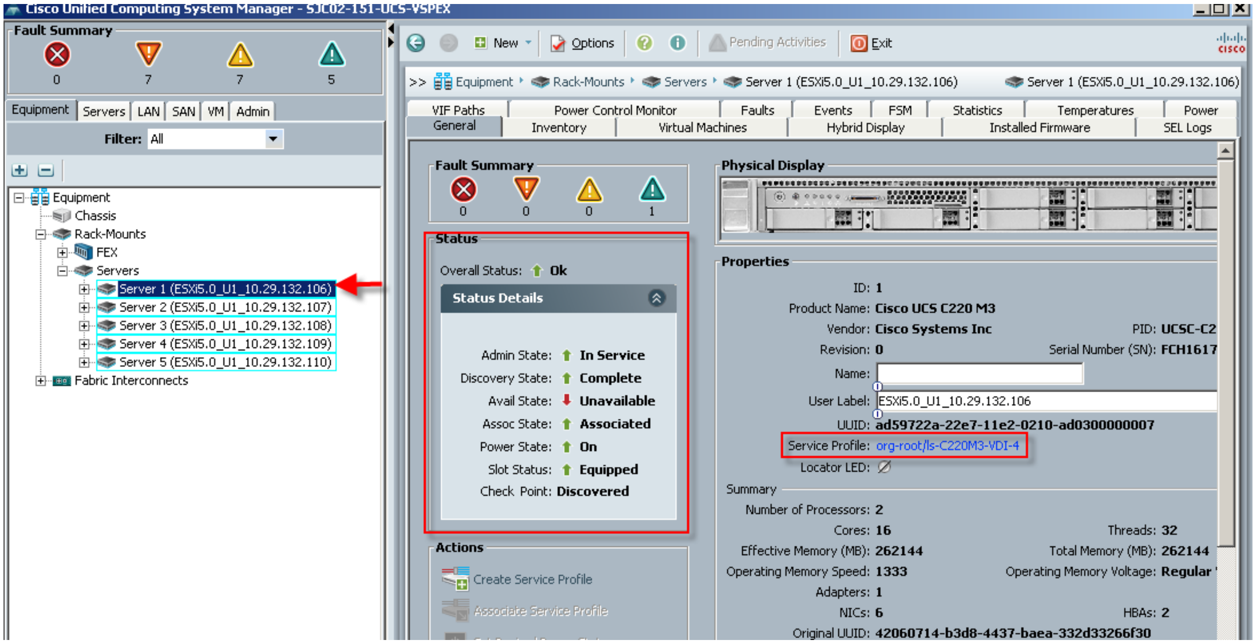
Name: default
Maintenance Policy Instance: org-root/maint-default
Description:
Reboot Policy: Immediate

Management IP Address

Management IP Address Policy: None

Each of the Cisco UCS C220 M3 servers was automatically assigned one of the service profiles based on its pool and pool qualification policy.

18 We verified that each server had a Service Profile.


Cisco Unified Computing System Manager - SJC02-151-UCS-VSPEX
Fault Summary
0
7
7
5
Equipment
Servers
LAN
SAN
VM
Admin
Filter: All
Equipment
Chassis
Rack-Mounts
FEX
Servers
Server 1 (ESXi5.0_U1_10.29.132.106)
Server 2 (ESXi5.0_U1_10.29.132.107)
Server 3 (ESXi5.0_U1_10.29.132.108)
Server 4 (ESXi5.0_U1_10.29.132.109)
Server 5 (ESXi5.0_U1_10.29.132.110)
Fabric Interconnects
New
Options
Pending Activities
Exit
>> Equipment › Rack-Mounts › Servers › Server 1 (ESXi5.0_U1_10.29.132.106)
Server 1 (ESXi5.0_U1_10.29.132.106)
VIF Paths
Power Control Monitor
Faults
Events
FSM
Statistics
Temperatures
Power
General
Inventory
Virtual Machines
Hybrid Display
Installed Firmware
SEL Logs
Fault Summary
0
0
0
1
Physical Display
Actions
Create Service Profile
Associate Service Profile

Status

Overall Status: Ok

Status Details

Admin State: In Service
Discovery State: Complete
Avail State: Unavailable
Assoc State: Associated
Power State: On
Slot Status: Equipped
Check Point: Discovered

Properties

ID: 1
Product Name: Cisco UCS C220 M3
Vendor: Cisco Systems Inc
PID: UCSC-C2
Revision: 0
Serial Number (SN): FCH1617
Name:
User Label: ESXi5.0_U1_10.29.132.106
UUID: ad59722a-22e7-11e2-0210-ad0300000007
Service Profile: org-root/ls-C220M3-VDI-4
Locator LED:

Summary

Number of Processors: 2
Cores: 16
Threads: 32
Effective Memory (MB): 262144
Total Memory (MB): 262144
Operating Memory Speed: 1333
Operating Memory Voltage: Regular
Adapters: 1
NICs: 6
HBAs: 2
Original UUID: 42060714-b3d8-4437-baea-332d33266f30

At this point, the Cisco UCS Blade Servers are ready for hypervisor installation.

6.2.2 QoS and CoS in Cisco Unified Computing System

Cisco Unified Computing System provides different system class of service to implement quality of service including:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames.

Applications like the Cisco Unified Computing System and other time sensitive applications have to adhere to a strict QOS for optimal performance.

6.2.3 System Class Configuration

Systems Class is the global operation where entire system interfaces are with defined QoS rules.

- By default system has Best Effort Class and FCoE Class.
- Best effort is equivalent in MQC terminology as “match any”
    - FCoE is special Class define for FCoE traffic. In MQC terminology “match cos 3”
- System class allowed with 4 more users define class with following configurable rules.
    - CoS to Class Map
    - Weight: Bandwidth
    - Per class MTU
    - Property of Class (Drop v/s no drop)
- Max MTU per Class allowed is 9216.
- Via UCS we can map one CoS value to particular class.
- Apart from FcoE class there can be only one more class can be configured as no-drop property.
- Weight can be configured based on 0 to 10 numbers. Internally system will calculate the bandwidth based on following equation (there will be rounding off the number).
    - % b/w shared of given Class = $\dfrac{\text{(Weight of the given priority * 100)}}{\text{Sum of weights of all priority}}$

6.2.4 Cisco UCS System Class Configuration

Cisco Unified Computing System defines user class names as follows.

- Platinum
- Gold
- Silver
- Bronze

Table 3 *Name Table Map between Cisco Unified Computing System and the NXOS*

Cisco UCS Names	NXOS Names
Best effort	Class-default
FC	Class-fc
Platinum	Class-Platinum
Gold	Class-Gold
Silver	Class-Silver
Bronze	Class-Bronze

Table 4 *Class to CoS Map by default in Cisco Unified Computing System*

Cisco UCS Class Names	Cisco UCS Default Class Value
Best effort	Match any
Fc	3
Platinum	5
Gold	4
Silver	2
Bronze	1

Table 5 *Default Weight in Cisco Unified Computing System*

Cisco UCS Class Names	Weight
Best effort	5
Fc	5

6.2.5 Steps to Enable QOS on the Cisco Unified Computing System

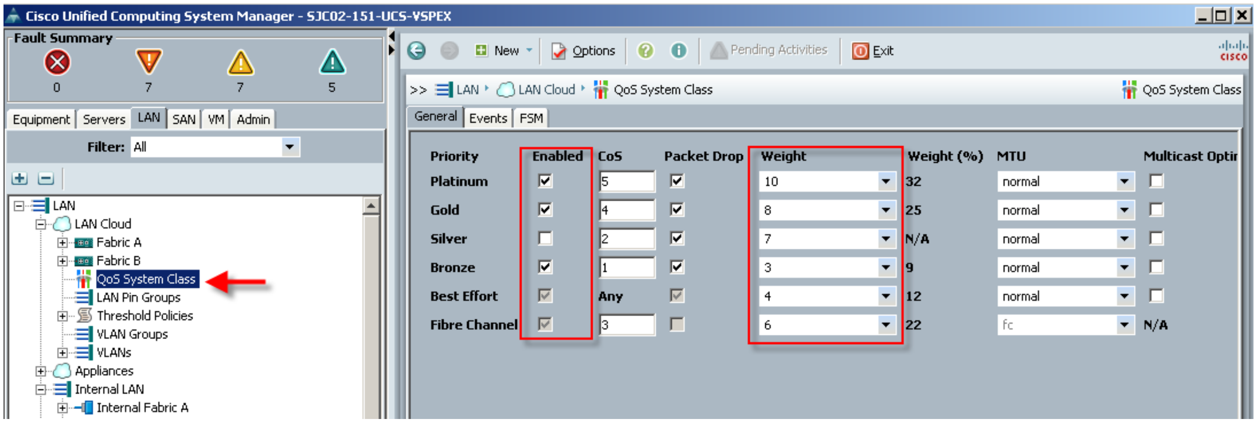
For this study, we utilized four Cisco UCS QoS System Classes to priorities four types of traffic in the infrastructure:

Table 6 *QoS Priority to vNIC and VLAN Mapping*

Cisco UCS Qos Priority	vNIC Assignment	VLAN Supported
Platinum	eth2, eth3	100 (VDI)
Gold	eth0, eth1	132 (ESXi_Management)
Bronze	eth4, eth5	51 (vMotion)

Configure Platinum, Gold, and Bronze System Classes by checking the enabled box.

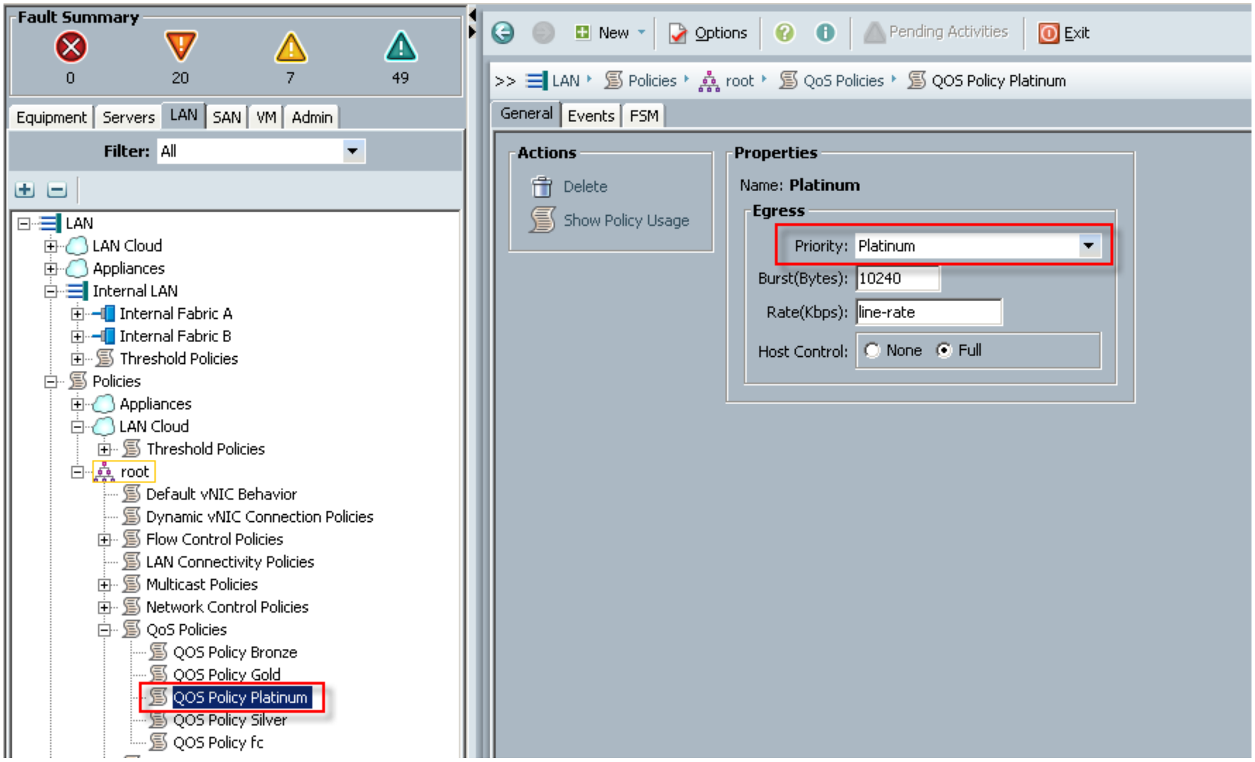
Figure 13 Cisco UCS QoS System Class Configuration



Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optir
Platinum	☑	5	☑	10	32	normal	☐
Gold	☑	4	☑	8	25	normal	☐
Silver	☐	2	☑	7	N/A	normal	☐
Bronze	☑	1	☑	3	9	normal	☐
Best Effort	☑	Any	☑	4	12	normal	☐
Fibre Channel	☑	3	☐	6	22	fc	N/A

Next, in the LAN tab under Policies, Root, QoS Polices, verify QoS Policies Platinum, Gold, Silver and Bronze exist, with each QoS policy mapped to its corresponding Priority.

Figure 14 Cisco UCS QoS Policy Configuration



Properties

Name: **Platinum**

Egress

Priority: Platinum

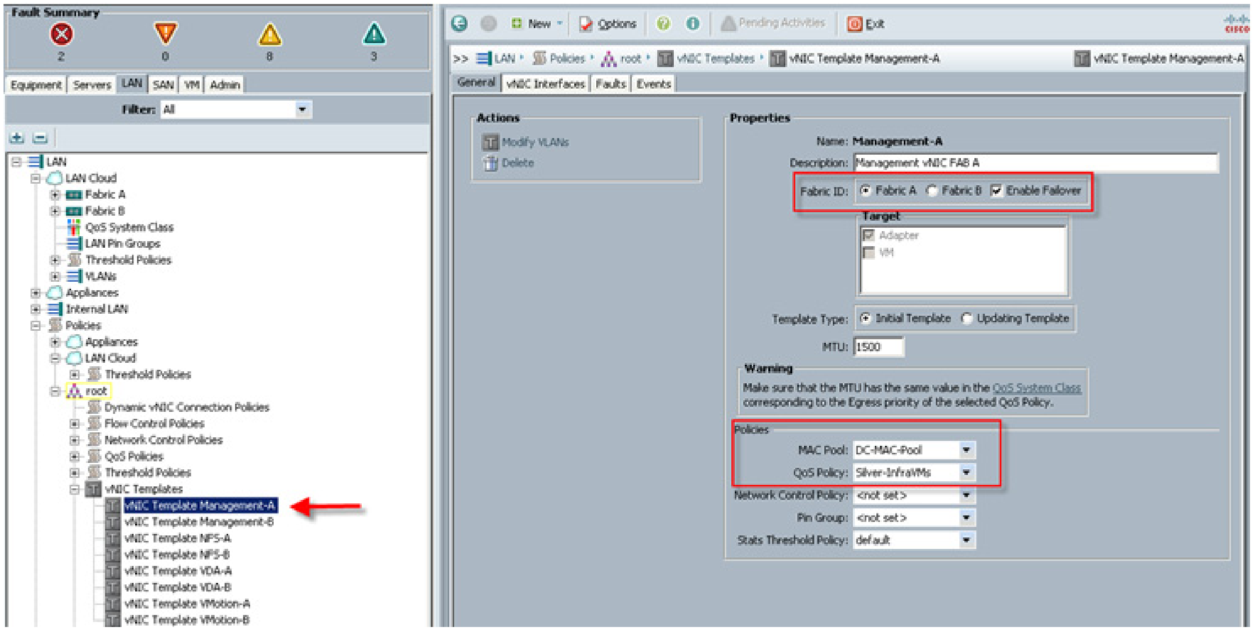
Burst(Bytes): 10240

Rate(Kbps): line-rate

Host Control: ○ None ● Full

Finally, include the corresponding QoS Policy into each vNIC template using the QoS policy drop down, using the QoS Priority to vNIC and VLAN Mapping table above.

Figure 15 Utilize QoS Policy in vNIC Template



Filter: All

Name: **Management-A**

Description: Management vNIC FAB A

Fabric ID: ● Fabric A ○ Fabric B ☑ Enable Failover

Target: ☑ Adapter □ VM

Template Type: ● Initial Template ○ Updating Template

MTU: 1500

Warning: Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.

MAC Pool: DC-MAC-Pool

QoS Policy: Silver-InfraVMs

Network Control Policy: <not set>

Pin Group: <not set>

Stats Threshold Policy: default

This is a unique value proposition for Cisco UCS with respect to end-to-end QOS.

6.3 LAN Configuration

The access layer LAN configuration consists of a pair of Cisco Nexus 5548s (N5Ks,) a family member of our low-latency, line-rate, 10 Gigabit Ethernet and FCoE switches for our VDI deployment.

6.3.1 Nexus 5548UP and VNX5300 Connectivity (Unmanaged NFS Variant)

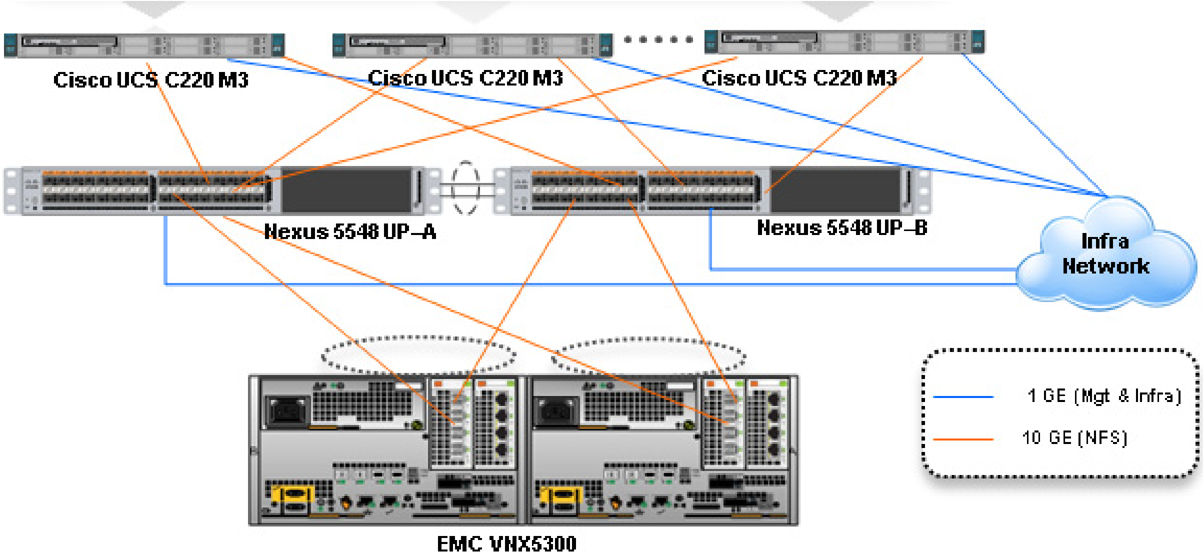
The access layer LAN configuration consists of a pair of Cisco Nexus 5548UPs (N5Ks,) a family member of our low-latency, line-rate, 10 Gigabit Ethernet and FCoE switches for our VDI deployment uplinked to the Customers existing L3 network.

In the Unmanaged NFS Variant, the Cisco UCS C220 M3 servers are managed in standalone mode, requiring a management/infrastructure network connection and a separate high speed data connection to the EMC VNX5300 storage system.

Five UCS C220 M3 Rack-Mount servers are connected via their VIC1225 to 10Gb ports on a pair of N5Ks to the EMC VNX NFS storage. One or both of each servers' integrated 1 Gb ethernet ports is/are connected to the upstream or top of rack L3 switch for management and all infrastructure communications.

Note The upstream configuration is beyond the scope of this document; there are some good reference documents that talk about best practices of using the Cisco Nexus 5000 and 7000 Series Switches. New with the Nexus 5500 series is an available Layer 3 module that was not used in these tests and that will not be covered in this document.

Figure 16 Unmanaged NFS Variant Ethernet Network Configuration with Cisco Nexus 5500 Series Switches

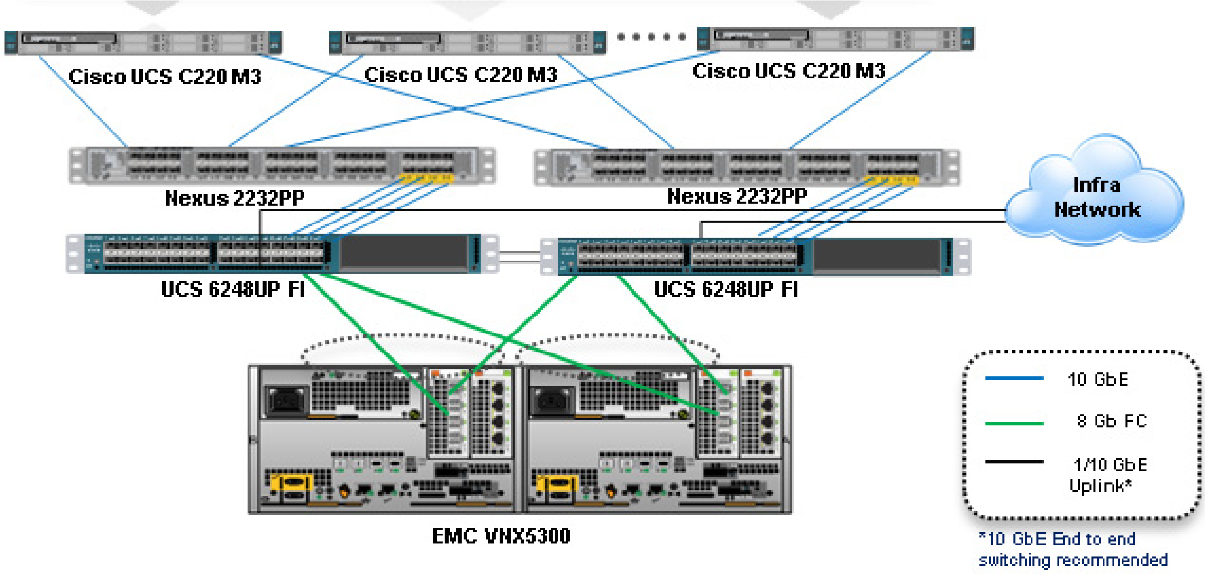


6.3.2 Cisco UCS Fabric Interconnect 6248UP and VNX5300 Connectivity (Managed FC Variant)

In the Managed FC Variant, the UCS C220 M3 servers are connected to a pair of UCS 6248UP Fabric Interconnects (FIs) via two Nexus 2232PP Fabric Extenders. The VNX5300 is connected to the FI FC Storage Ports directly via Fiber Channel. Fibre Channel zoning is done on the FIs. The FIs are uplinked to the Customer top of rack L3 switch.

In this configuration, called Managed Single Wire Cluster Setup, only the two 10 GbE ports on the VIC1225 CNA are used for all communications. In addition, Cisco UCS Manager 2.1 manages the configuration of the servers through Cisco UCS Service Profiles.

Figure 17 Managed FC Variant Network Configuration



6.4 SAN Configuration

For the two variants of this study, different equipment was used to connect to the VNX5300 storage outlined in Section 6.3 above. Only the Managed FC Variant supports booting from the VNX5300. This section describes the SAN Configuration supporting boot from SAN.

6.4.1 Boot from SAN Benefits

Booting from SAN is another key feature which helps in moving towards stateless computing in which there is no static binding between a physical server and the OS / applications it is tasked to run. The OS is installed on a SAN LUN and boot from SAN policy is applied to the service profile template or the service profile. If the service profile were to be moved to another server, the pwwn of the HBAs and the Boot from SAN (BFS) policy also moves along with it. The new server now takes the same exact character of the old server, providing the true unique stateless nature of the Cisco UCS Blade Server.

The key benefits of booting from the network:

- Reduce Server Footprints: Boot from SAN alleviates the necessity for each server to have its own direct-attached disk, eliminating internal disks as a potential point of failure. Thin diskless servers also take up less facility space, require less power, and are generally less expensive because they have fewer hardware components.
- Disaster and Server Failure Recovery: All the boot information and production data stored on a local SAN can be replicated to a SAN at a remote disaster recovery site. If a disaster destroys functionality of the servers at the primary site, the remote site can take over with minimal downtime.
- Recovery from server failures is simplified in a SAN environment. With the help of snapshots, mirrors of a failed server can be recovered quickly by booting from the original copy of its image. As a result, boot from SAN can greatly reduce the time required for server recovery.
- High Availability: A typical data center is highly redundant in nature - redundant paths, redundant disks and redundant storage controllers. When operating system images are stored on disks in the SAN, it supports high availability and eliminates the potential for mechanical failure of a local disk.
- Rapid Redeployment: Businesses that experience temporary high production workloads can take advantage of SAN technologies to clone the boot image and distribute the image to multiple servers for rapid deployment. Such servers may only need to be in production for hours or days and can be readily removed when the production need has been met. Highly efficient deployment of boot images makes temporary server usage a cost effective endeavor.
- Centralized Image Management: When operating system images are stored on networked disks, all upgrades and fixes can be managed at a centralized location. Changes made to disks in a storage array are readily accessible by each server.

With Boot from SAN, the image resides on a SAN LUN and the server communicates with the SAN through a host bus adapter (HBA). The HBAs BIOS contain the instructions that enable the server to find the boot disk. All FC-capable Converged Network Adapter (CNA) cards supported on Cisco UCS B-series blade servers support Boot from SAN.

After power on self-test (POST), the server hardware component fetches the boot device that is designated as the boot device in the hardware BOIS settings. Once the hardware detects the boot device, it follows the regular boot process.

6.4.2 Configuring Boot from SAN Overview

There are three distinct phases during the configuration of Boot from SAN. The high level procedures are:

1. SAN zone configuration on the Nexus 5548UPs
2. Storage array host initiator configuration
3. Cisco UCS configuration of Boot from SAN policy in the service profile.

In each of the following sections, each high level phase will be discussed.

6.4.3 SAN Configuration on Cisco UCS Manager

The Cisco UCS Local Zoning feature requires that the UCS Fabric Interconnects be configured in FC Switching Mode rather than the default of FC End Host Mode. Once that task is completed, the properties of the VSAN used in the deployment must have the FC Zoning Setting set to Enabled.

These tasks are outlined in Section 6.2.1 Base UCS System Configuration above in step 15.

When enabled, the UCS Manager Service Profile Template creation wizard will provide the steps necessary to complete the Fibre Channel Zoning for the project.

These tasks are outlined in Section 6.2.1 Base UCS System Configuration above in step 16.

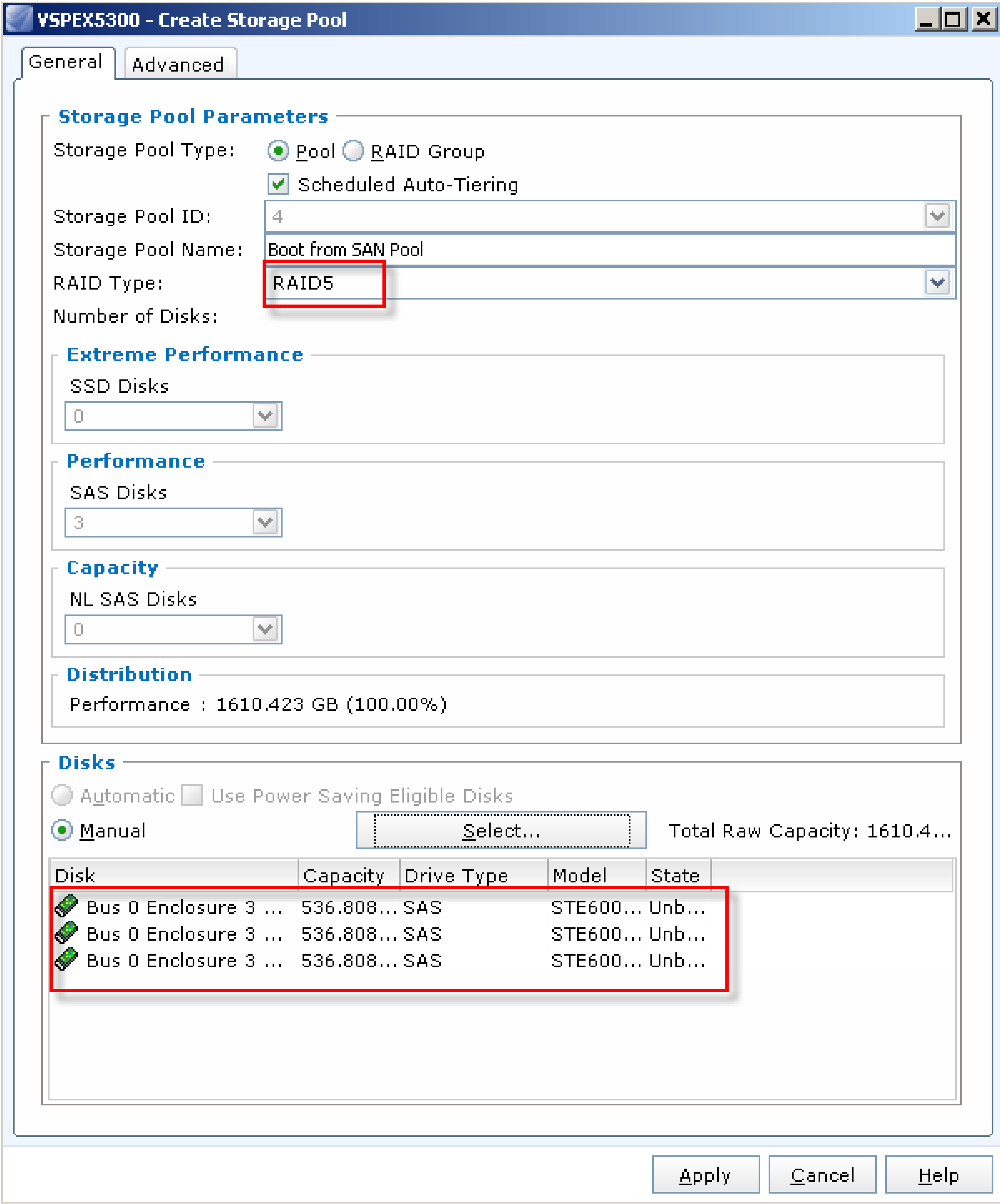
It is possible to perform FC zoning on the Fabric Interconnects from the command line. Using that method is not covered in this paper. Please refer to the Cisco UCS Manager CLI Command Reference, Release 2.1 that can be found at:

http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/cli/command/reference/2.1/b_command_reference_2.1_chapter_0100.html

6.4.4 Configuring Boot from SAN on EMC VNX

The steps required to configure boot from SAN LUNs on EMC VNX are as follows:

1. Create a storage pool from which LUNs will be provisioned. RAID type, drive number and type are specified in the dialogue box below. Three 600GB SAS drives are used in this example to create a RAID 5 pool. Uncheck “Schedule Auto-Tiering” to disable automatic tiering.



VSPEX5300 - Create Storage Pool

Storage Pool Parameters

Storage Pool Type: ● Pool ○ RAID Group

☑ Scheduled Auto-Tiering

Storage Pool ID: 4

Storage Pool Name: Boot from SAN Pool

RAID Type: RAID5

Number of Disks:

Extreme Performance

SSD Disks: 0

Performance

SAS Disks: 3

Capacity

NL SAS Disks: 0

Distribution

Performance : 1610.423 GB (100.00%)

Disks

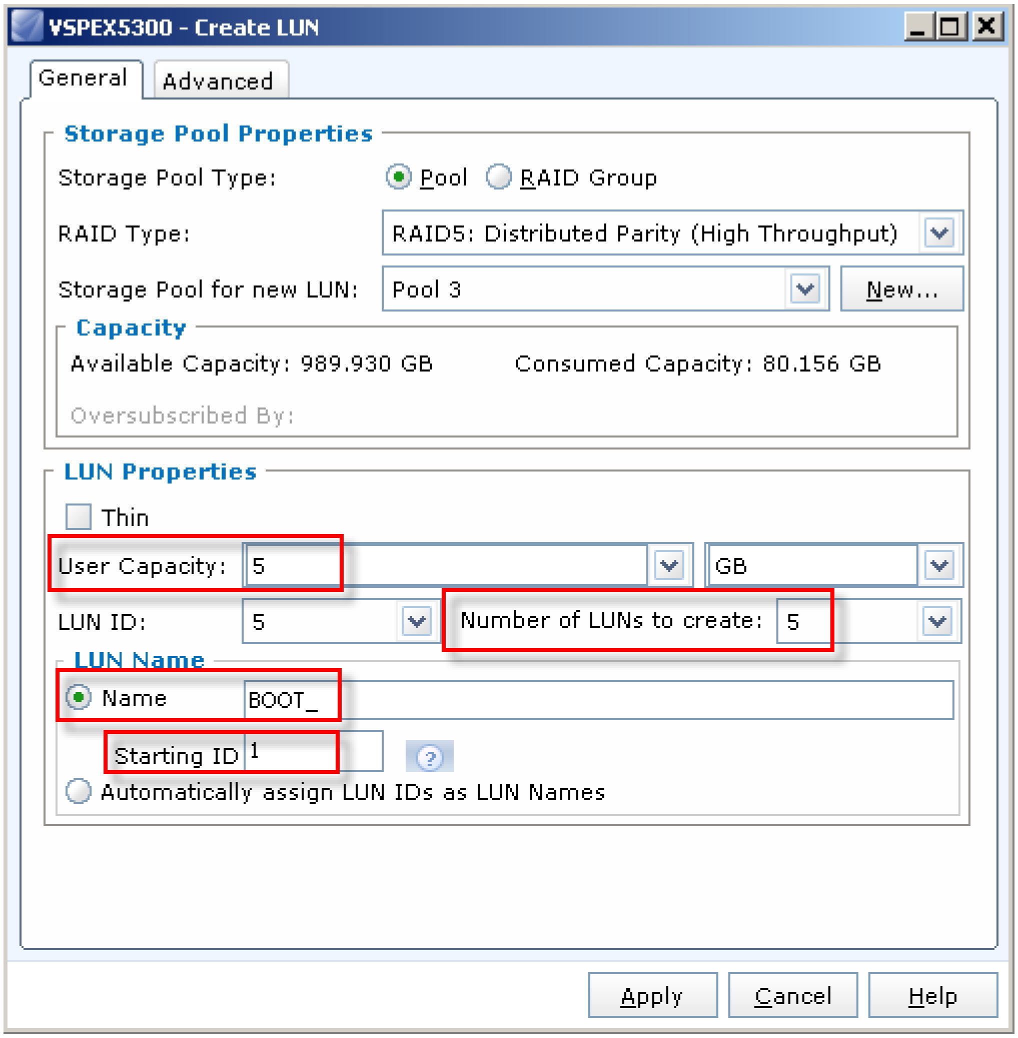
○ Automatic □ Use Power Saving Eligible Disks

● Manual

Total Raw Capacity: 1610.4...

Disk	Capacity	Drive Type	Model	State
Bus 0 Enclosure 3 ...	536.808...	SAS	STE600...	Unb...
Bus 0 Enclosure 3 ...	536.808...	SAS	STE600...	Unb...
Bus 0 Enclosure 3 ...	536.808...	SAS	STE600...	Unb...

2. Provision LUNs from the storage pool created in step 1. Each LUN is 12GB in size to store the ESXi hypervisor OS.



VSPEX5300 - Create LUN

Storage Pool Properties

Storage Pool Type: ● Pool ○ RAID Group

RAID Type: RAID5: Distributed Parity (High Throughput)

Storage Pool for new LUN: Pool 3

Capacity

Available Capacity: 989.930 GB Consumed Capacity: 80.156 GB

Oversubscribed By:

LUN Properties

□ Thin

User Capacity: 5 GB

LUN ID: 5 Number of LUNs to create: 5

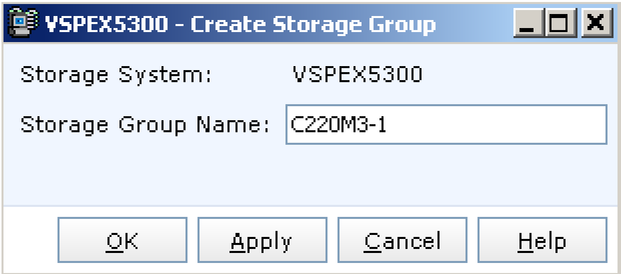
LUN Name

● Name BOOT_

Starting ID 1

○ Automatically assign LUN IDs as LUN Names

3. Create a storage group, the container used for host to LUN mapping, for each of the ESXi hosts.

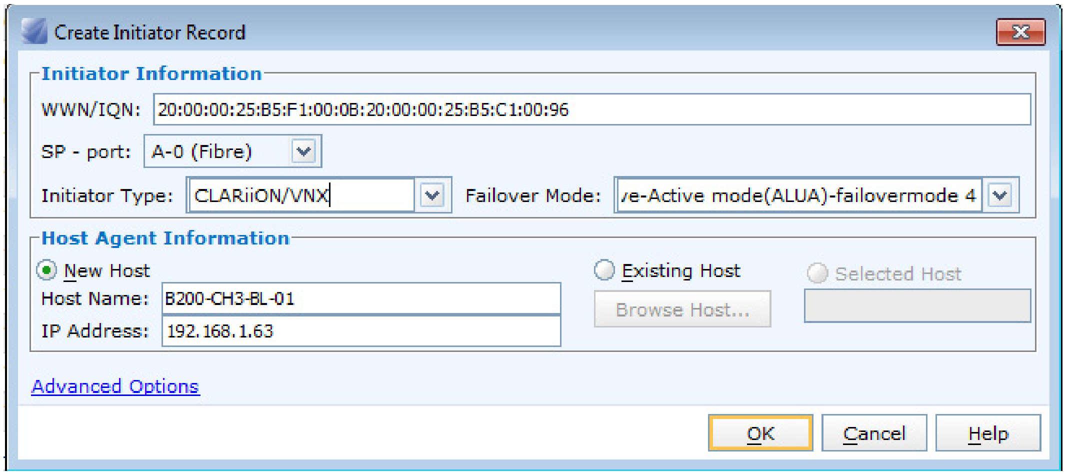


VSPEX5300 - Create Storage Group

Storage System: VSPEX5300

Storage Group Name: C220M3-1

4. Register host initiators with the storage array to associate a set of initiators with a given host. The registered host will be mapped to a specific boot LUN in the following step.



Create Initiator Record

Initiator Information

WWN/IQN: 20:00:00:25:B5:F1:00:0B:20:00:00:25:B5:C1:00:96

SP - port: A-0 (Fibre)

Initiator Type: CLARiiON/VNX

Failover Mode: /e-Active mode(ALUA)-failovermode 4

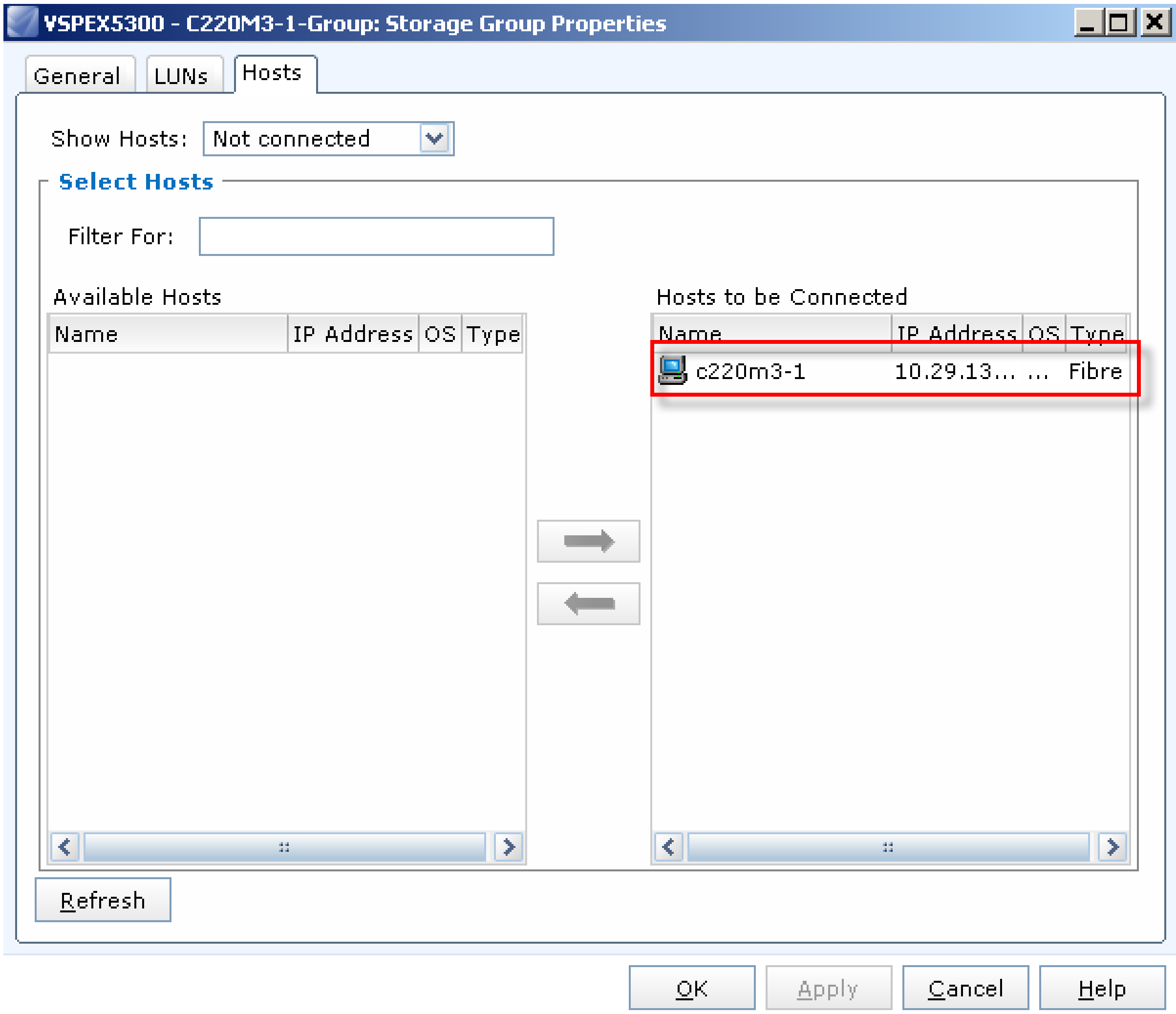
Host Agent Information

● New Host ○ Existing Host ○ Selected Host

Host Name: B200-CH3-BL-01

IP Address: 192.168.1.63

5. Assign each registered host to a separate storage group as shown below.



VSPEX5300 - C220M3-1-Group: Storage Group Properties

Show Hosts: Not connected

Select Hosts

Filter For:

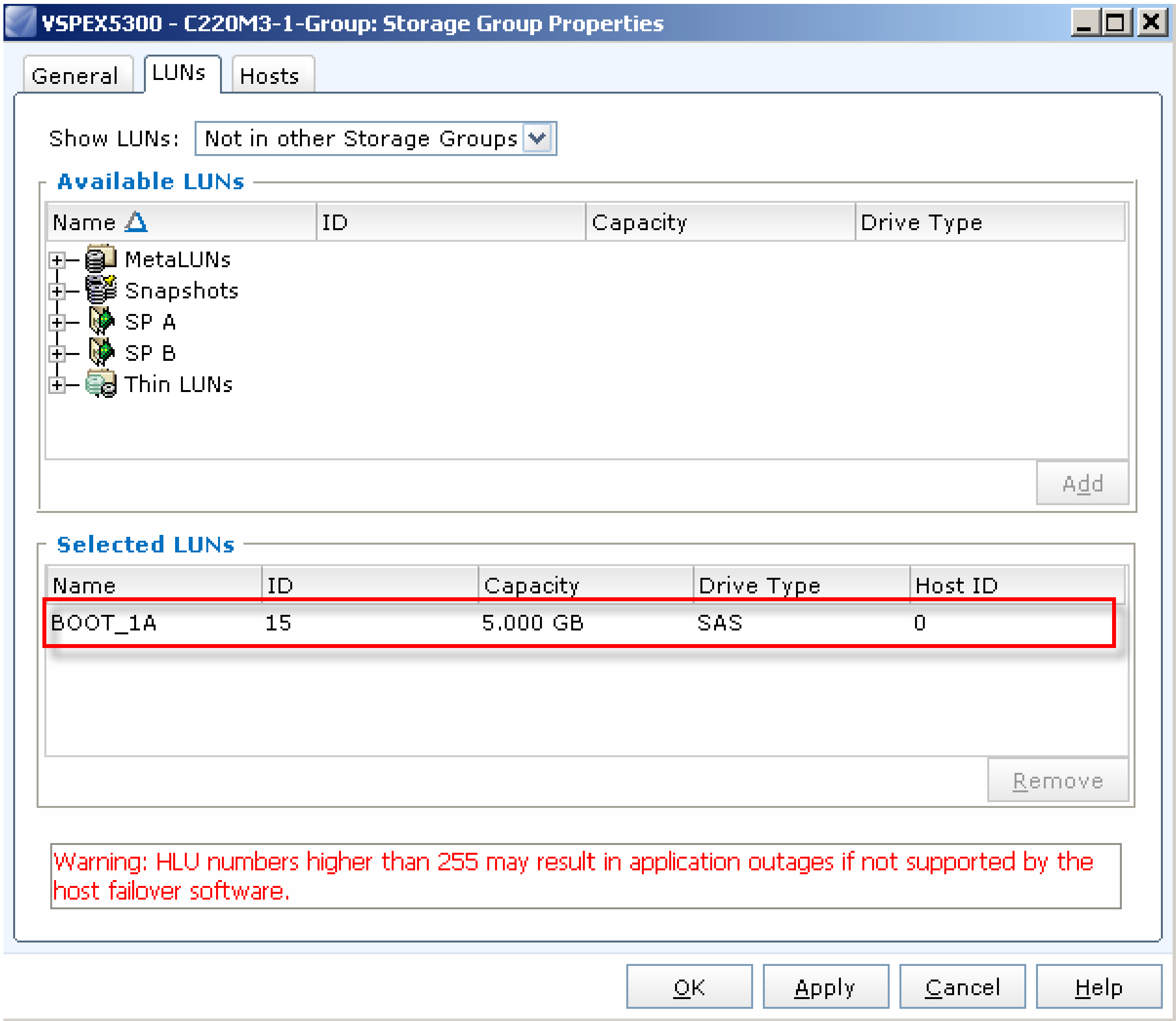
Available Hosts

Name	IP Address	OS	Type

Hosts to be Connected

Name	IP Address	OS	Type
c220m3-1	10.29.13...	...	Fibre

6. Assign a boot LUN to each of the storage groups. A host LUN ID is chosen to make visible to the host. It does not need to match the array LUN ID. All boot LUNs created for the testing are assigned host LUN ID 0.



Show LUNs: Not in other Storage Groups

Available LUNs

Name	ID	Capacity	Drive Type
MetaLUNs			
Snapshots			
SP A			
SP B			
Thin LUNs			

Selected LUNs

Name	ID	Capacity	Drive Type	Host ID
BOOT_1A	15	5.000 GB	SAS	0

Warning: HLU numbers higher than 255 may result in application outages if not supported by the host failover software.

When the Cisco UCS Blade Server boots up, its vHBAs will connect to the provisioned EMC Boot LUNs and the hypervisor operating system can be installed.

6.4.5 SAN Configuration on Cisco UCS Manager

The configuration of the Boot from SAN policy in UCS Manager is covered in Section 6.2.1 Base Cisco UCS System Configuration above in step 13.

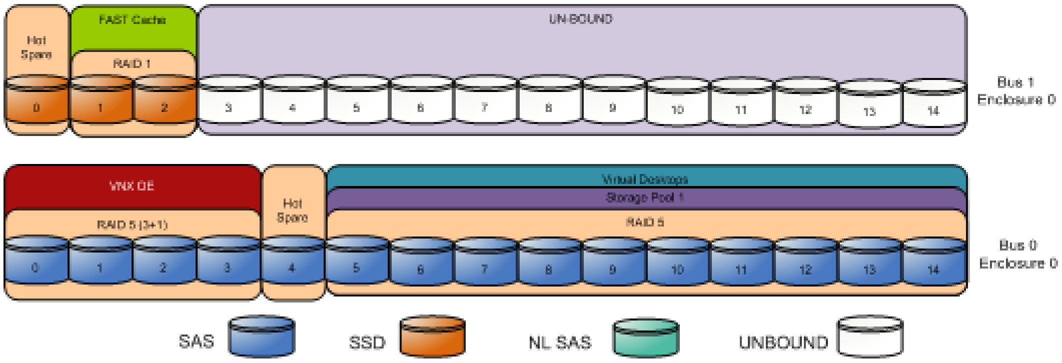
The policy created is incorporate in the Service Profile Template in Section 6.2.1 Base Cisco UCS System Configuration above in step 16o.

6.5 EMC VNX5300 Storage Configuration

The Managed FC Variant and Unmanaged NFS Variant have the same configuration to the pool level on the VNX5300. The configuration varies from there as described below.

6.5.1 Physical and Logical Storage Layout for Managed FC and Unmanaged NFS Variants

The figure below shows the physical storage layout of the disks in the reference architecture. This configuration accommodates up to 600 virtual desktops.



The above storage layout is used for the following configurations:

Managed Fibre Channel Variant

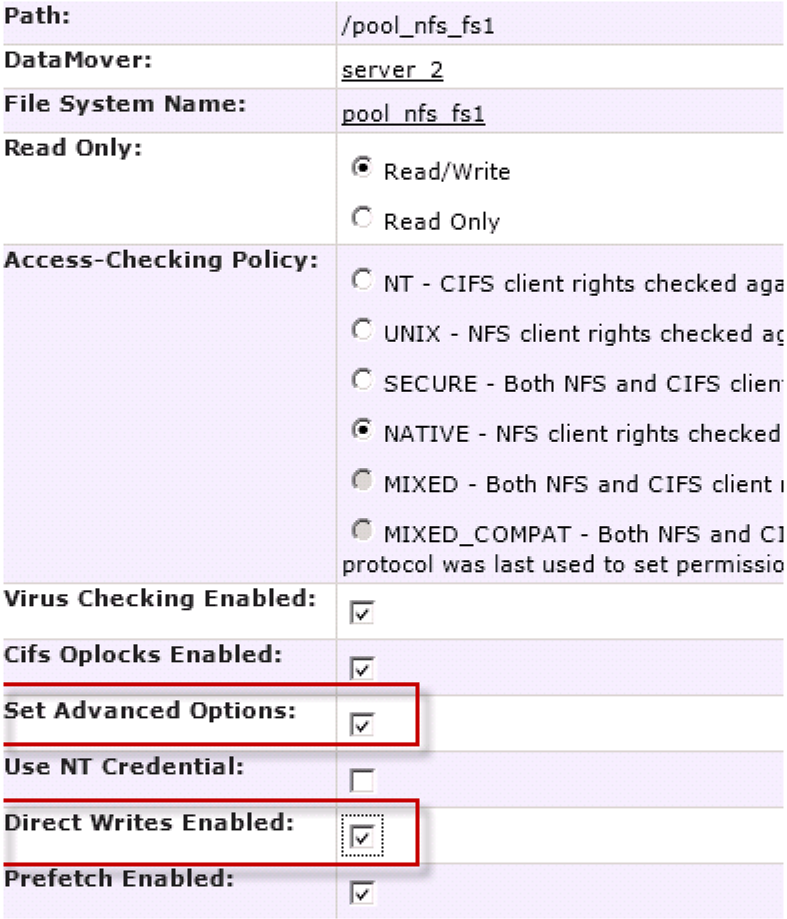
- Four SAS disks are used for the VNX OE.
- One SAS disk is a hot spare for SAS disks.
- One SSD Disk is hot spare for SSD drives.
- Two 100GB Flash drives are used for EMC VNX FAST Cache. See the “EMC FAST Cache in Practice” section below to follow the FAST Cache configuration best practices.
- 10 600GB SAS disks on a single RAID 5 storage pool with Fast Cache enabled for virtual desktop write cache drives.
- Four LUNs of 500GB each are carve out to the block pool to present to the ESXi servers as four VMFS datastores

Note The Managed Fibre Channel Variant was validated with 600 virtual desktops.

Unmanaged NFS Variant

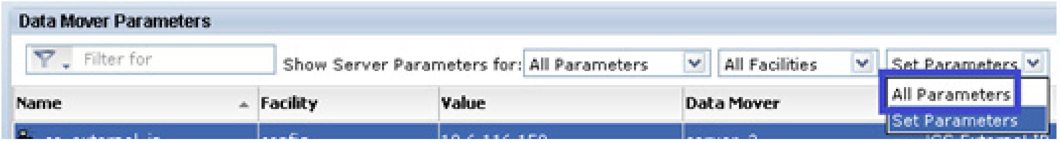
- Four SAS disks are used for the VNX OE.
- One SAS disk is a hot spare for SAS disks.
- One SSD Disk is hot spare for SSD drives.
- Two 100GB Flash drives are used for EMC VNX FAST Cache. See the “EMC FAST Cache in Practice” section below to follow the FAST Cache configuration best practices.
- 10 600GB SAS disks on a single RAID 5 storage pool with Fast Cache enabled for virtual desktop write cache drives.
- Ten LUNs of 200GB each are carve out to the NAS pool to present to the Data Movers as dvols that belong to a system defined NAS pool.
- Four file systems of 500 GB each are carved out of the NAS pool to present to the ESXi servers as four NFS datastores

Note To enable an NFS performance fix for VNX File that significantly reduces NFS write latency, the file systems must be mounted on the Data Mover using the **Direct Writes** mode as shown in Export the file systems using NFS, and give root access to ESXi servers.. The **Set Advanced Options** check box must be selected to enable the **Direct Writes** check box.



Path:	/pool_nfs_fs1
DataMover:	server_2
File System Name:	pool_nfs_fs1
Read Only:	● Read/Write ○ Read Only
Access-Checking Policy:	○ NT - CIFS client rights checked aga ○ UNIX - NFS client rights checked ag ○ SECURE - Both NFS and CIFS clien ● NATIVE - NFS client rights checked ○ MIXED - Both NFS and CIFS client r ○ MIXED_COMPAT - Both NFS and CI protocol was last used to set permissio
Virus Checking Enabled:	☑
Cifs Oplocks Enabled:	☑
Set Advanced Options:	☑
Use NT Credential:	□
Direct Writes Enabled:	☑
Prefetch Enabled:	☑

- Export the file systems using NFS, and give root access to ESXi servers.
- In Unisphere, click **Settings** > **Data Mover Parameters** to make changes to the Data Mover configuration. Click the drop down menu to the right of **Set Parameters** and change the setting to "All Parameters" as shown in the figure below. Scroll down to the **nthreads** parameter and click **Properties** to update the setting. The default number of threads dedicated to serve NFS requests is 384 per Data Mover on VNX. Since up to 600 desktop connections are required in this solution, it is recommended to increase the number of active NFS threads to a maximum of 1024 on each Data Mover.

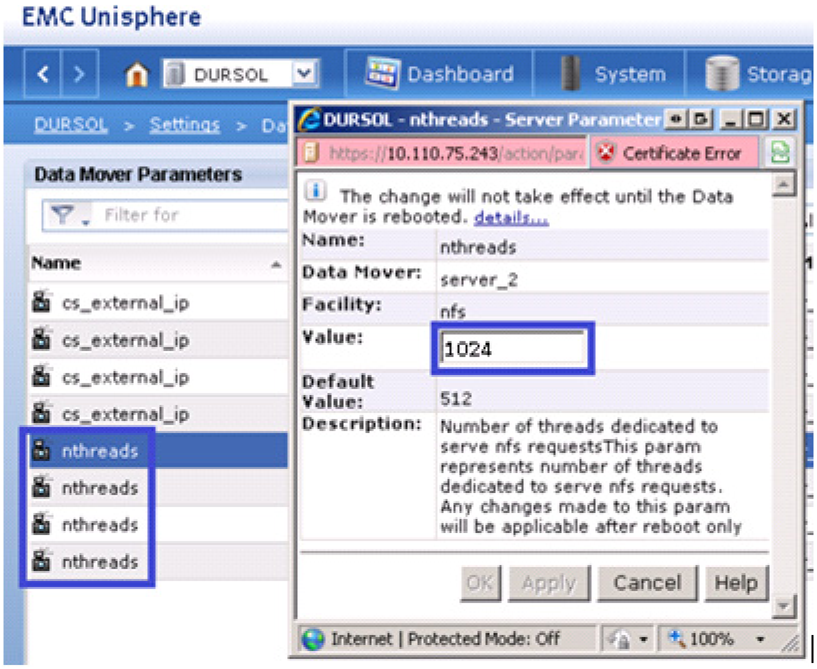


Data Mover Parameters

Filter for

Show Server Parameters for: All Parameters | All Facilities | Set Parameters

Name	Facility	Value	Data Mover



The change will not take effect until the Data Mover is rebooted. details...

Name: nthreads

Data Mover: server_2

Facility: nfs

Value: 1024

Default Value: 512

Description: Number of threads dedicated to serve nfs requestsThis param represents number of threads dedicated to serve nfs requests. Any changes made to this param will be applicable after reboot only

Note The Unmanaged NFS Variant was validated with 600 virtual desktops.

6.5.2 EMC Storage Configuration for VMware ESXi 5.0 Infrastructure Servers

If storage required for infrastructure virtual machines (that is, SQL server, domain controller, vCenter server, and/or XenDesktop controllers) does not exist in the production environment already and the optional user data disk pack has been purchased, configure a NFS file system or one or more FC LUNS on VNX to be used as a NFS datastore or VMFS datastore in which the infrastructure virtual machines reside.

In this study we used 5 600GB SAS drives for the Infrastructure Pool in a RAID 5 array to provision 2 500GB VMFS LUNS for our infrastructure virtual machines and files. Fast Cache was disabled on the Infrastructure Pool.

6.5.3 EMC FAST Cache in Practice

EMC FAST Cache uses Flash drives to add an extra layer of cache between the dynamic random access memory (DRAM) cache and rotating disk drives, thereby creating a faster medium for storing frequently accessed data. FAST Cache is an extendable Read/Write cache. It boosts application performance by ensuring that the most active data is served from high-performing Flash drives and can reside on this faster medium for as long as is needed.

FAST Cache tracks data activity at a granularity of 64KB and promotes hot data in to FAST Cache by copying from the hard disk drives (HDDs) to the Flash drives assigned to FAST Cache. Subsequent IO access to that data is handled by the Flash drives and is serviced at Flash drive response times-this ensures very low latency for the data. As data ages and becomes less active, it is flushed from FAST Cache to be replaced by more active data.

Only a small number of Flash drives are needed enabling FAST Cache to provide greater performance increases than implementing a large number of short-stroked HDDs. This results in cost savings in data center space, power, and cooling requirements that lowers overall TCO for the business.

FAST Cache is particularly suited to applications that randomly access storage with high frequency, such as Oracle and SQL OLTP databases. OLTP databases have inherent locality of reference with varied IO.

6.6Installing and Configuring ESXi 5.0 Update 1

In this study, we used Fibre Channel storage to boot the hosts from LUNs on the VNX7500 storage system. Prior to installing the operating system, storage groups are created, assigning specific boot LUNs to individual hosts. (See Section 6.4.4 Configuring Boot from SAN on EMC VNX for details.)

VMware ESXi 5.0 Update 1 can be installed in boot-from-SAN mode using standard hypervisor deployment techniques including:

1. Mounting a Cisco Customized ESXi 5.0 Update 1 ISO image from the KVM of the blade
2. Using automated deployment tools from third party sources (Optional)

6.6.1 Install VMware ESXi 5.0 Update 1

ESXi was installed from the Cisco UCS Manager (UCSM) KVM console using a ESXi 5.0 Update 1 iso image downloaded from the VMware site.

The IP address, hostname, and NTP server were configured using Direct Console ESXi Interface accessed from UCSM KVM console.

See the following VMware documentation for configuring network settings help.

(http://pubs.vmware.com/vsphere-50/topic/com.vmware.vsphere.install.doc_50/GUID-26F3BC88-DAD8-43E7-9EA0-160054954506.html).

6.6.2 Install and Configure vCenter

To manage hypervisors and virtual machines a dedicated vCenter server instance was installed on Windows 2008R2 virtual machine.

Vmware vCenter Server			
OS:	Windows 2008 R2	**Service Pack:**	
CPU:	1vCPUs	**RAM:**	4GB
Disk:	40GB	**Network:**	1x10Gbps

To support vCenter instance one Microsoft SQL Server 2008 R2 was created to host vCenter database.

If the Customer wants to utilize fault tolerance at the SQL Server level, refer to Microsoft documentation on configuring SQL Server clusters.

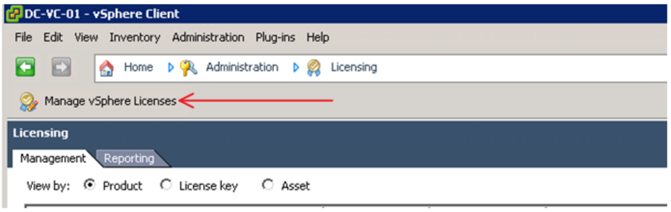
http://msdn.microsoft.com/en-us/library/ms189134(v=sql.105).aspx
http://msdn.microsoft.com/en-us/library/ms189134(v=sql.105).aspx

To install and configure vCenter, use the following steps:

1. Install the Microsoft® SQL Server® 2008 R2 Native Client for ODBC connections (http://www.microsoft.com/en-us/download/details.aspx?id=16978 look for Native Client for your architecture)
2. Create a System DSN (control panel, administrative tools, Data Sources ODBC) and connect to your vCenter-SQL server. Note: Ensure to use FQDN's for everything.
3. Create Active Directory user account and call it vcenter. (This user account will be used for XD to connect to vCenter, you will have to follow a Citrix specific procedure and assign specific permissions on vCenter for XD to connect to vCenter http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-vmware-rho.html).
4. Install vCenter server package, connect to the database.
5. Connect your vSphere client to vCenter and create a datacenter.
6. Create self-signed certificate (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021514).

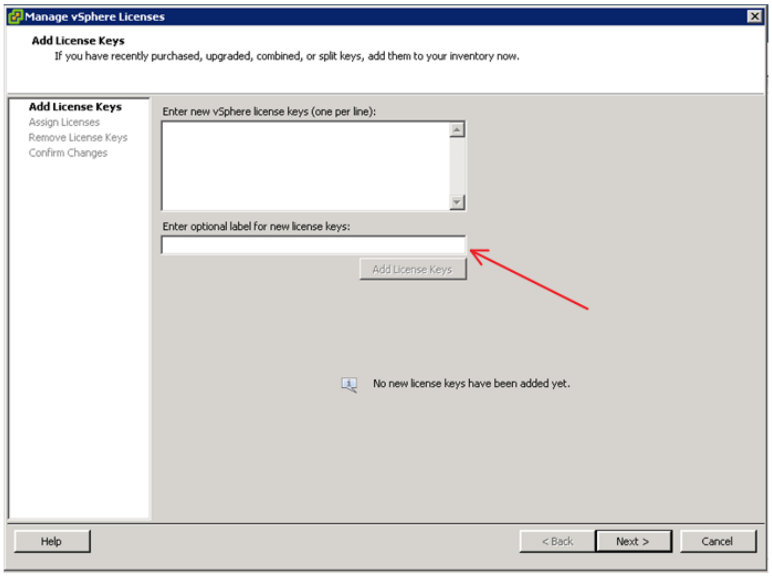
6.6.3 Install Licenses

1. Connect to vCenter using vSphere client.
2. Go to Home → Administration → Licensing
3. Click on Manage vSphere Licenses:



View by: ● Product ○ License key ○ Asset

4. Add License keys for vCenter and Hosts



Manage vSphere Licenses

Add License Keys

If you have recently purchased, upgraded, combined, or split keys, add them to your inventory now.

Enter new vSphere license keys (one per line):

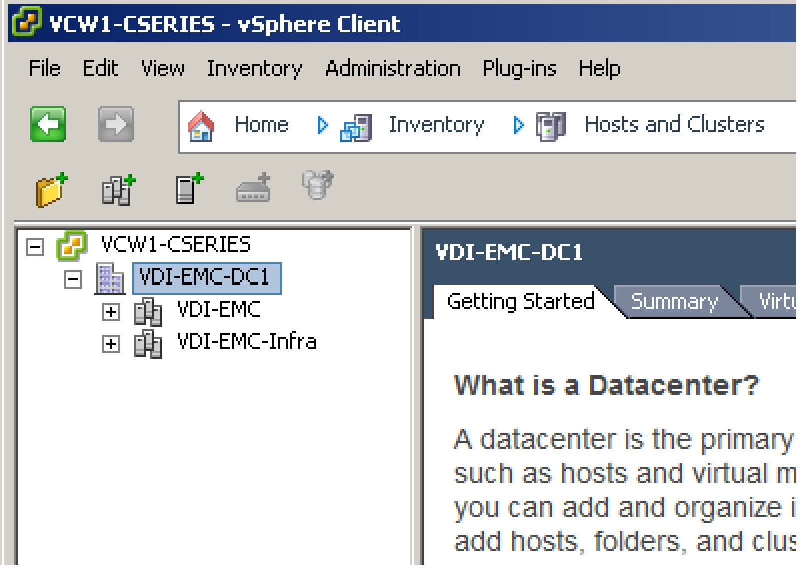
Enter optional label for new license keys:

No new license keys have been added yet.

6.6.4 ESXi 5.0 Update 1 Cluster Configuration

To accommodate maximum recommendations for ESXi 5 clustering, we created two ESXi 5 clusters described below:

- VDI-EMC
- VDI-EMC-Infra



VCW1-CSERIES - vSphere Client

What is a Datacenter?

A datacenter is the primary
such as hosts and virtual m
you can add and organize i
add hosts, folders, and clus

6.6.4.1 VDI-EMC- Infrastructure Cluster

The VDI-EMC-Infra cluster was used to host all of the virtualized servers within the VDA Infrastructure, including Active Directory servers providing authentication, DNS, DHCP and group policy services, a MS SQL 2008 R2 server for vCenter and XenDesktop databases, a pair of XenDesktop 5.6 FP1 servers, a file server for MS Roaming Profiles, a virtual file server for Login VSI files, and twenty Server 2008 R2 SP1 virtual machines as Login VSI Launchers.

Two physical UCS C220 M3 hosts were used in this cluster.

Standard ESXi vSwitches were used and configure as follows:

Managed FC Variant (All 10 Gb)
* Default vmkernel vSwitch for VMware Management
* Vmkernel vSwitch for VMotion
* Standard vSwitch for VDI traffic

Unmanaged NFS Variant
* Default vmkernel vSwitch for VMware Management and VDI traffic (1 Gb)
* Vmkernel vSwitch for vMotion (10 Gb)
* Vmkernel vSwitch for NFS storage (10 Gb)

It is not necessary to create an Infrastructure Cluster. If the existing Customer ESXi deployment has capacity, the required virtual machines can be added there.

Note Separate LUNS or NFS file systems were created for the Infrastructure Cluster hosts

6.7.4.2 Virtual Desktop Clusters

A single vSohere cluster was used to host 600 virtual desktops:

- Infra

The cluster was configured with a VMware ESXi 5 standard vSwitch providing the required network connectivity.

6.6.4.2 VDI-EMC Virtual Desktop Cluster

The **VDI-EMC** desktop cluster was used to host 600 of the Windows 7 SP1 32-bit virtual desktops.

Five physical Cisco UCS C220 M3 hosts were used in this cluster.

Standard ESXi vSwitches were used and configure as follows:

Managed FC Variant (All 10 Gb)
* Default vmkernel vSwitch for VMware Management
* Vmkernel vSwitch for VMotion
* Standard vSwitch for VDI traffic

Unmanaged NFS Variant
* Default vmkernel vSwitch for VMware Management and VDI traffic (1 Gb)
* Vmkernel vSwitch for vMotion (10 Gb)
* Vmkernel vSwitch for NFS storage (10 Gb)

We recommend creating a separate cluster for VDI workloads. It will provide a management container that will allow growth for the VDI use.

6.7 Installing and Configuring Citrix XenDesktop 5.6

Two XenDesktop 5.6 Delivery Controllers were virtualized on VMware ESXi 5.0 hosted on Cisco C220 M3 infrastructure blades. (Alternatively, they could be installed on Customer's existing ESXi 5.0 U1 hosts.)

Beginning with XenDesktop 5, Citrix replaced the proprietary IMA protocol encrypted data store in favor of Microsoft SQL Server databases. Concurrently the concept of XenDesktop Farms (used in XenDesktop 4 and earlier) was eliminated in favor of the concept of Sites.

From a management standpoint, Citrix introduced two new management consoles beginning with XenDesktop 5.

- Desktop Studio
- Desktop Director

The Desktop Studio is the main administration console where hosts, machine catalogs, desktop groups and applications are created and managed. The Desktop Studio is where HDX policy is configured and applied to the site. The Desktop Studio is a Microsoft Management Console snap in and fully supports PowerShell.

6.7.1 Pre-requisites

The following is a list of pre-requisites that are required with installing XenDesktop 5.6. They are as follows:

- One of the following operating systems:
  - Windows Server 2008, Standard or Enterprise Edition (32- or 64-bit), with Service Pack 2
  - Windows Server 2008 R2, Standard or Enterprise Edition (64-bit only)

  Note that you can mix operating systems within a site.
- Microsoft .NET Framework 3.5 with Service Pack 1.
- If you do not have this on your server, it is installed automatically for you. The XenDesktop installation media also contain this installer in the Support\DotNet35SP1 folder.
- Internet Information Services (IIS) and ASP.NET 2.0. IIS is required only if you are installing the Web Interface or Desktop Director:
  - For Windows Server 2008, IIS Version 7.0
  - For Windows Server 2008 R2, IIS Version 7.5

  If you do not have these on your server, you may be prompted for the Windows Server installation media, and they are installed for you.
- Visual J# 2.0 Redistributable Package, Second Edition.
- This is required only if the Web Interface is installed on the server. If you do not have this on your server, it is installed automatically for you. The XenDesktop installation media also contain this installer in the Support\JSharp20SE folder.
- Visual C++ 2008 with Service Pack 1 Redistributable Package.
- If you do not have this on your server, it is installed automatically for you. The XenDesktop installation media also contain this installer in the Support\vcredist\2008_SP1 folder.
- Windows PowerShell version 2.0.

- If you are using Windows Server 2008 (not Windows Server 2008 R2), Windows Management Framework is installed automatically if it is not already present on the server; it includes Windows PowerShell 2.0.

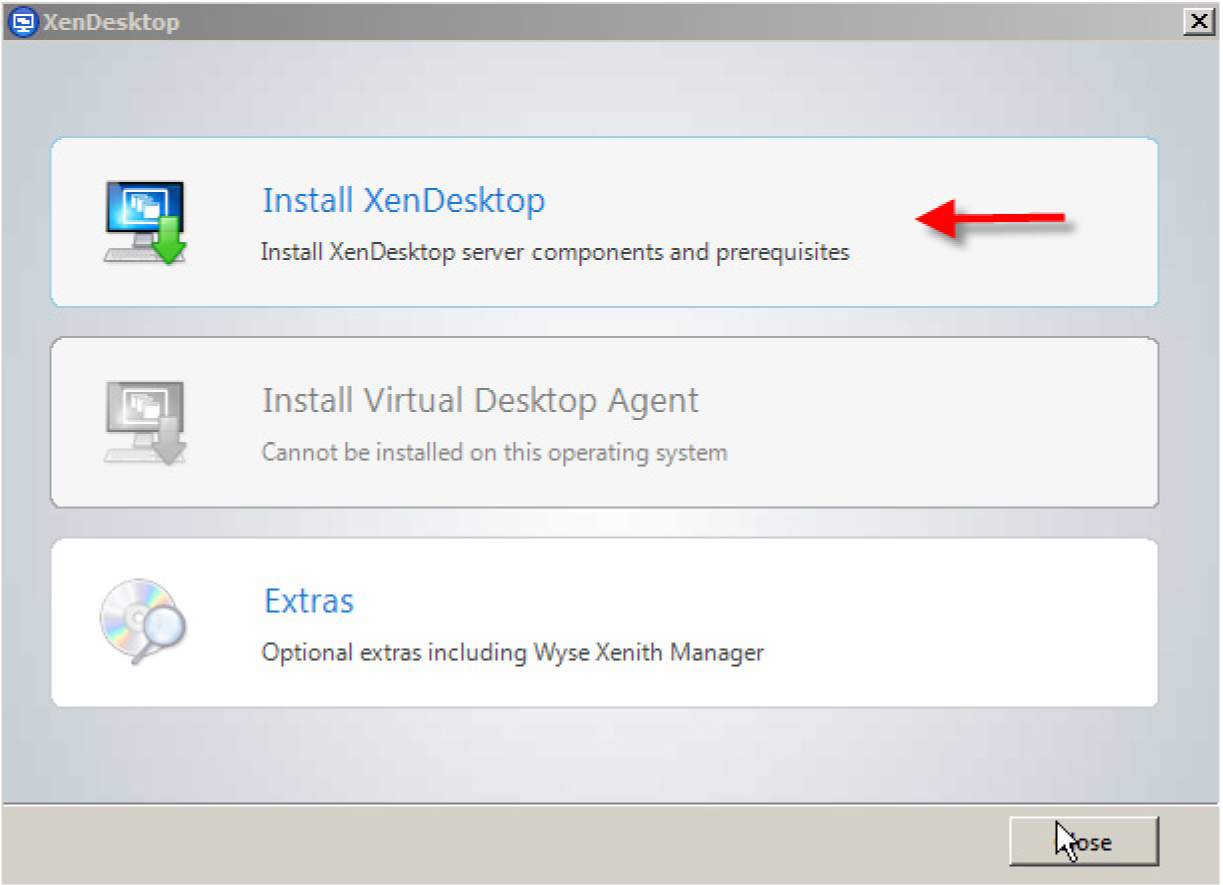
Note Windows Management Framework must be downloaded, so either ensure an Internet connection is available or pre-install Windows Management Framework.

- One of the following browsers if you are running the License Administration Console on the controller:
  - Internet Explorer 8 or 9
  - Firefox 3 to 8.*x*
  - Google Chrome
- Disk space requirements:
  - 100 MB for the Controller and SDKs
  - 50 MB for Desktop Studio
  - 50 MB for Desktop Director
  - 40 MB for Citrix Licensing
  - 100 MB for the Web Interface (and client software included in the installation)

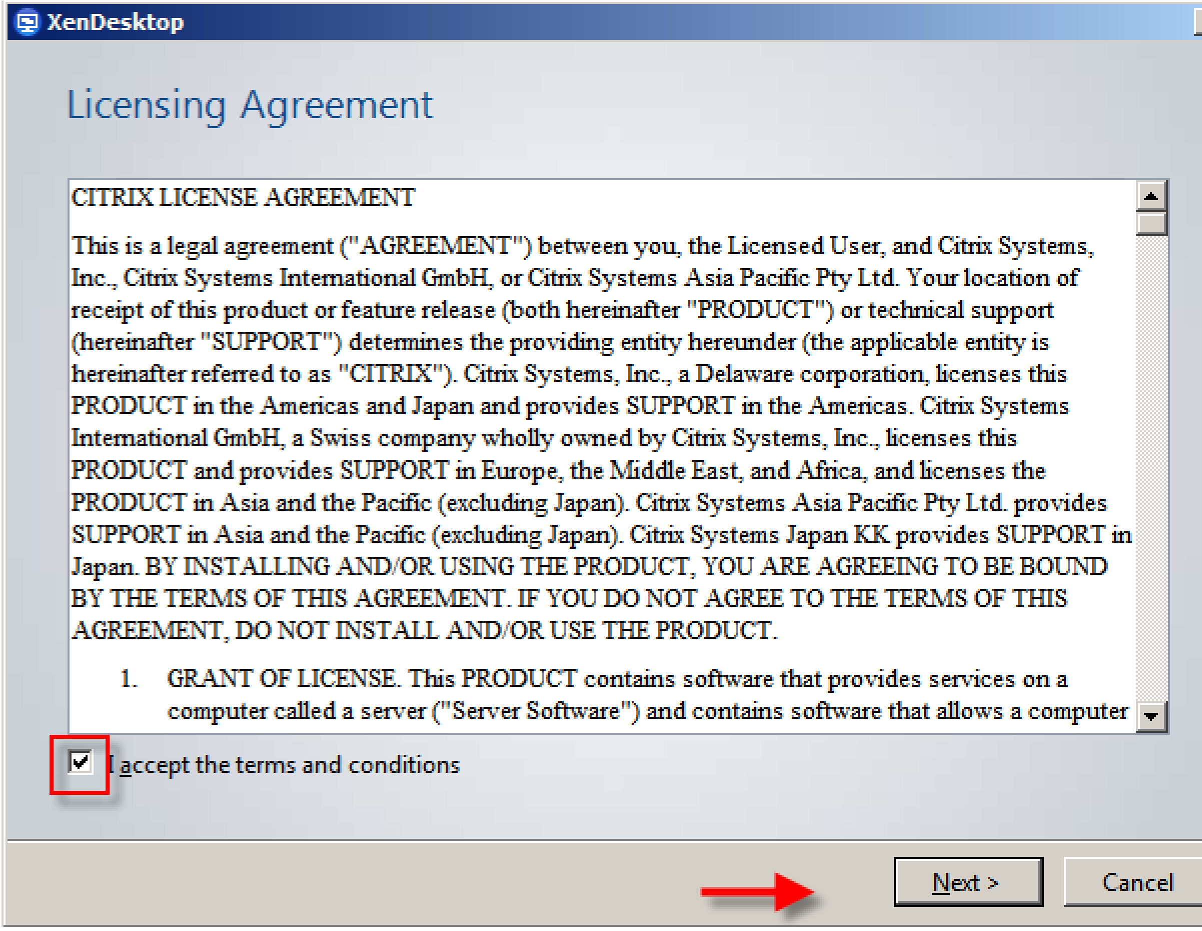
6.7.2 Install Citrix XenDesktop, Web Interface, Citrix XenDesktop Studio, and Optional Components

The steps identified below show the process used when installing XenDesktop, XenDesktop Studio and optional components

1. Start the XenDesktop installation wizard
2. Click on Install XenDesktop


XenDesktop
Install XenDesktop
Install XenDesktop server components and prerequisites
Install Virtual Desktop Agent
Cannot be installed on this operating system
Extras
Optional extras including Wyse Xenith Manager
Close

3. Accept the EULA and click Next



Licensing Agreement

CITRIX LICENSE AGREEMENT

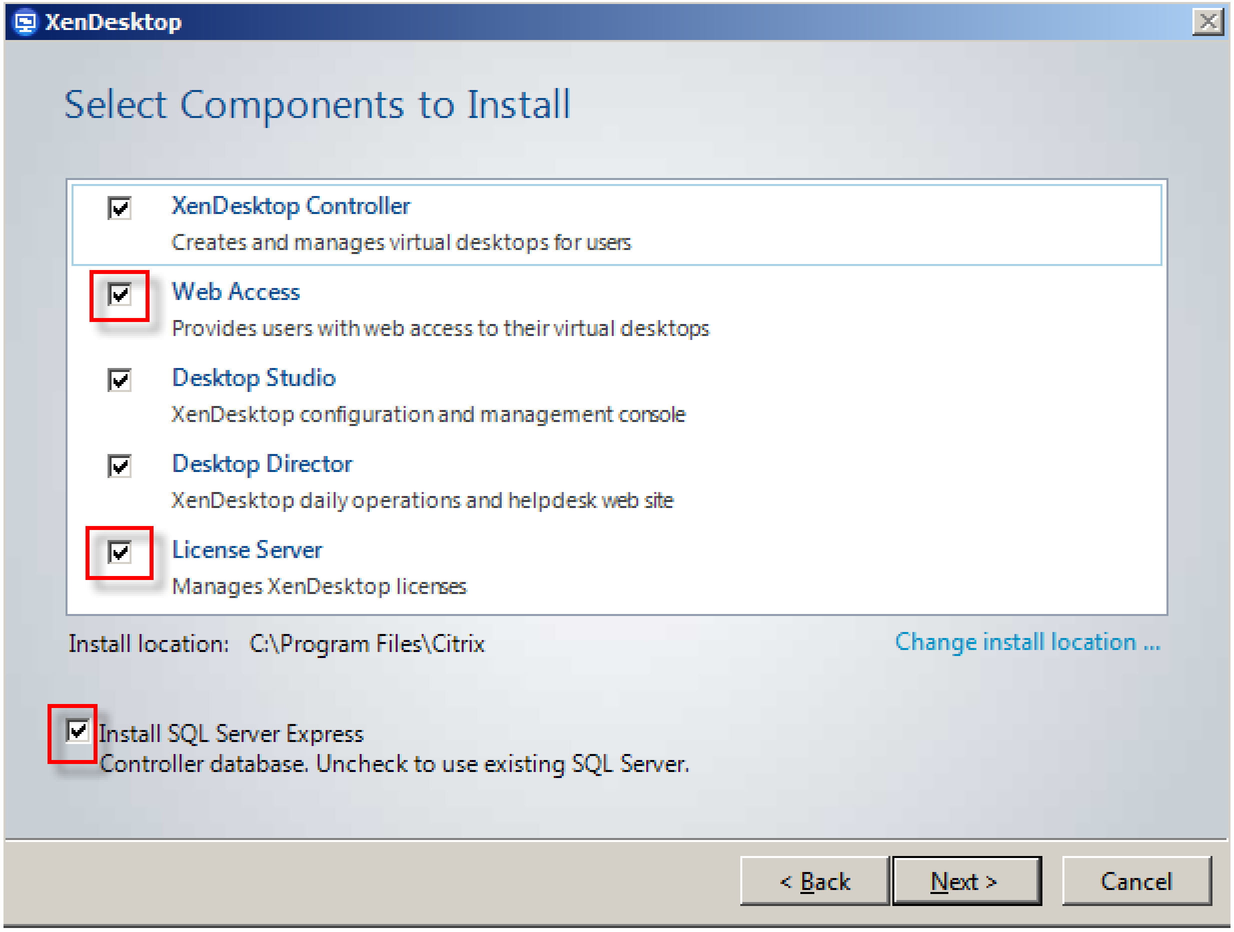
This is a legal agreement ("AGREEMENT") between you, the Licensed User, and Citrix Systems, Inc., Citrix Systems International GmbH, or Citrix Systems Asia Pacific Pty Ltd. Your location of receipt of this product or feature release (both hereinafter "PRODUCT") or technical support (hereinafter "SUPPORT") determines the providing entity hereunder (the applicable entity is hereinafter referred to as "CITRIX"). Citrix Systems, Inc., a Delaware corporation, licenses this PRODUCT in the Americas and Japan and provides SUPPORT in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., licenses this PRODUCT and provides SUPPORT in Europe, the Middle East, and Africa, and licenses the PRODUCT in Asia and the Pacific (excluding Japan). Citrix Systems Asia Pacific Pty Ltd. provides SUPPORT in Asia and the Pacific (excluding Japan). Citrix Systems Japan KK provides SUPPORT in Japan. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT.

1. GRANT OF LICENSE. This PRODUCT contains software that provides services on a computer called a server ("Server Software") and contains software that allows a computer

☑ I accept the terms and conditions

4. Select Components to install
5. Verify that XenDesktop Controller, Web Access, Desktop Studio, Desktop Director and License Server are selected.
6. If you have an existing Web Interface Server, Citrix License Server, or Microsoft SQL Server, uncheck the appropriate boxes, then, click Next. For this study, we unchecked the Install SQL Server Express checkbox.

Note Web Interface and Desktop Director was installed on only the first XenDesktop Controller.



XenDesktop

Select Components to Install

☑ XenDesktop Controller
Creates and manages virtual desktops for users

☑ Web Access
Provides users with web access to their virtual desktops

☑ Desktop Studio
XenDesktop configuration and management console

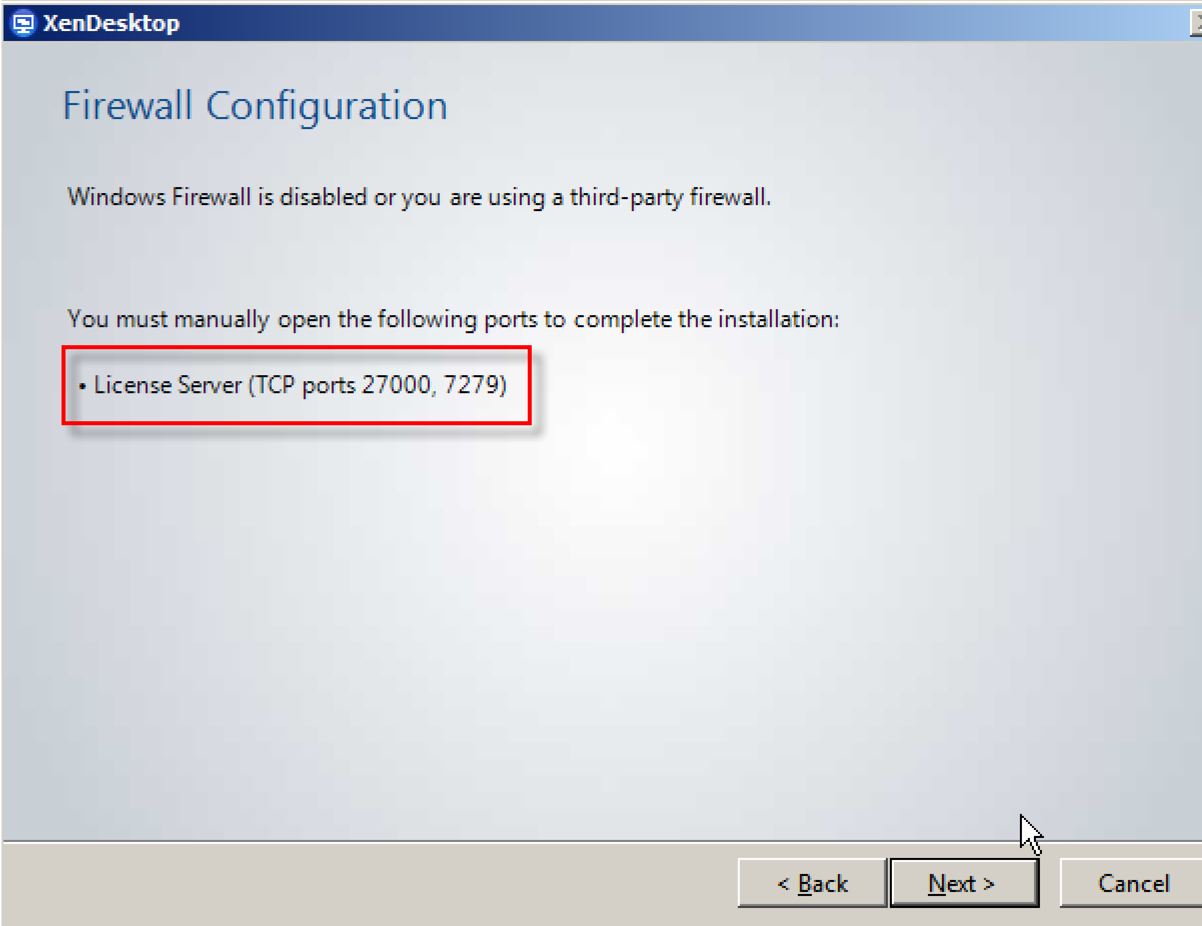
☑ Desktop Director
XenDesktop daily operations and helpdesk web site

☑ License Server
Manages XenDesktop licenses

Install location: C:\Program Files\Citrix

☑ Install SQL Server Express
Controller database. Uncheck to use existing SQL Server.

7. Click “**Next**”
8. If you are installing the License Server, note the firewall ports that need to be allowed, then click Next



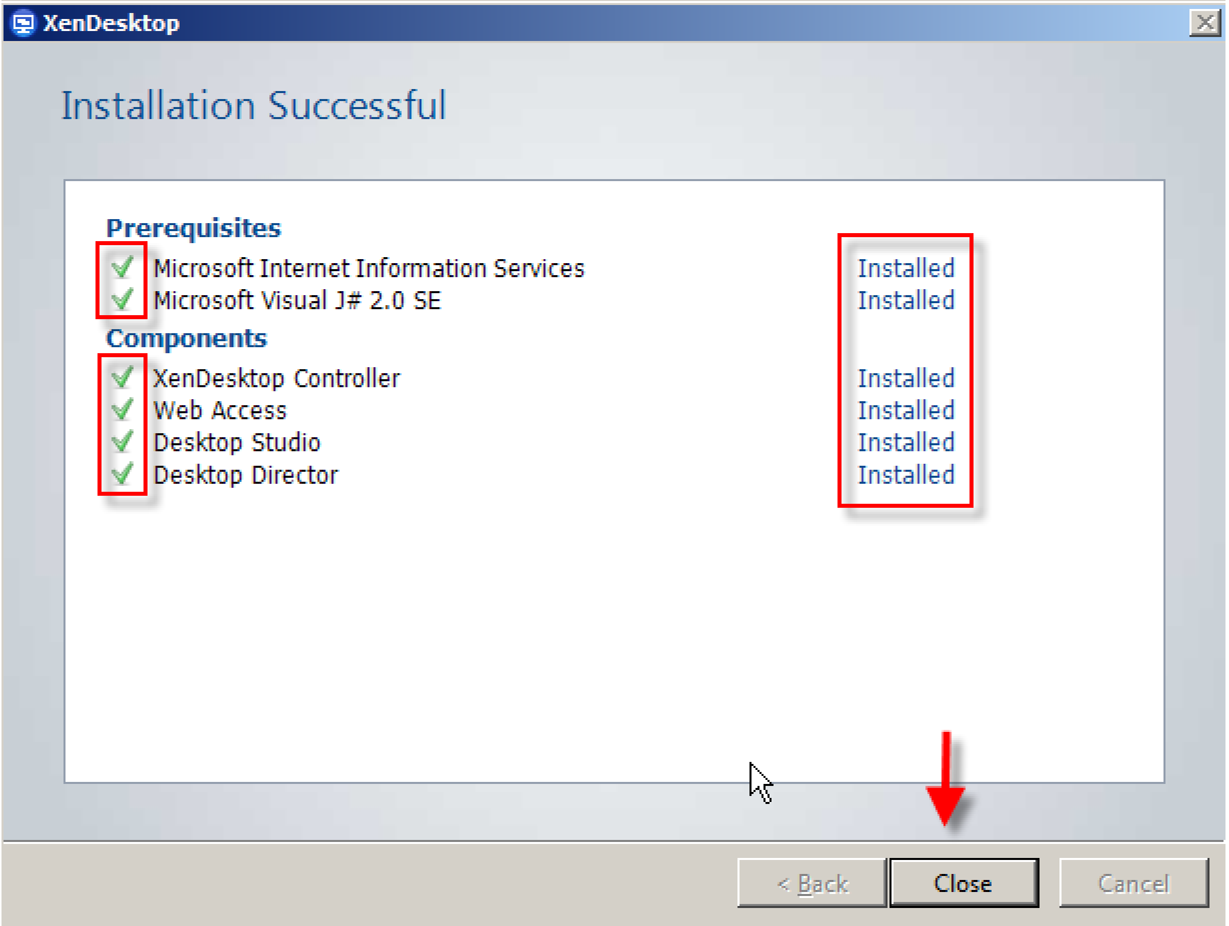
Firewall Configuration

Windows Firewall is disabled or you are using a third-party firewall.

You must manually open the following ports to complete the installation:

- License Server (TCP ports 27000, 7279)

9. Click “Install” in the Summary page to continue installation.
10. Click “OK” on the Installation Successful window to finalize your installation.



Installation Successful

Prerequisites

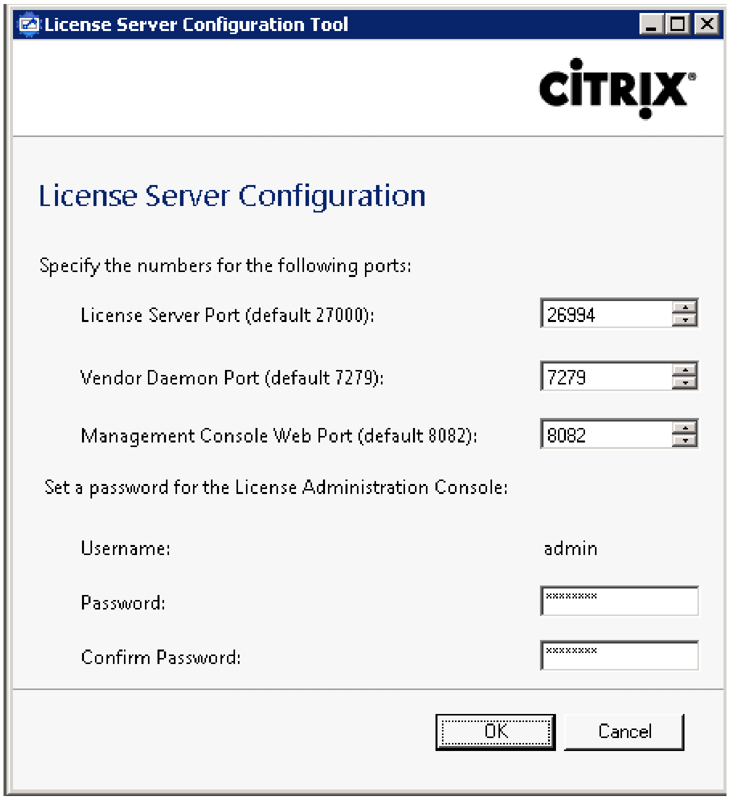
✓	Microsoft Internet Information Services	Installed
✓	Microsoft Visual J# 2.0 SE	Installed

Components

✓	XenDesktop Controller	Installed
✓	Web Access	Installed
✓	Desktop Studio	Installed
✓	Desktop Director	Installed

6.7.3 Configuring the License Server

1. Open the License Server Configuration Tool
2. Accept the Default ports and provide the password for the Admin account



License Server Configuration

Specify the numbers for the following ports:

License Server Port (default 27000): 26994

Vendor Daemon Port (default 7279): 7279

Management Console Web Port (default 8082): 8082

Set a password for the License Administration Console:

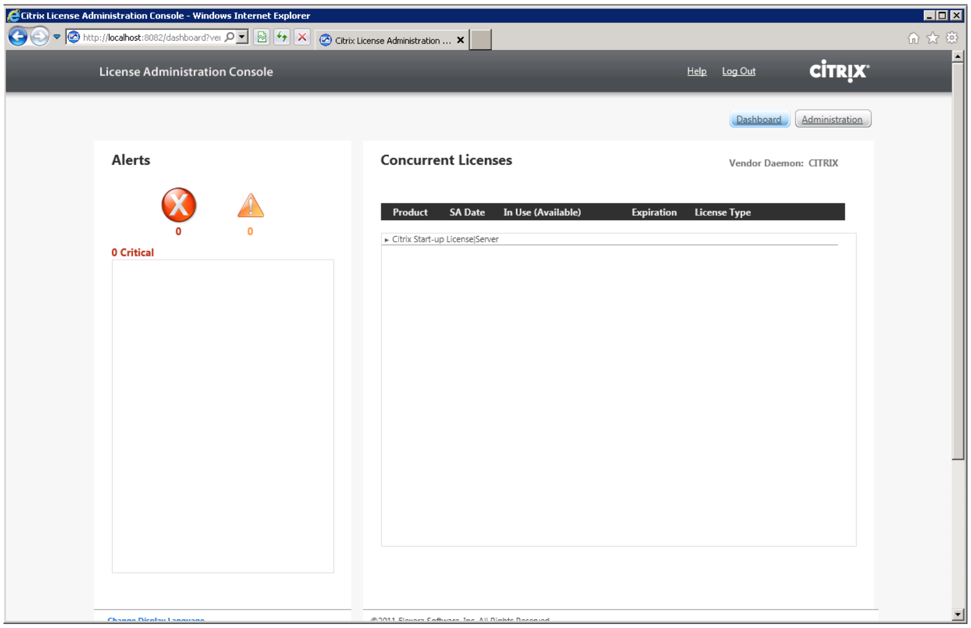
Username: admin

Password: ********

Confirm Password: ********

3. Click OK

4. Go to Start | All Programs | Citrix | Management Consoles and click on License Administration Console



Citrix License Administration Console - Windows Internet Explorer
http://localhost:8082/dashboard?vei
Citrix License Administration ...
License Administration Console
Help
Log Out
CiTRIX
Dashboard
Administration
Alerts
0
0
0 Critical

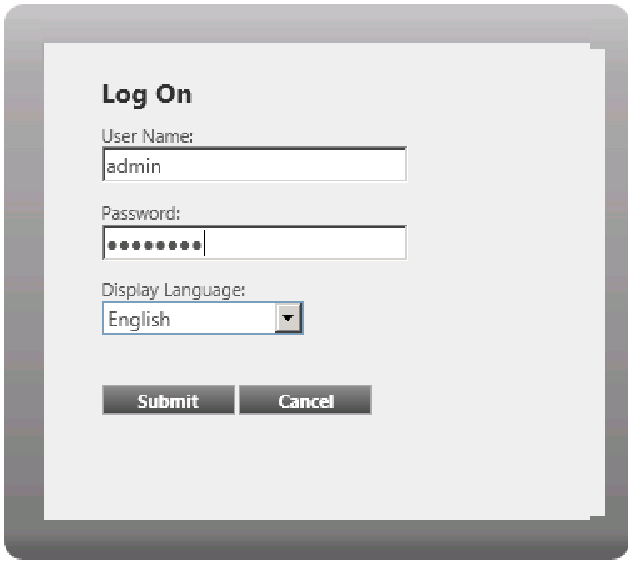
Concurrent Licenses

Vendor Daemon: CITRIX

Product	SA Date	In Use (Available)	Expiration	License Type
▸ Citrix Start-up License|Server				

5. Click on the Administration button

6. Enter the Admin credentials



Log On

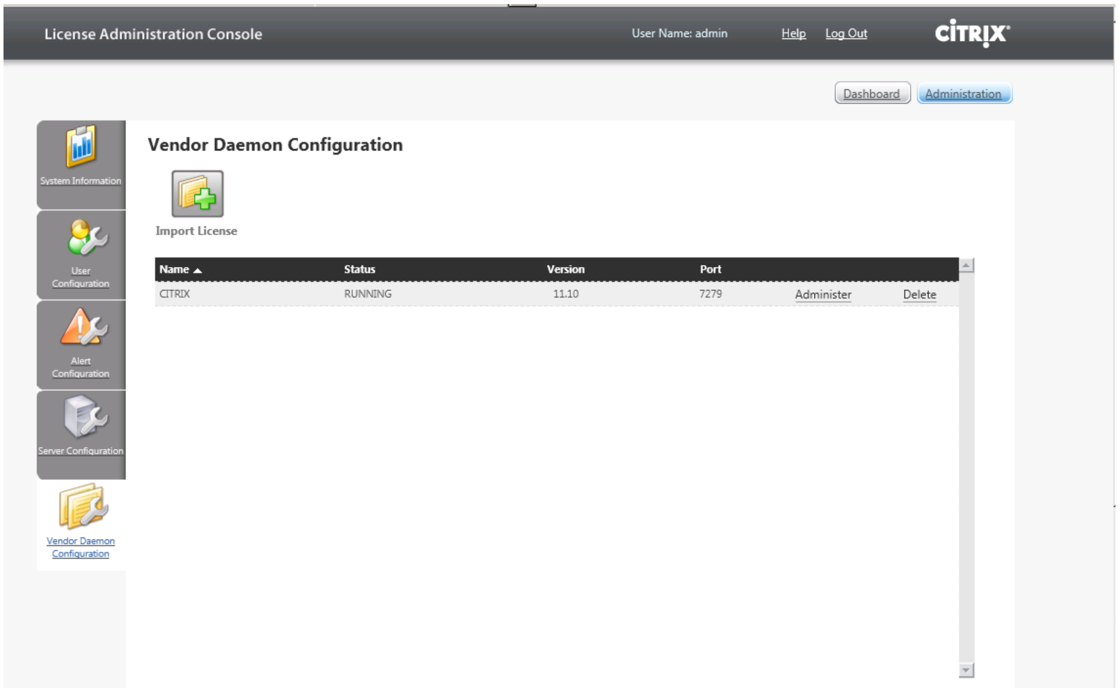
User Name: admin

Password: ••••••••

Display Language: English

7. Click Submit

8. Click on the Vendor Daemon Configuration tab on the left part of the screen

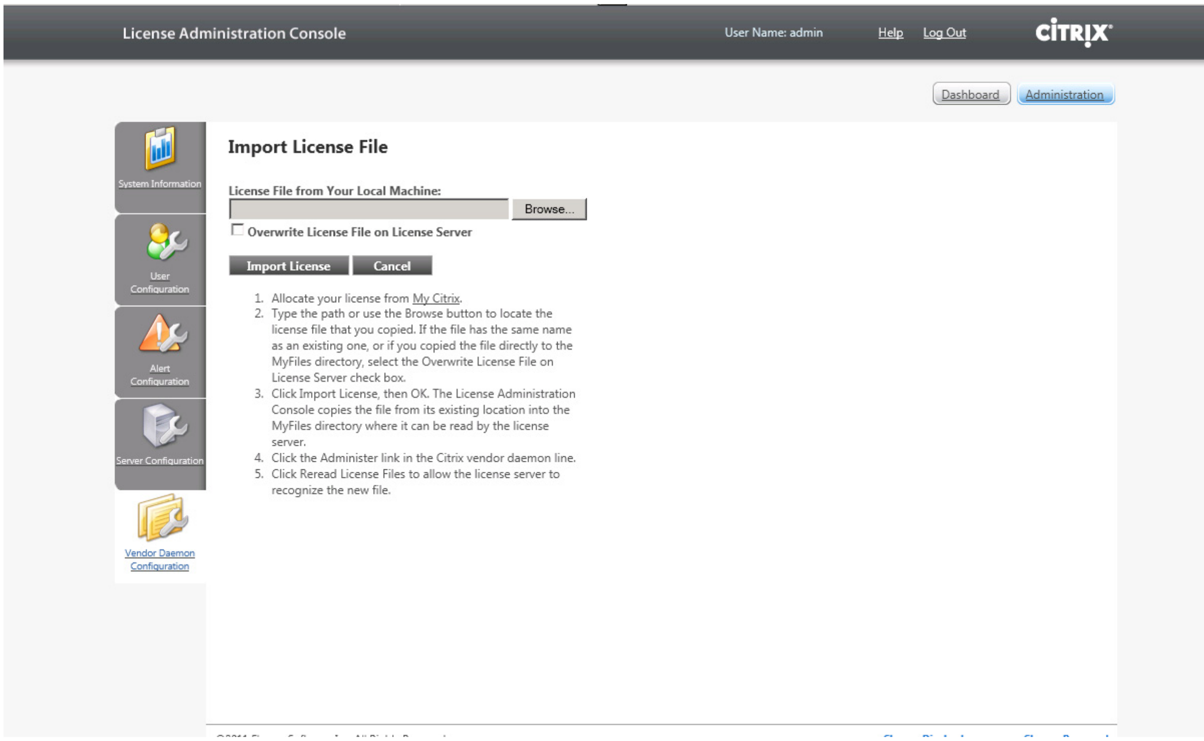


Vendor Daemon Configuration

Name ▲	Status	Version	Port		
CITRIX	RUNNING	11.10	7279	Administer	Delete

9. Click on Import License

10. Click Browse to locate the license file you are applying to the server



Import License File

License File from Your Local Machine:

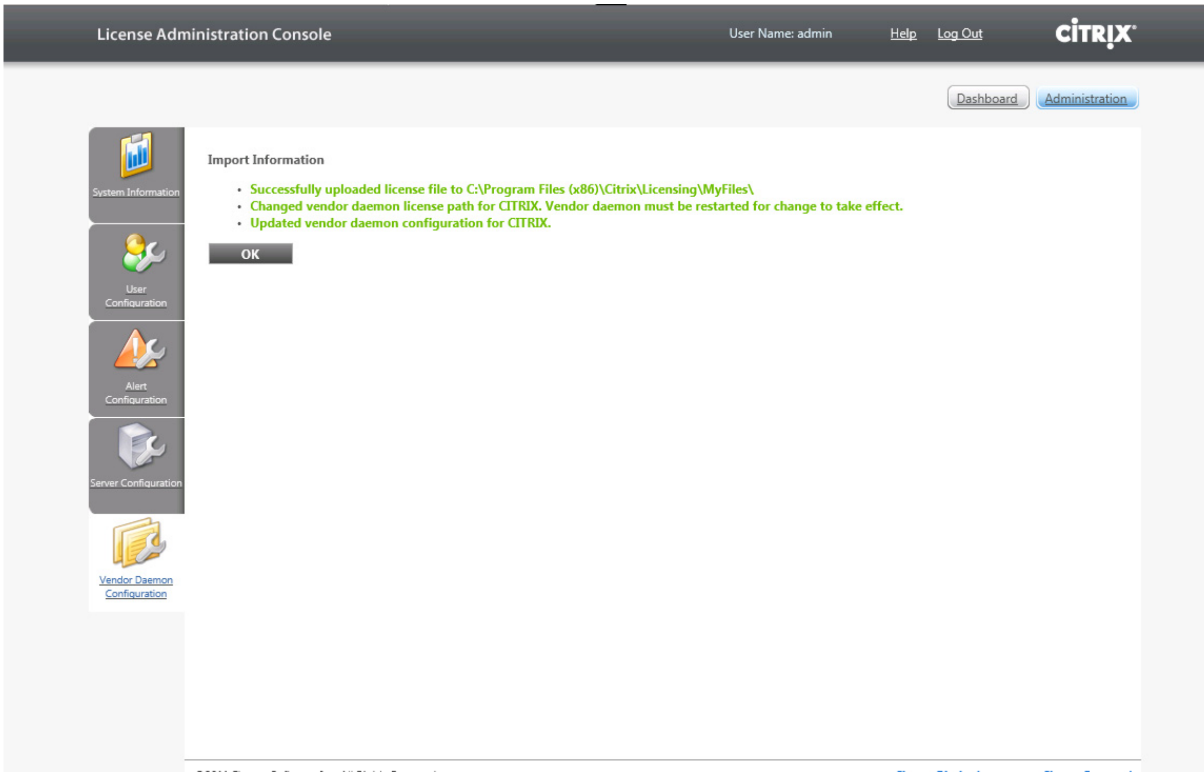
□ Overwrite License File on License Server

1. Allocate your license from My Citrix.
2. Type the path or use the Browse button to locate the license file that you copied. If the file has the same name as an existing one, or if you copied the file directly to the MyFiles directory, select the Overwrite License File on License Server check box.
3. Click Import License, then OK. The License Administration Console copies the file from its existing location into the MyFiles directory where it can be read by the license server.
4. Click the Administer link in the Citrix vendor daemon line.
5. Click Reread License Files to allow the license server to recognize the new file.

11. Select the file and Click Open

12. Click on Import License

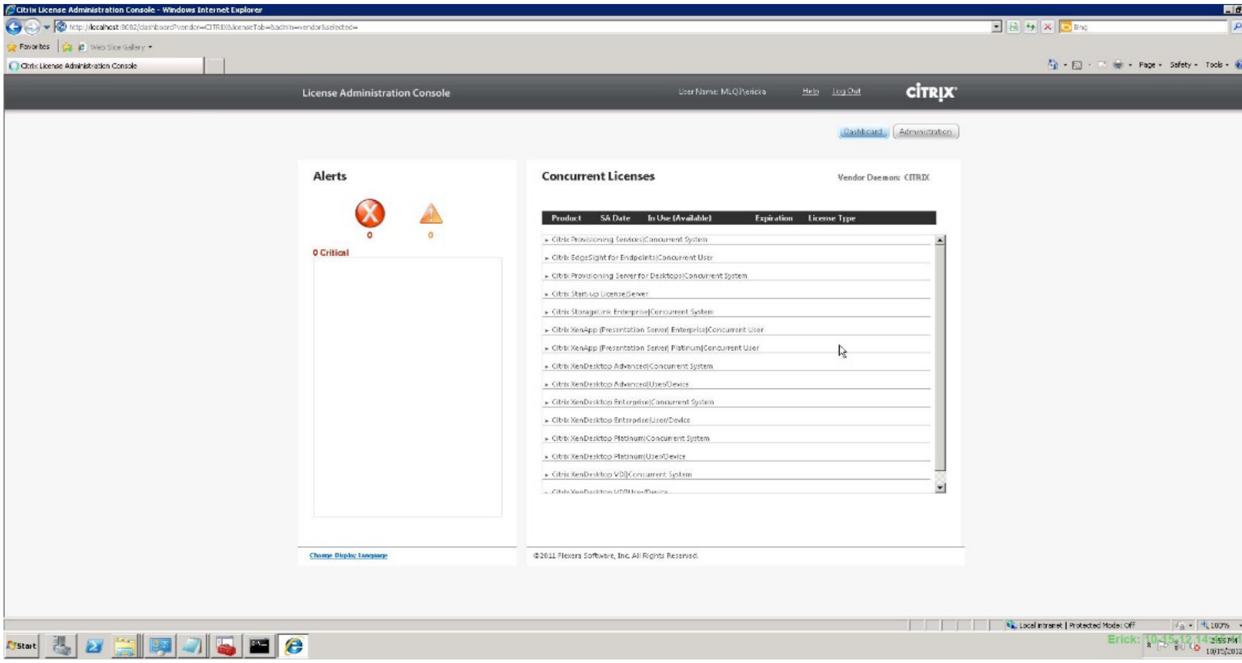
13. Validate that the import was successful



Import Information

- Successfully uploaded license file to C:\Program Files (x86)\Citrix\Licensing\MyFiles\
- Changed vendor daemon license path for CITRIX. Vendor daemon must be restarted for change to take effect.
- Updated vendor daemon configuration for CITRIX.

14. Click OK
15. Click on the Dashboard button
16. Validate that the necessary licenses have been installed



Concurrent Licenses

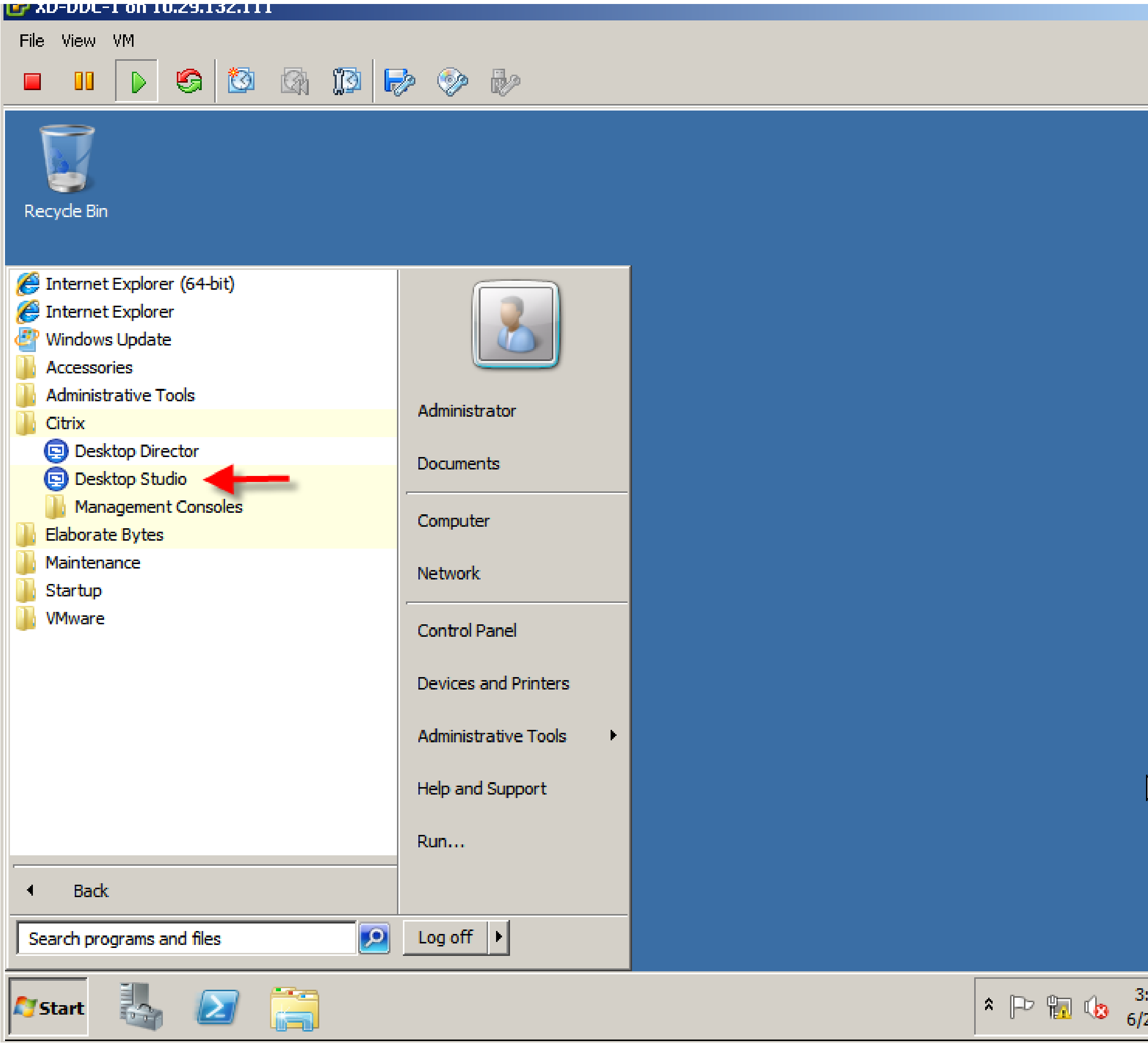
Vendor Daemon: CITRIX

Product	SA Date	In Use (Available)	Expiration	License Type
Citrix Provisioning Services|Concurrent System				
Citrix EdgeSight for Endpoints|Concurrent User				
Citrix Provisioning Server for Desktops|Concurrent System				
Citrix Start-up License|Server				
Citrix StorageLink Enterprise|Concurrent System				
Citrix XenApp (Presentation Server) Enterprise|Concurrent User				
Citrix XenApp (Presentation Server) Platinum|Concurrent User				
Citrix XenDesktop Advanced|Concurrent System				
Citrix XenDesktop Advanced|User/Device				
Citrix XenDesktop Enterprise|Concurrent System				
Citrix XenDesktop Enterprise|User/Device				
Citrix XenDesktop Platinum|Concurrent System				
Citrix XenDesktop Platinum|User/Device				
Citrix XenDesktop VDI|Concurrent System				
Citrix XenDesktop VDI|User/Device				

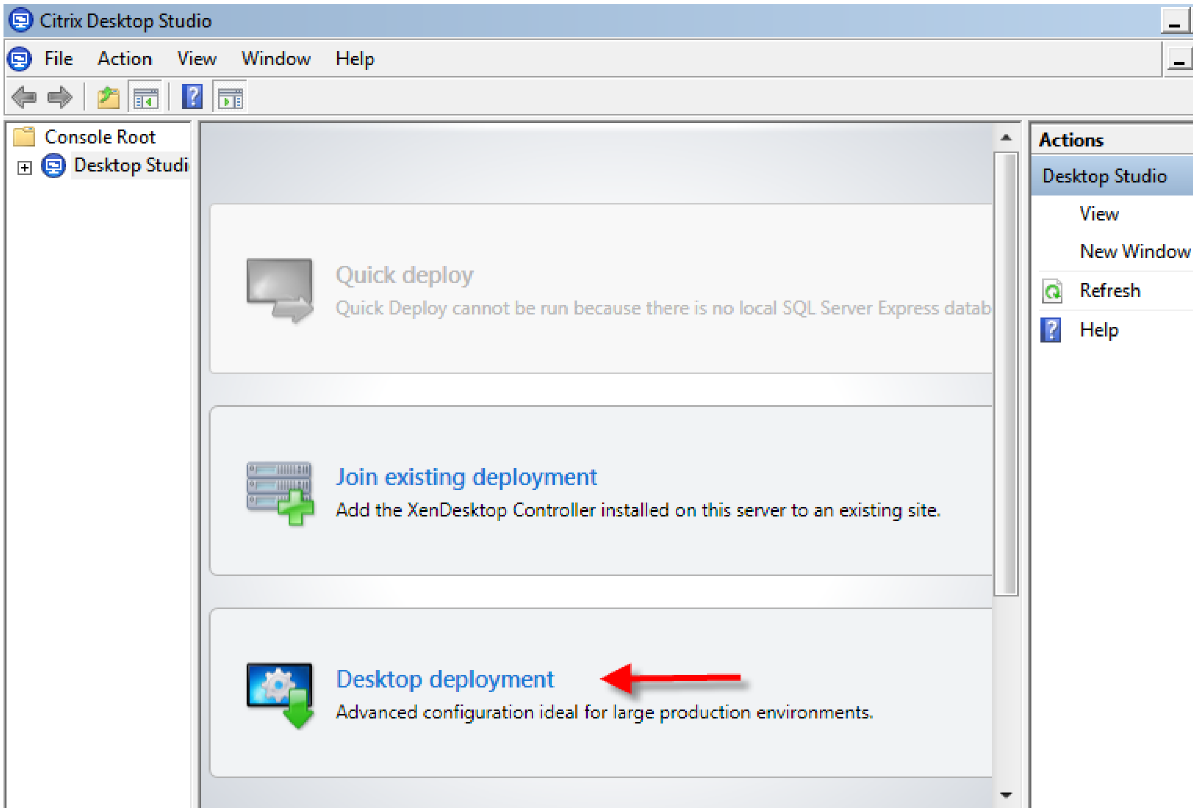
©2011 Flexera Software, Inc. All Rights Reserved.

6.7.4 Create SQL Database for Citrix XenDesktop

1. After successfully installing XenDesktop, go to Start,>All Programs> Citrix>Desktop Studio (or if you checked the box Configure XenDesktop after Closing, it will launch automatically.)



2. Click on Desktop deployment in the XenDesktop Wizard.



Quick deploy

Quick Deploy cannot be run because there is no local SQL Server Express datab

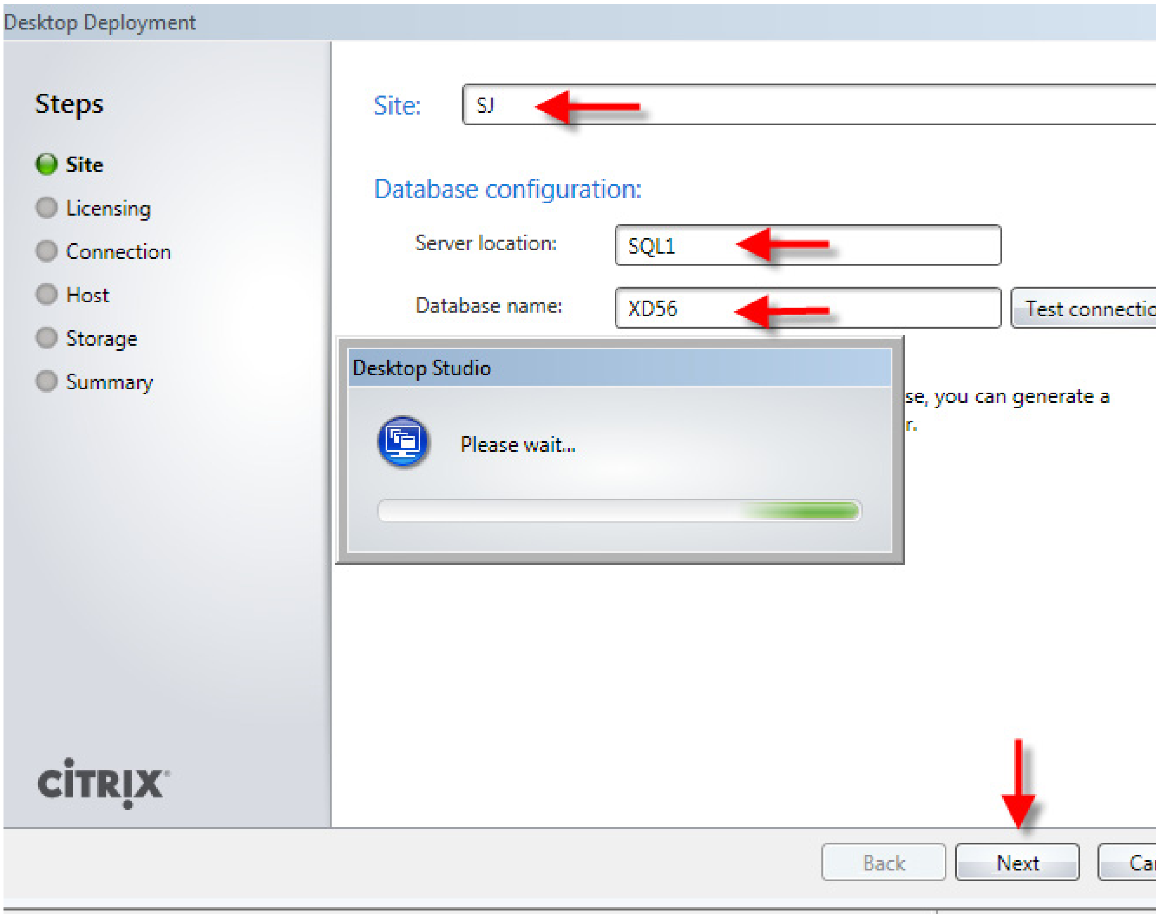
Join existing deployment

Add the XenDesktop Controller installed on this server to an existing site.

Desktop deployment

Advanced configuration ideal for large production environments.

3. Name the Site



Desktop Deployment

Site: SJ

Database configuration:

Server location: SQL1

Database name: XD56

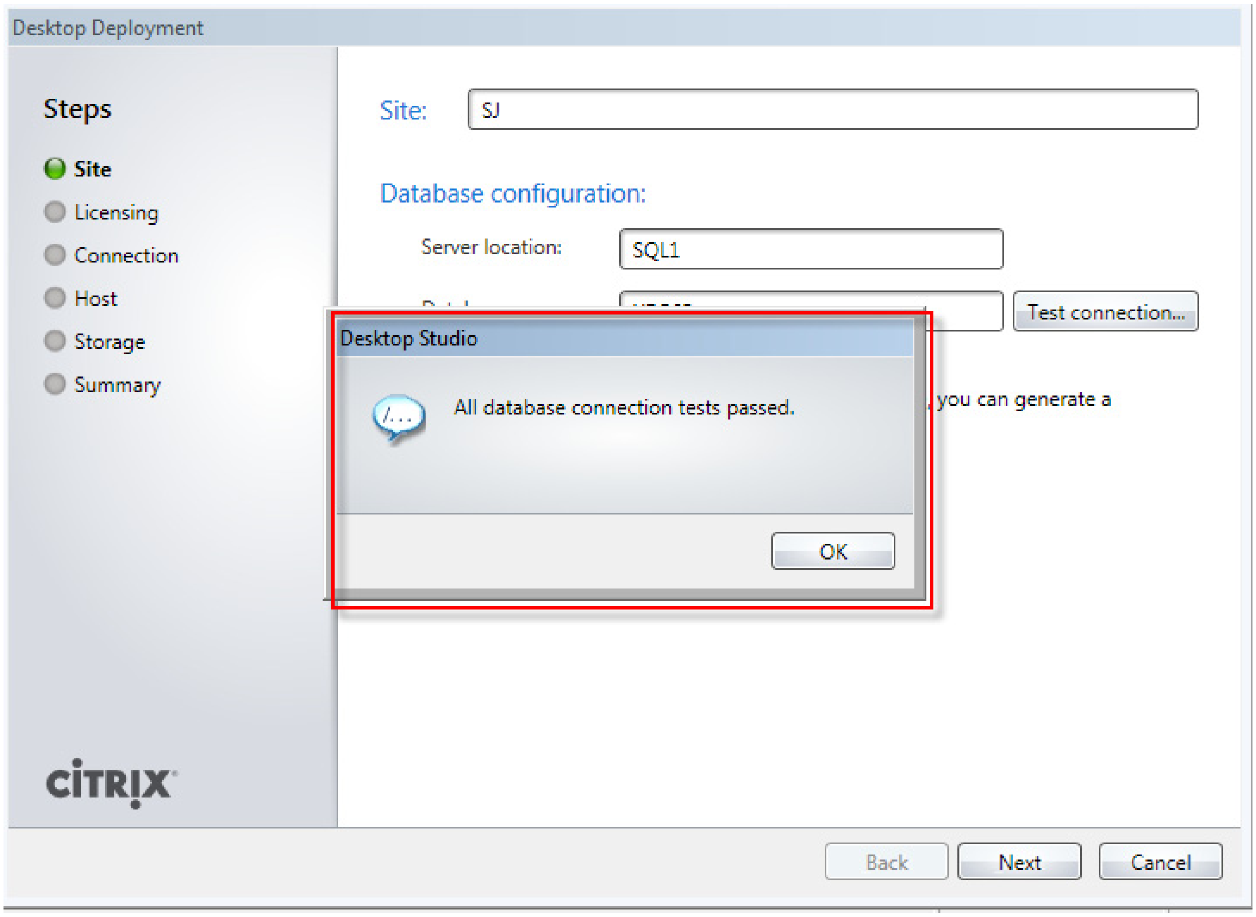
Desktop Studio

Please wait...

4. Database Configuration:

- Enter the name of the SQL server installed earlier.
- In the Database name field, enter the name of the database.
- Leave the prepopulated default Database name as it is, so that the wizard can create the database.

Note To validate connectivity to the SQL Server, use the **Test Connection** button. If the database does not exist then an exception will be shown. However, connectivity to the SQL database validates successfully.



Site: SJ

Database configuration:

Server location: SQL1

Desktop Studio

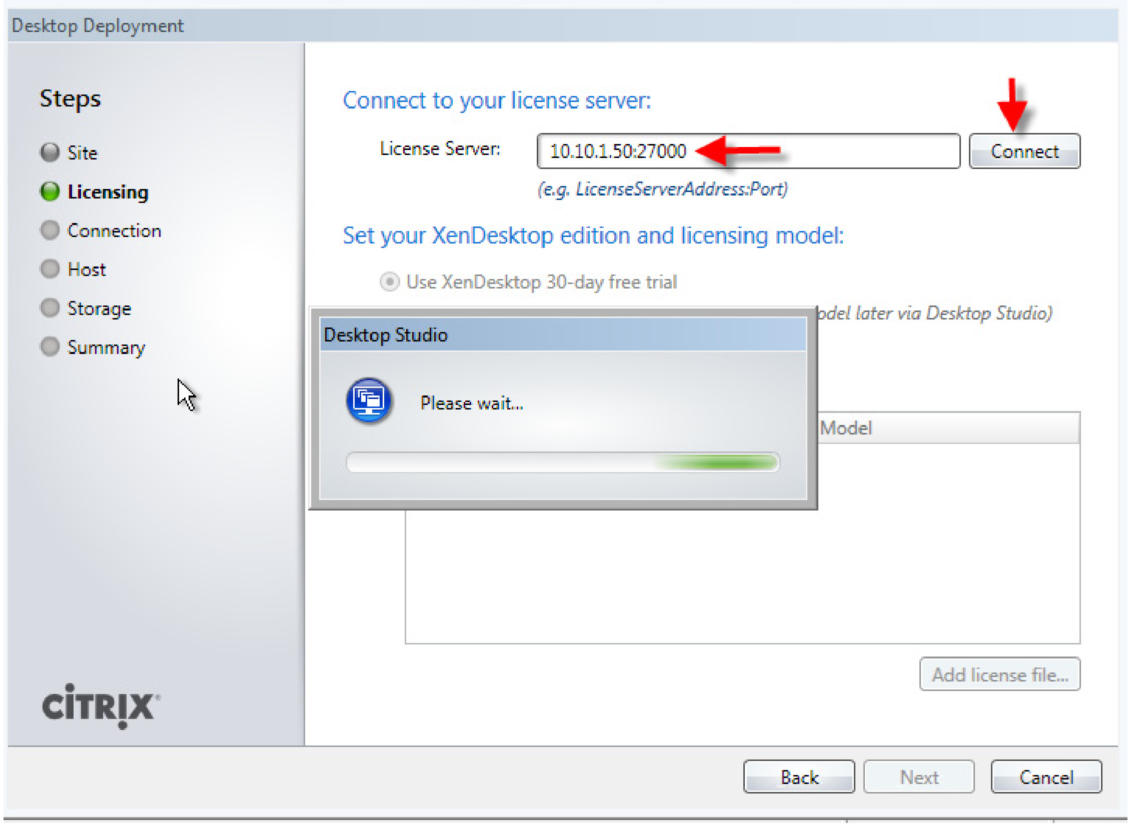
All database connection tests passed.

5. Click “**Next**”.

When your first XenDesktop server is installed and configured, you can repeat the procedure in Section 6.7.2 Install XenDesktop above to create load balancing and a fault tolerant XenDesktop environment.

6.7.5 Configure the Citrix XenDesktop Site Hosts and Storage

1. Enter licensing server name or IP address, click Connect and select a license. Click “**Next**”.



Connect to your license server:

License Server: 10.10.1.50:27000

(e.g. LicenseServerAddress:Port)

Set your XenDesktop edition and licensing model:

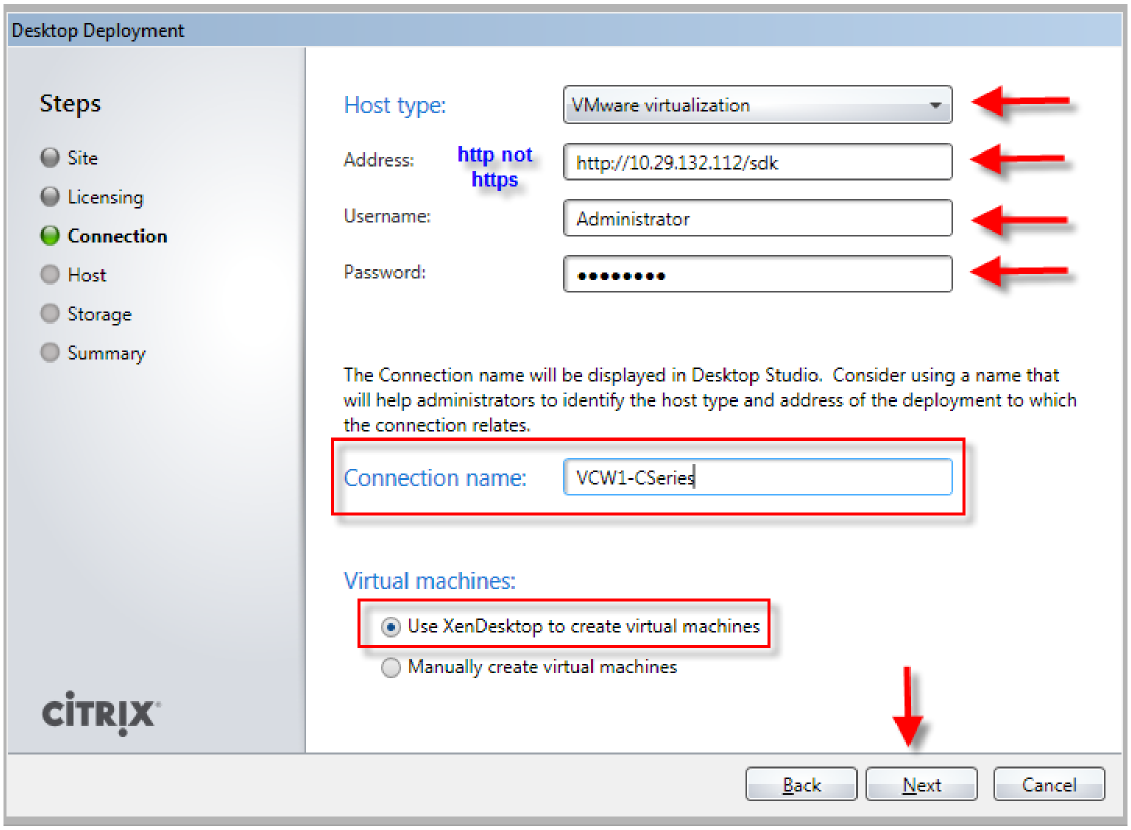
○ Use XenDesktop 30-day free trial

odel later via Desktop Studio)

2. Select VMware Virtualization from the Host Type dropdown
3. Enter VCenter URL information

Note Your vCenter server or appliance must have a trusted 3rd Party SSL certificate to use https.

4. Enter the vCenter administrator user name and password.
5. Click “**Next**”.



Desktop Deployment

Host type: VMware virtualization

Address: http://10.29.132.112/sdk

http not https

Username: Administrator

Password: ••••••••

The Connection name will be displayed in Desktop Studio. Consider using a name that will help administrators to identify the host type and address of the deployment to which the connection relates.

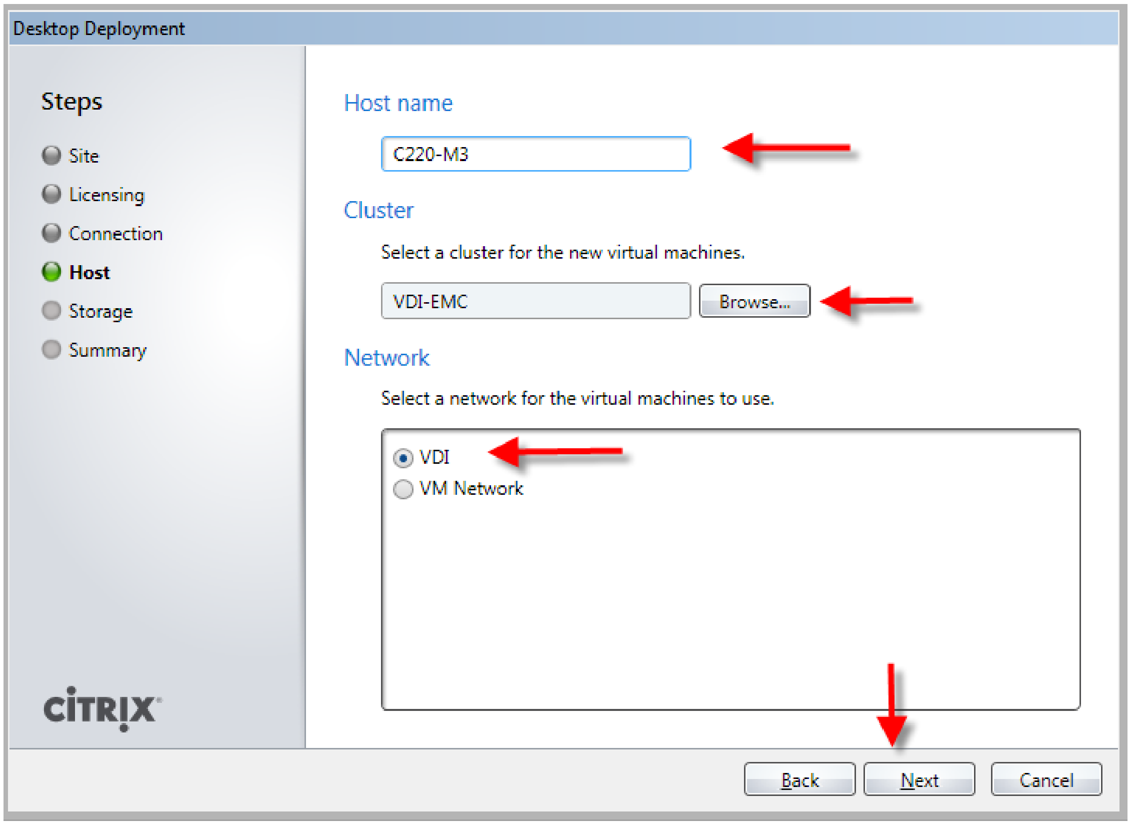
Connection name: VCW1-CSeries

Virtual machines:

● Use XenDesktop to create virtual machines

○ Manually create virtual machines

6. Configure hostname and select cluster and Network (port profile on VMware)



Desktop Deployment

Host name: C220-M3

Cluster

Select a cluster for the new virtual machines.

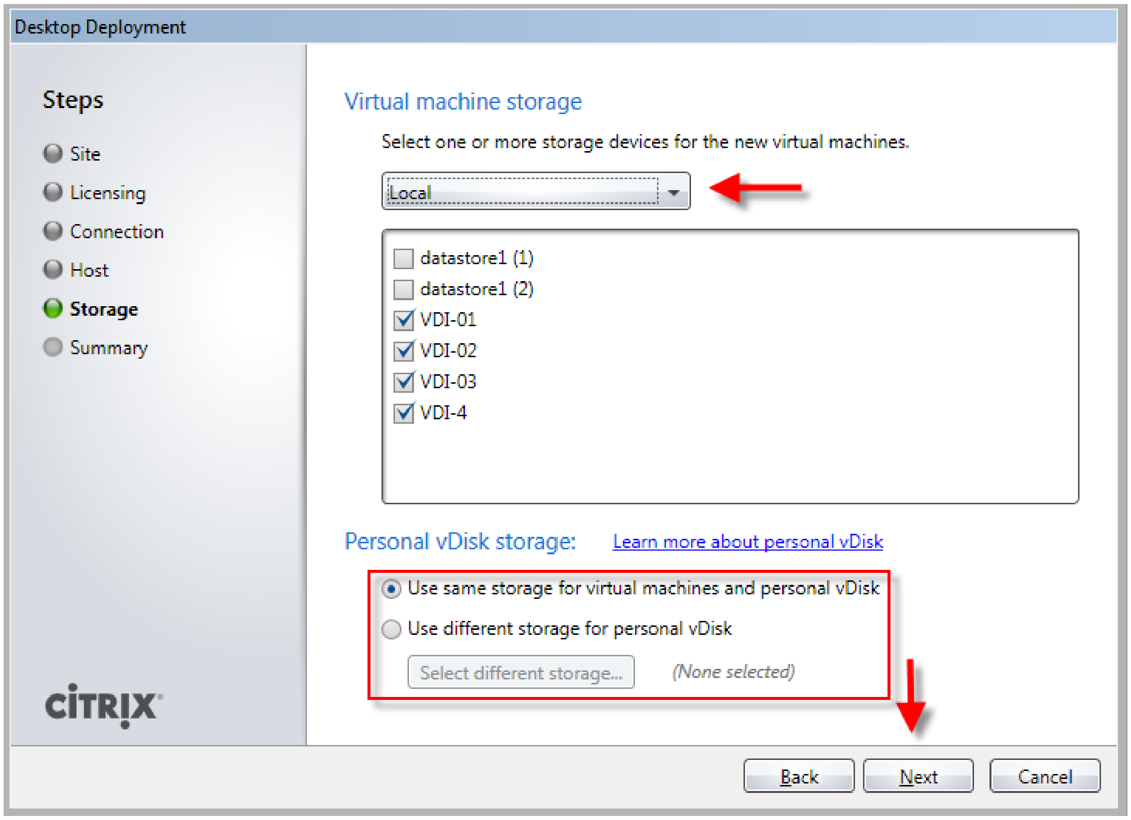
VDI-EMC

Select a network for the virtual machines to use.

● VDI
○ VM Network

7. Click “**Next**”
8. Select storage - this correlates to your vCenter’s Datastore.

Note For FC datastores, select Local from the dropdown to enable each datastore assigned to the hosts.



Desktop Deployment

Virtual machine storage

Select one or more storage devices for the new virtual machines.

Local

- ☐ datastore1 (1)
- ☐ datastore1 (2)
- ☑ VDI-01
- ☑ VDI-02
- ☑ VDI-03
- ☑ VDI-4

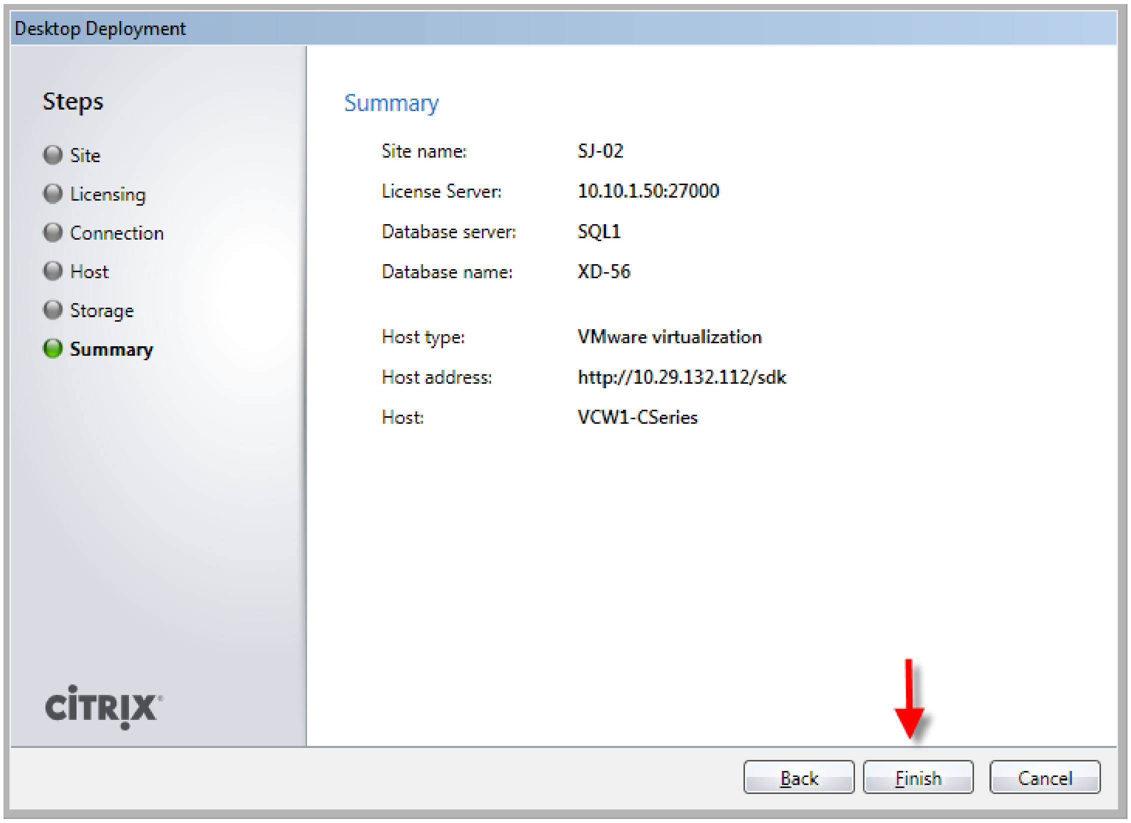
Personal vDisk storage: Learn more about personal vDisk

● Use same storage for virtual machines and personal vDisk

○ Use different storage for personal vDisk

Select different storage... (None selected)

9. Click “**Next**”

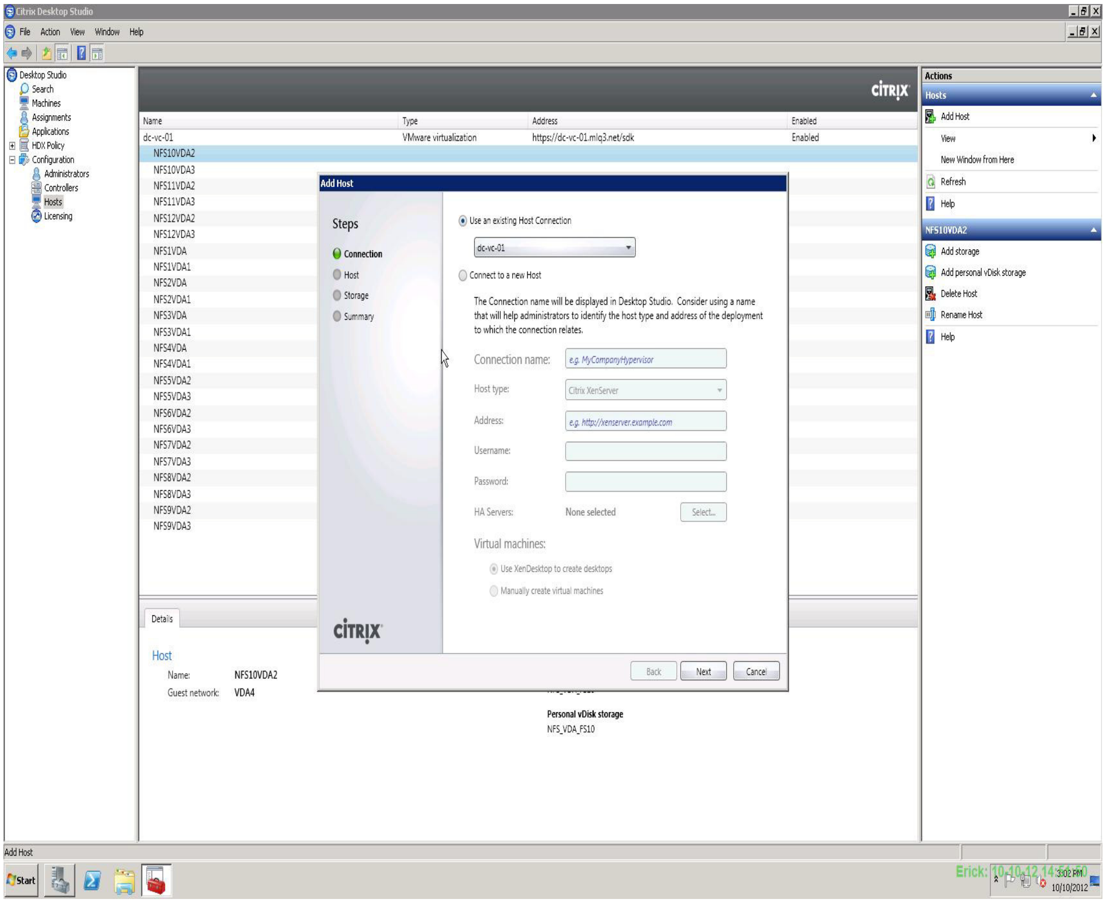


Desktop Deployment

Summary

Site name:	SJ-02
License Server:	10.10.1.50:27000
Database server:	SQL1
Database name:	XD-56
Host type:	VMware virtualization
Host address:	http://10.29.132.112/sdk
Host:	VCW1-CSeries

10. Click “Finish”
11. Create additional hosts per datastore & network.
    - Right click on your existing VCenter Storage “Host” connection
    - Select “Add Storage”
    - Select “Use an Existing Host connection”



Name	Type	Address	Enabled
dc-vc-01	VMware virtualization	https://dc-vc-01.mlq3.net/sdk	Enabled
NFS10VDA2			
NFS10VDA3			
NFS11VDA2			
NFS11VDA3			
NFS12VDA2			
NFS12VDA3			
NFS1VDA			
NFS1VDA1			
NFS2VDA			
NFS2VDA1			
NFS3VDA			
NFS3VDA1			
NFS4VDA			
NFS4VDA1			
NFS5VDA2			
NFS5VDA3			
NFS6VDA2			
NFS6VDA3			
NFS7VDA2			
NFS7VDA3			
NFS8VDA2			
NFS8VDA3			
NFS9VDA2			
NFS9VDA3			

Details

Host

Name: NFS10VDA2

Guest network: VDA4

Personal vDisk storage

NFS_VDA_FS10

Add Host

Steps

- Connection
- Host
- Storage
- Summary

● Use an existing Host Connection

dc-vc-01

○ Connect to a new Host

The Connection name will be displayed in Desktop Studio. Consider using a name that will help administrators to identify the host type and address of the deployment to which the connection relates.

Connection name: e.g. MyCompanyHypervisor

Host type: Citrix XenServer

Address: e.g. http://xenserver.example.com

Username:

Password:

HA Servers: None selected [Select...]

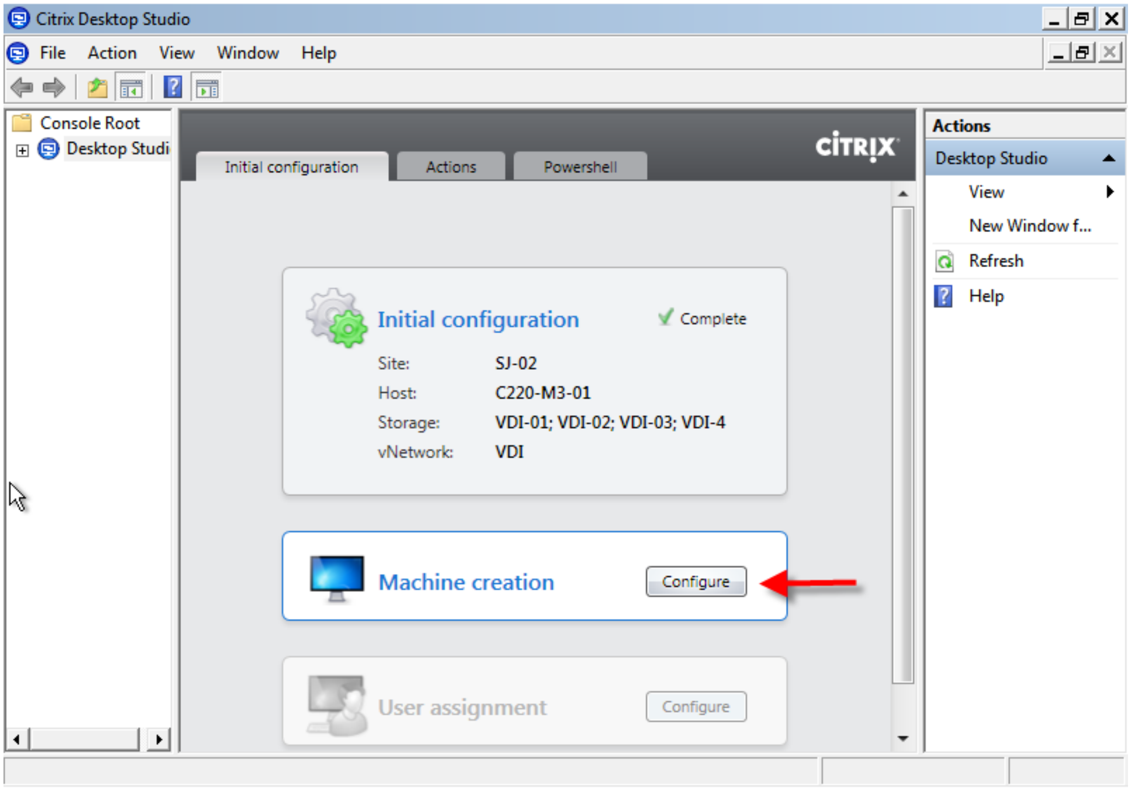
Virtual machines:

● Use XenDesktop to create desktops

○ Manually create virtual machines

[Back] [Next] [Cancel]

The configuration wizard will show the Initial configuration is now complete.



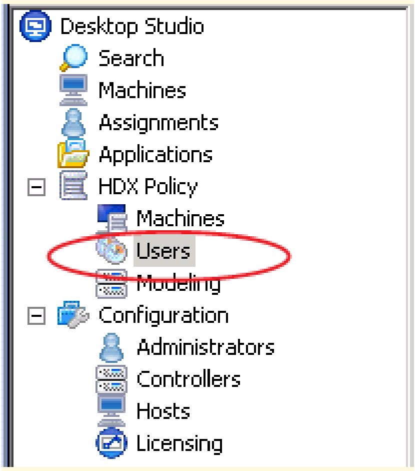
Site: SJ-02
Host: C220-M3-01
Storage: VDI-01; VDI-02; VDI-03; VDI-4
vNetwork: VDI

6.7.6 Configure Citrix XenDesktop HDX Polices

When testing with VSI a XenDesktop policy should be created to disable client printer mapping which is enabled by default. HDX policies configured and applied in Citrix Desktop Studio.

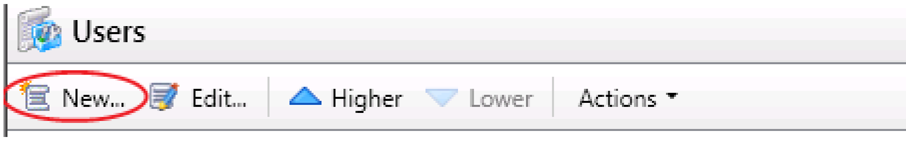
§ Open Desktop Studio, expand the Desktop Studio node

§ Proceed to HDX Policy → Users in the left pane

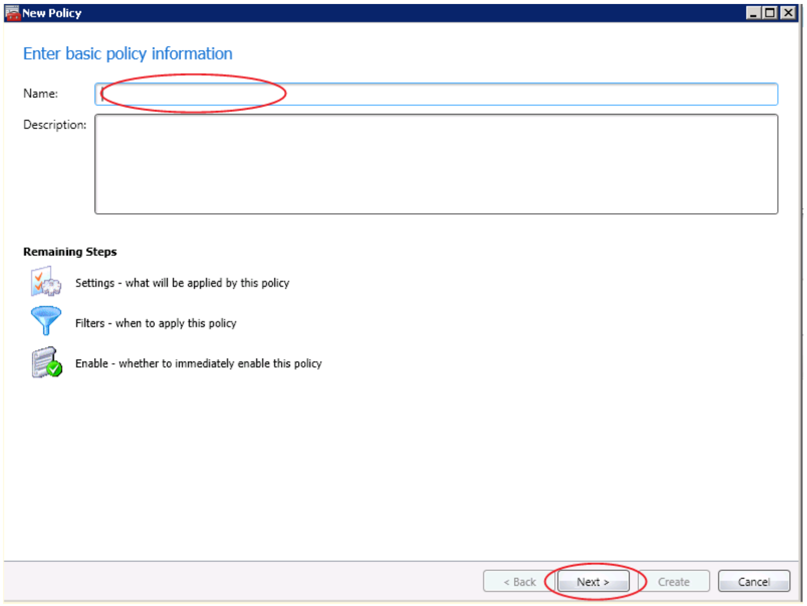


§ Click “New..” in the center pane to start the policy creation

process



§ Enter a name for your policy and click “Next”


New Policy

Enter basic policy information

Name:

Description:

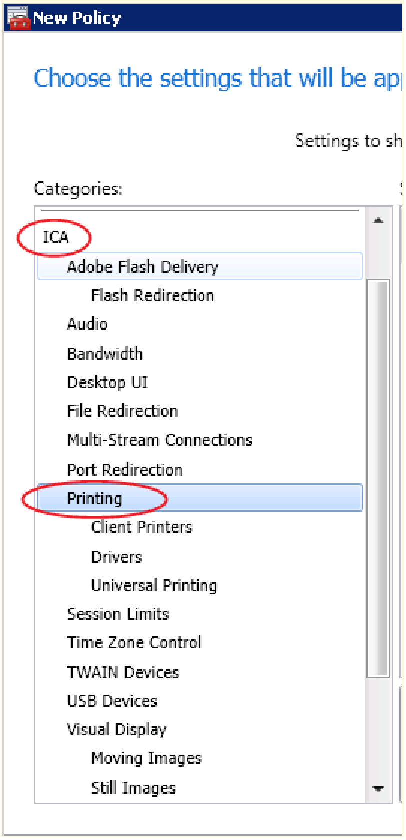
Remaining Steps

Settings - what will be applied by this policy

Filters - when to apply this policy

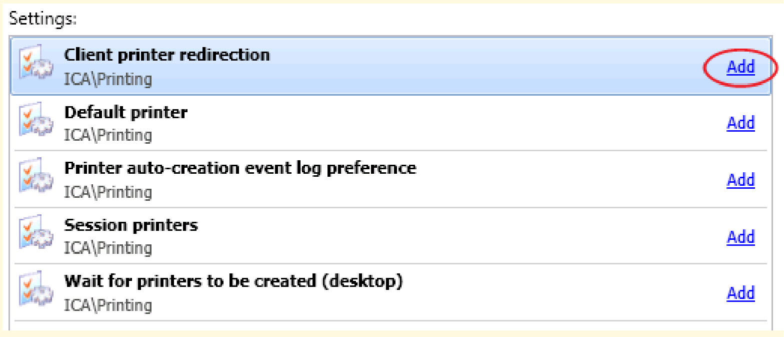
Enable - whether to immediately enable this policy

§ Select from Categories ICA→ Printing



Choose the settings that will be ap

§ Select Client printer redirection and click "add"


Settings:

Client printer redirection ICA\Printing Add

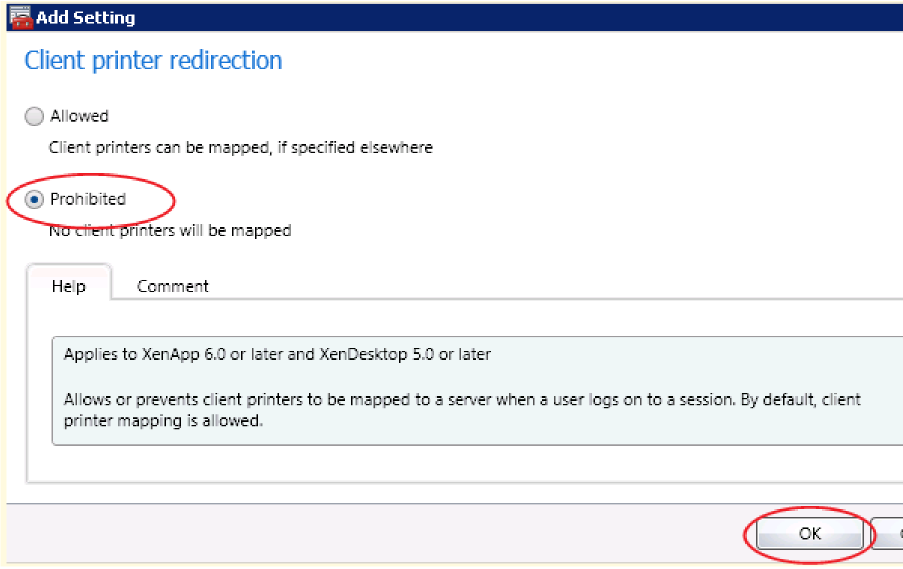
Default printer ICA\Printing Add

Printer auto-creation event log preference ICA\Printing Add

Session printers ICA\Printing Add

Wait for printers to be created (desktop) ICA\Printing Add

§ Click on “Prohibited” and then click “OK”



Add Setting

Client printer redirection

○ Allowed

Client printers can be mapped, if specified elsewhere

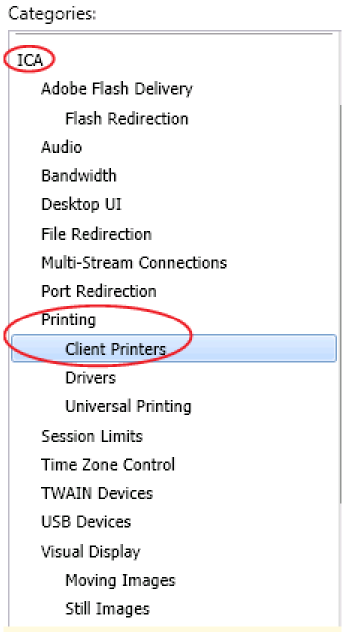
● Prohibited

No client printers will be mapped

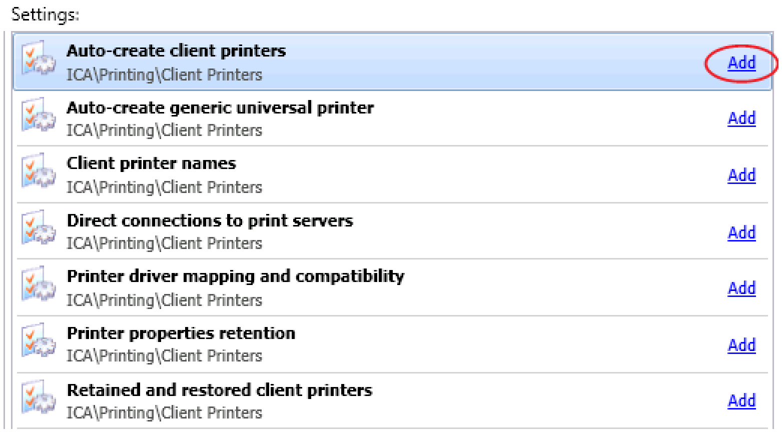
Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

Allows or prevents client printers to be mapped to a server when a user logs on to a session. By default, client printer mapping is allowed.

§ Select from Categories ICA→ Printing → Client Printers



§ Select “Auto-create client printers” and click “Add”



Settings:

Auto-create client printers
ICA\Printing\Client Printers — Add

Auto-create generic universal printer
ICA\Printing\Client Printers — Add

Client printer names
ICA\Printing\Client Printers — Add

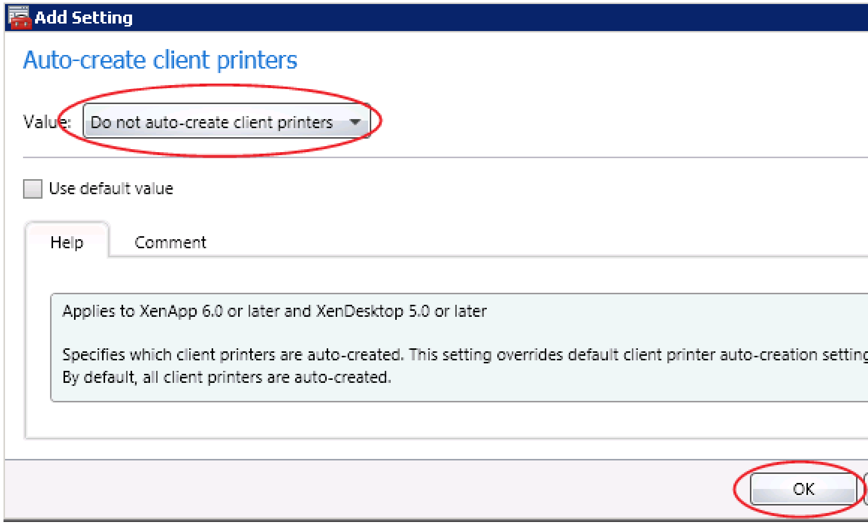
Direct connections to print servers
ICA\Printing\Client Printers — Add

Printer driver mapping and compatibility
ICA\Printing\Client Printers — Add

Printer properties retention
ICA\Printing\Client Printers — Add

Retained and restored client printers
ICA\Printing\Client Printers — Add

§ From the drop-down list, pick “Do not auto-create client printers” and click “OK”



Add Setting

Auto-create client printers

Value: Do not auto-create client printers

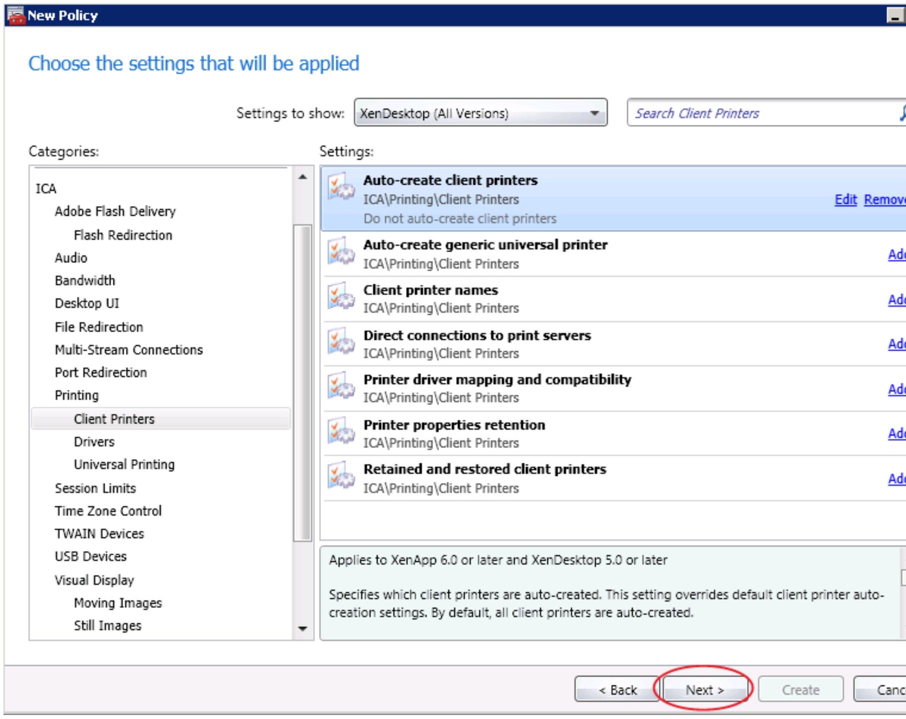
□ Use default value

Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

Specifies which client printers are auto-created. This setting overrides default client printer auto-creation setting

By default, all client printers are auto-created.

- Click “Next”



New Policy

Choose the settings that will be applied

Settings to show: XenDesktop (All Versions)

Search Client Printers

Categories:

ICA
Adobe Flash Delivery
Flash Redirection
Audio
Bandwidth
Desktop UI
File Redirection
Multi-Stream Connections
Port Redirection
Printing
Client Printers
Drivers
Universal Printing
Session Limits
Time Zone Control
TWAIN Devices
USB Devices
Visual Display
Moving Images
Still Images

Settings:

Auto-create client printers
ICA\Printing\Client Printers
Do not auto-create client printers
Edit Remov

Auto-create generic universal printer
ICA\Printing\Client Printers

Client printer names
ICA\Printing\Client Printers

Direct connections to print servers
ICA\Printing\Client Printers

Printer driver mapping and compatibility
ICA\Printing\Client Printers

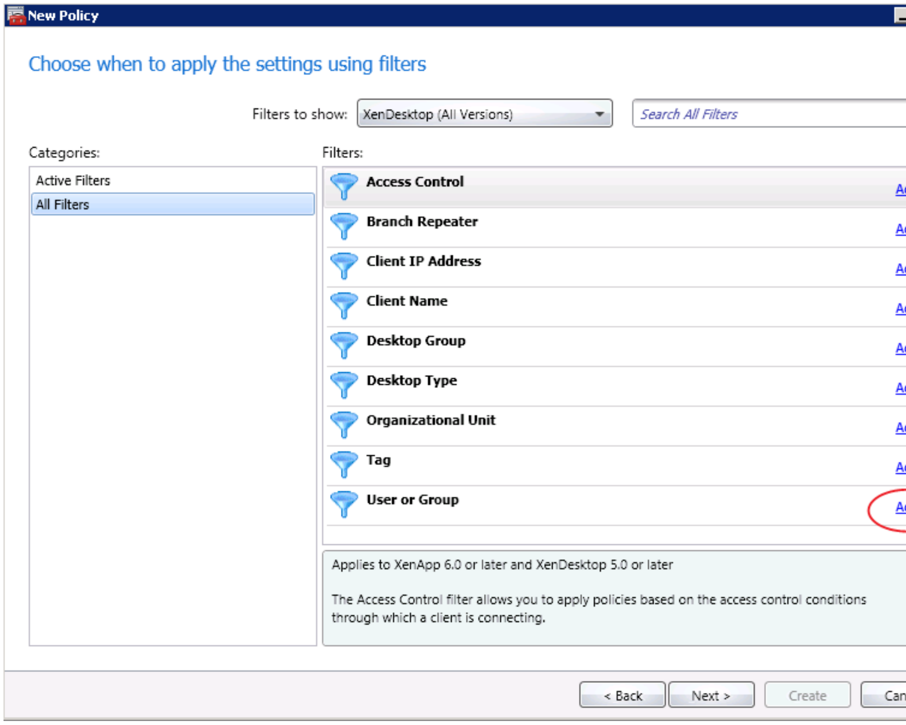
Printer properties retention
ICA\Printing\Client Printers

Retained and restored client printers
ICA\Printing\Client Printers

Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

Specifies which client printers are auto-created. This setting overrides default client printer auto-creation settings. By default, all client printers are auto-created.

- Select All Filters → “User or Group” and click “Add” Create policy filter



New Policy

Choose when to apply the settings using filters

Filters to show: XenDesktop (All Versions)

Search All Filters

Categories:

Active Filters
All Filters

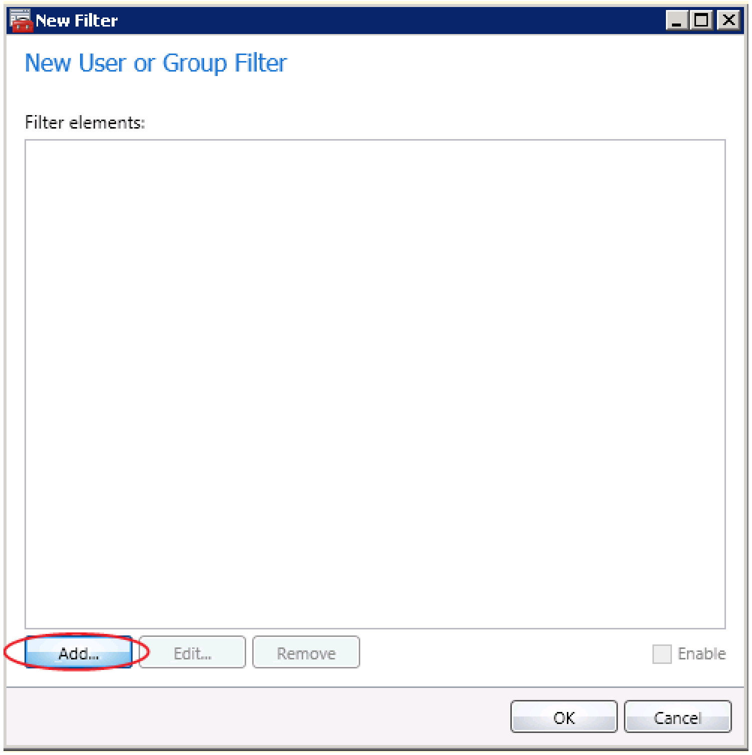
Filters:

Access Control
Branch Repeater
Client IP Address
Client Name
Desktop Group
Desktop Type
Organizational Unit
Tag
User or Group

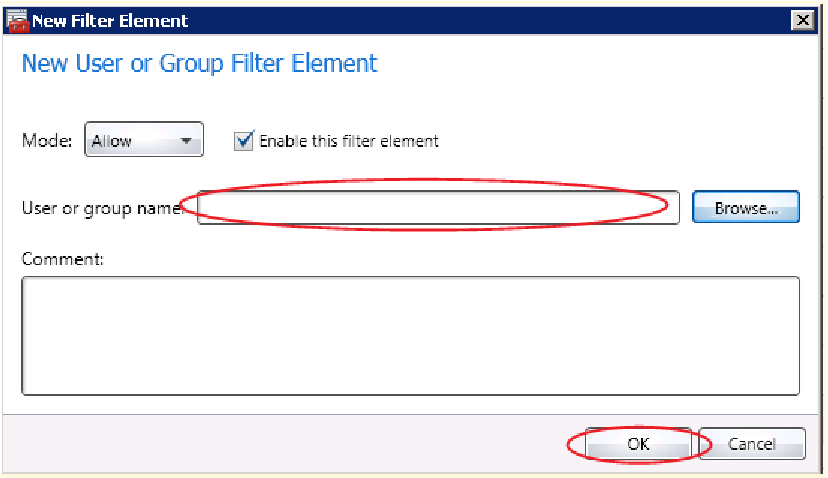
Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

The Access Control filter allows you to apply policies based on the access control conditions through which a client is connecting.

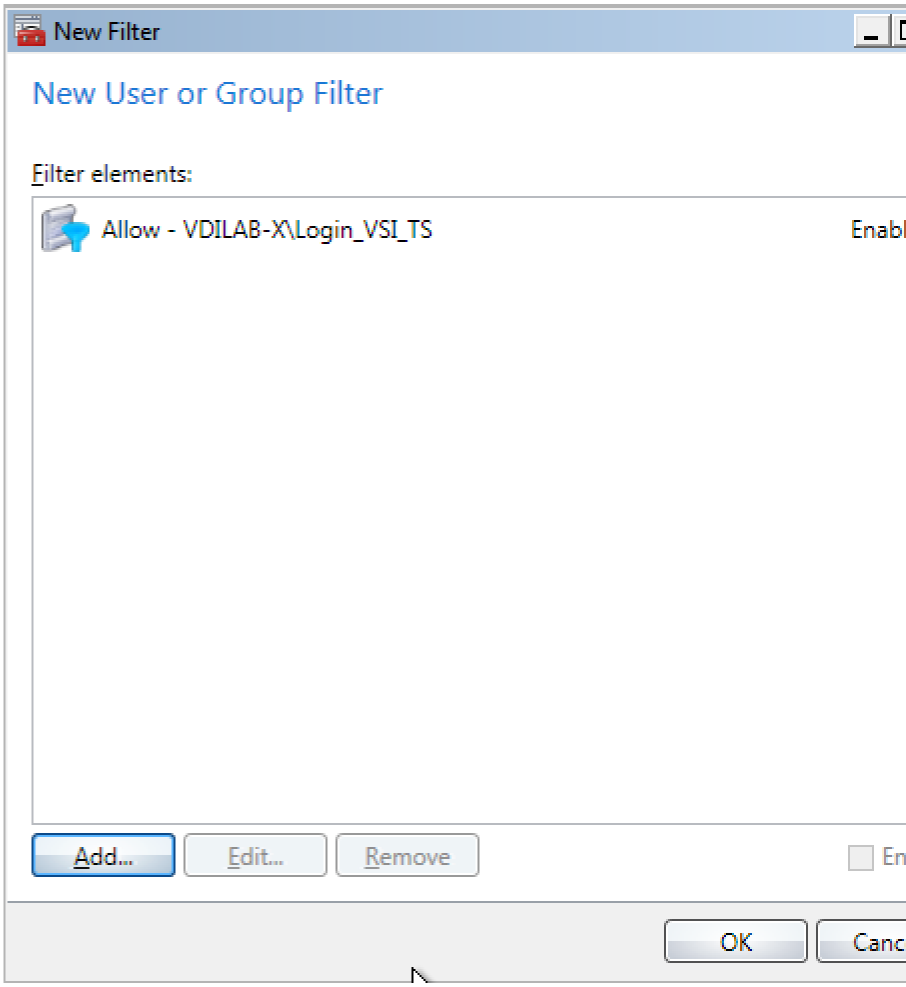
§ Click "Add…"



§ Pick User Group you'll be applying this policy to



§ Click “OK”



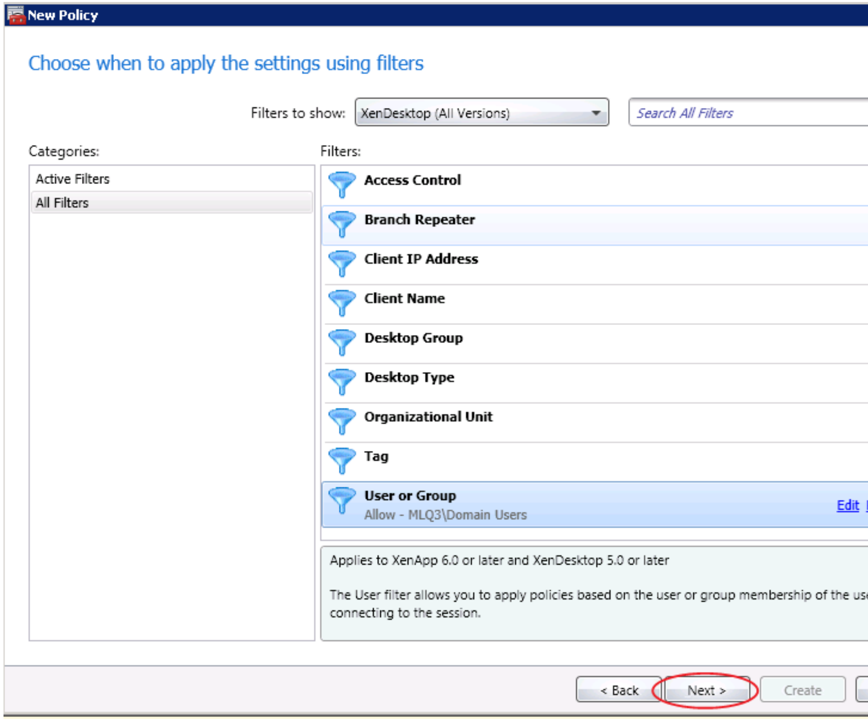
New Filter

New User or Group Filter

Filter elements:

Allow - VDILAB-X\Login_VSI_TS Enabl

§ Click “Next”



New Policy

Choose when to apply the settings using filters

Filters to show: XenDesktop (All Versions)

Search All Filters

Categories:

- Active Filters
- All Filters

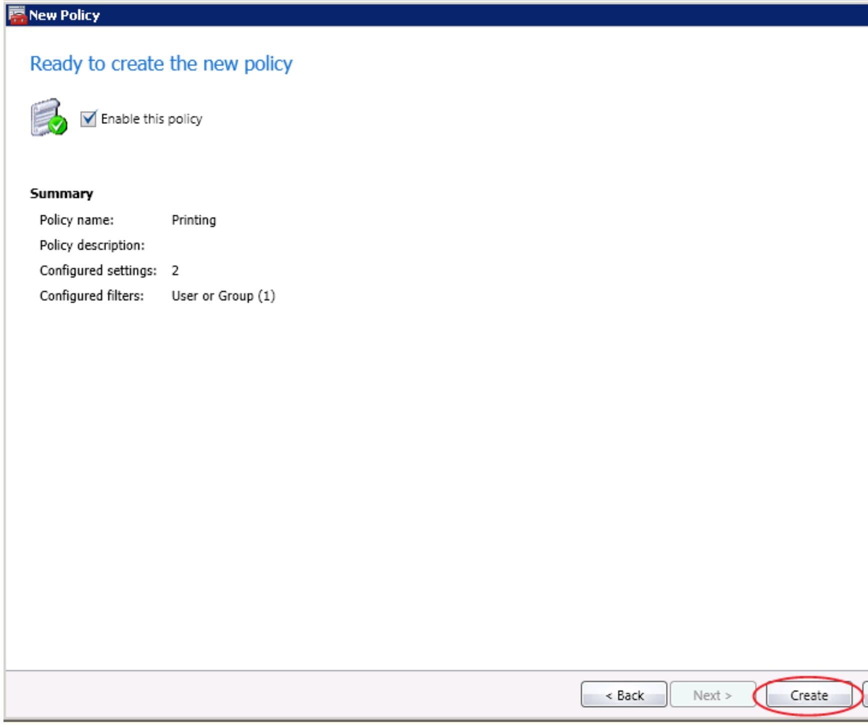
Filters:

- Access Control
- Branch Repeater
- Client IP Address
- Client Name
- Desktop Group
- Desktop Type
- Organizational Unit
- Tag
- User or Group
  Allow - MLQ3\Domain Users — Edit

Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

The User filter allows you to apply policies based on the user or group membership of the us connecting to the session.

§ Click “Create”



New Policy

Ready to create the new policy

☑ Enable this policy

Summary

Policy name:	Printing
Policy description:	
Configured settings:	2
Configured filters:	User or Group (1)

7 Desktop Delivery Infrastructure and Golden Image Creation

Many components are required to support the Virtual Desktop Infrastructure used in this project. This section details the key servers and their roles in the solution. Ultimately, XenDesktop 5.6 FP1 with Machine Creation Services managed the VDI environment in this project.

This section includes:

An overview of the component servers in the solution

User Profile Management

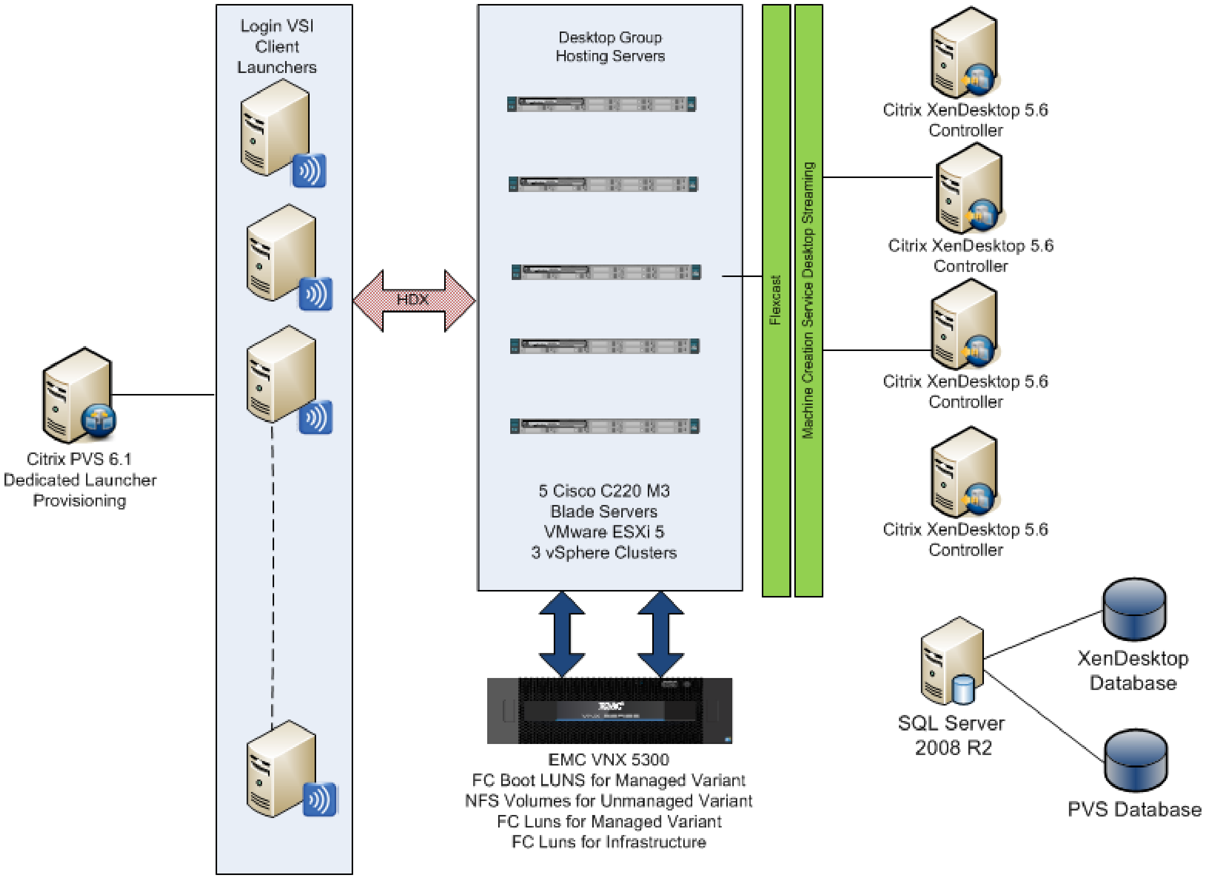
Creating the Windows 7 SP1 Golden Image

Using Machine Creation Services to create 600 virtual desktops

7.1 Overview of Solution Components

The image below provides a logical overview of the solution components in the environment.

Figure 18 Citrix XenDesktop 5.6 and Machine Creation Services Logical Diagram



Summary of the Environment:

- 5 ESXi-5.0.0 Update 1-on C220 M3 (build 623860-custom-Cisco-2.0.1.6) VDI Hosts

- 2 ESXi-5.0.0-on C250 M2 (build 469512-custom-Cisco-2.0.1d) Infrastructure Hosts
- 2 ESXi-5.0.0-on C250 M2 (build 469512-custom-Cisco-2.0.1d) LoginVSI Launcher Hosts
- 2 XenDesktop 5.6 FP1 Delivery Controllers
- 1 ESXi vCenter 5.0.0 Update 1b Build 804277
- 20 VSI Launcher VMs
- 600 Virtual Desktops equally distributed on 5 Hosts in one Cluster
- 1 Citrix Licensing Server
- 1 Web Interface Server
- 2 File Servers (User Roaming Profiles and LoginVSI Share)
- 1 Microsoft SQL Server 2008 R2 for XenDesktop and vCenter
- 2 Active Directory Domain Controllers hosting DNS and DHCP services

Storage on EMC VNX 7500.

- 5 5 GB Fibre Channel Boot LUNs (Managed FC Variant)
- 2 500 GB Shared XenDesktop infrastructure Fibre Channel LUNs or NFS Volumes
- 4 500 GB NFS mounts for Virtual Desktop MCS disks (Unmanaged NFS Variant)
- 4 500 GB FC LUNs for Virtual Desktop MCS disks (Managed FC Variant)

The following tables provide details on the configuration of the solution components.

Table 7 Solution Component Configurations

Vmware ESXi 5.0U1 Hosts			
Hardware:	Cisco C-Series Rack Servers	**Model:**	C220 M3
OS:	VMware ESXi 5.0U1	**RAM:**	256GB
CPU:	2X 8-Core CPUs	**Network:**	UCS VIC1225 Converged Network Adapter
Disk:	None (Boot LUNs)		

Citrix XenDesktop 5.6 Delivery Controllers			
Hardware:	Virtual Machine	**Model:**	
OS:	Windows 2008 R2	**RAM:**	4GB
CPU:	1vCPUs	**Network:**	1x1Gbps;1x10Gbps
Disk:	40GB		Variant Dependent

Vmware vCenter Server			
Hardware:	Virtual Machine	**Model:**	
OS:	Windows 2008 R2	**RAM:**	4GB
CPU:	1vCPU	**Network:**	1x1Gbps;1x10Gbps
Disk:	40GB		Variant Dependent

Microsoft SQL Server 2008 R2 for XenDesktop and Launcher PVS			
Hardware:	Virtual Machine	**Model:**	
OS:	Windows 2008 R2	**RAM:**	4GB
CPU:	2vCPUs	**Network:**	1x1Gbps;1x10Gbps
Disk:	40GB		Variant Dependent

Active Directory Domain Controllers			
Hardware:	Virtual Machine	**Model:**	
OS:	Windows 2008 R2	**RAM:**	2GB
CPU:	1vCPU	**Network:**	1x1Gbps;1x10Gbps
Disk:	40GB		Variant Dependent

File Servers			
Hardware:	Virtual Machine	**Model:**	
OS:	Windows 2008 R2	**RAM:**	2GB
CPU:	1vCPU	**Network:**	1x1Gbps;1x10Gbps
Disk:	40GB		Variant Dependent

7.2 File Servers for User Profile Management and Login VSI Share

We used one Microsoft Server 2008 R2 SP1 File Server for Microsoft Roaming User Profile storage for this testing. Customers who require resiliency can deploy clustered virtual machines.

Microsoft group policy was used to direct all user profiles to this server. A profile share was created on the machine following Microsoft best practices. Profiles were created for each user on first log on and downloaded to the virtual machine on subsequent logins.

For more information on best practices, see the article Best Practices for User Profiles:

http://technet.microsoft.com/en-us/library/cc784484(v=ws.10).aspx

A second Microsoft Server 2008 R2 SP1 File Server was deployed to house Login VSI shares. A shared folder was created to contain the necessary files for operations and data collection. This virtual machine is only required if Login VSI is deployed in the environment.

For more information on setting up the Login VSI share, see the following article, VSIshare Configuration:

http://www.loginvsi.com/documentation/v3/vsishare-configuration

7.3 Microsoft Windows 7 Golden Image Creation

7.3.1 Create Base Windows 7 SP1 32bit Virtual Machine

The Microsoft Windows 7 SP1 master or golden image with additional software was initially installed and prepared as a standard virtual machine on VMware ESXi prior to being used by XenDesktop 5.6 Machine Creation Services to deploy 600 virtual desktops.

With XenDesktop 5.6 the XenDesktop Setup Wizard was utilized.

The following section describes the process used to create the master or golden image and centralized Windows 7 vDisk used by Machine Creation Services.

Virtual Machine Base Software

- Install Win7 32-bit SP1 Enterprise
- Install Office 2010 Professional with Run All From My Computer
- Install Office 2010 Service Pack (most recent)
- Windows Updates (Be sure not to install IE9. Use IE8)

7.3.2 Add Citrix XenDesktop 5.6 Virtual Desktop Agent

1. Copy the VDA executable to the local machine
2. Launch executable
3. Select Advanced Install
4. Use default installation paths.
5. Enter XenDesktop Delivery Controller’s FQDN’s.
6. Click “**Next**”.
7. Do not install HDX or Citrix Receiver.
8. Click “**Finish**”.
9. Remove VDA Welcome Screen program from the Windows Startup folder
10. Restart VM
11. Log in and check the event log to ensure that the DDC registration has successfully completed

7.3.3 Add Login VSI Target Software (Login VSI Test Environments Only)

1. Launch setup wizard using run as Administrator
2. Enter VSI share path
3. Use default installation paths.
4. Reboot after installation completes

7.3.4 Citrix XenDesktop Optimizations

1. Delete XPS Printer
2. Ensure that Bullzip PDF is the default printer
3. Optimize
   - Configure SWAP file to 1536 MB (Cisco requirement)
   - Disable Windows Restore and service
     - Delete the restore points
   - Perform a disk cleanup
   - Disable Windows Firewall Service
   - Disable Windows Backup scheduled jobs
   - Open Computer Management | System Tools | Task Scheduler | Task Scheduler Library | Microsoft | Windows and disable the following:
     - Defrag
     - Offline files

- Windows Backup
- Windows Performance Settings
  - Smooth Edges
  - Use Visual Styles
  - Show Translucent
  - Show Window contents when dragging

4. Modify Action Center settings (uncheck all warnings)
5. Ensure that the Shadow Copy service is running and set to auto

7.3.5 Perform additional PVS and XenDesktop Optimizations

1. Increased the ARP cache lifespan to 600 seconds for stream service bound NICs (article is located in Provisioning Services Reference documentation at the end of the document)
2. Delete XPS Printer
3. Ensure that Bullzip PDF is the default printer
4. Optimize

- Configure SWAP file to 1536 MB (Cisco requirement)
- Disable Windows Restore and service
  - Delete the restore points
- Perform a disk cleanup
- Disable Windows Firewall Service
- Disable Windows Backup scheduled jobs
- Open Computer Management | System Tools | Task Scheduler | Task Scheduler Library | Microsoft | Windows and disable the following:
  - Defrag
  - Offline files
  - Windows Backup
- Windows Performance Settings
  - Smooth Edges
  - Use Visual Styles
  - Show Translucent
  - Show Window contents when dragging

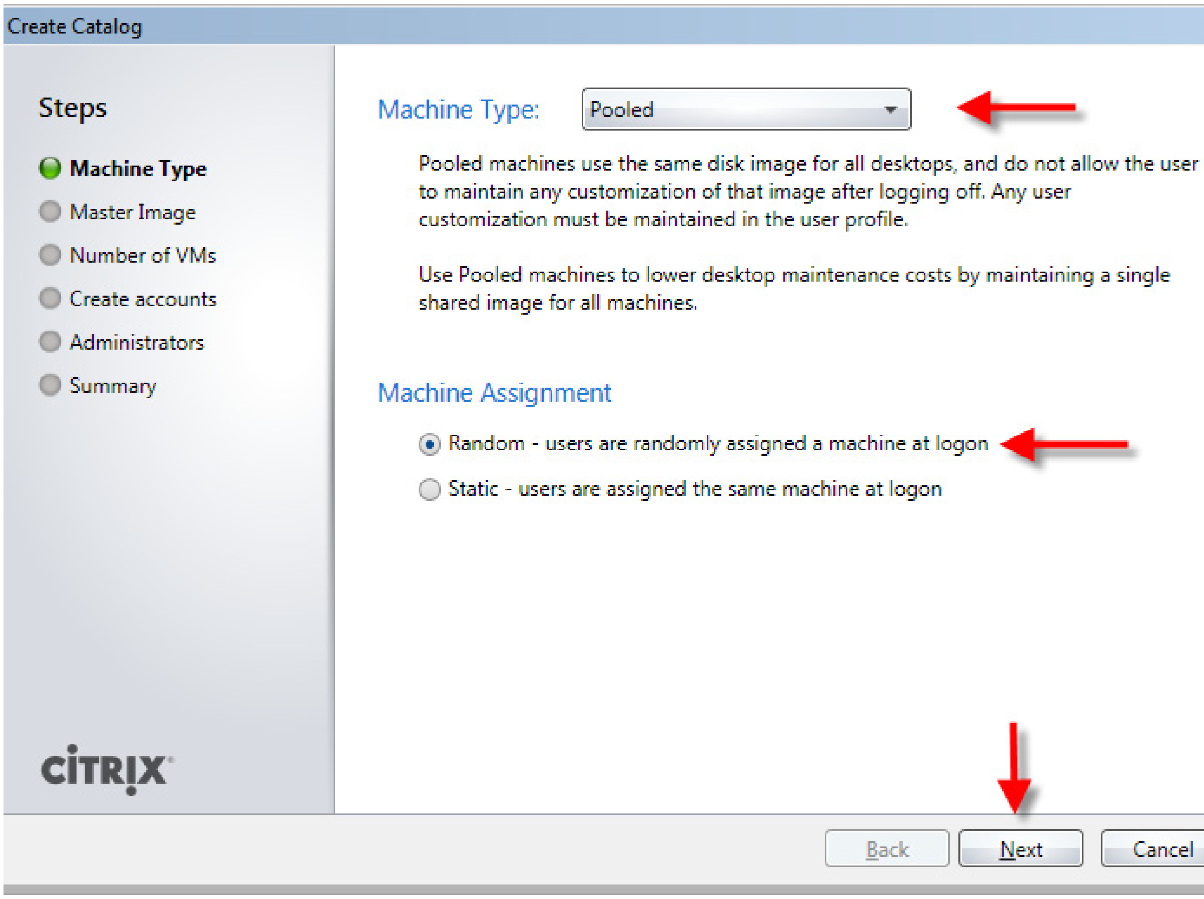
1. Modify Action Center settings (uncheck all warnings)
2. Ensure that the Shadow Copy service is running and set to auto

7.4 Virtual Machine Creation Using Citrix XenDesktop Machine Creation Services

When the golden image machine is created and optimized, shut it down and take a snapshot. We recommend cloning the machine to template as an added protection.

Follow this procedure to use XenDesktop Machine Creation Services to create 600 virtual machines:

1. Open the XenDesktop Studio Console and expand the Desktop Studio node in the navigation page
2. Click the Machines node in the navigation page, then click Create Catalog in the Actions pane
3. Select Pooled for the Machine Type, Random for the Machine Assignment, then click Next



Create Catalog

Steps

- Machine Type
- Master Image
- Number of VMs
- Create accounts
- Administrators
- Summary

Machine Type: Pooled

Pooled machines use the same disk image for all desktops, and do not allow the user to maintain any customization of that image after logging off. Any user customization must be maintained in the user profile.

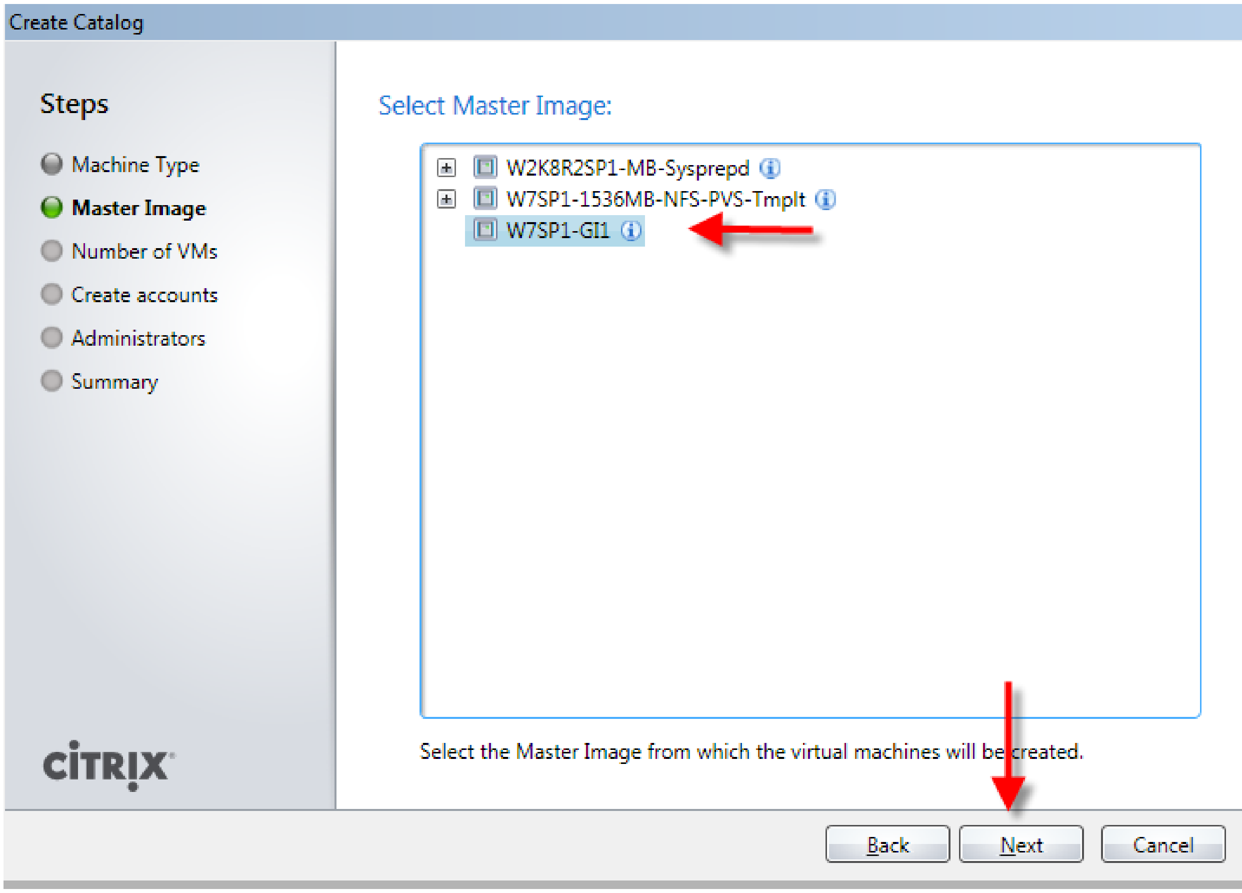
Use Pooled machines to lower desktop maintenance costs by maintaining a single shared image for all machines.

Machine Assignment

● Random - users are randomly assigned a machine at logon

○ Static - users are assigned the same machine at logon

4. Click the golden image created earlier (not the template you may have also created) on the Select Master Image page, then click Next



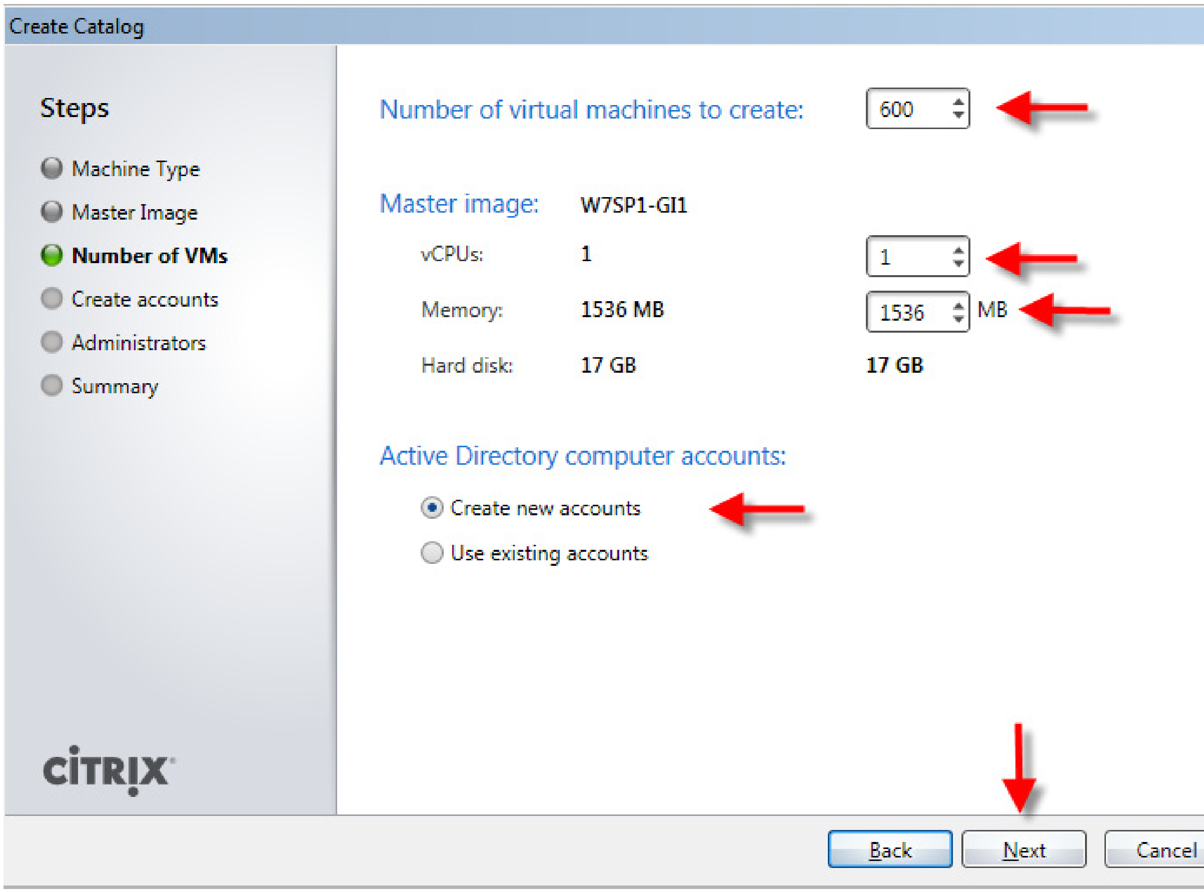
Create Catalog

Steps

Select Master Image:

Select the Master Image from which the virtual machines will be created.

5. Enter the Number of vms to create, confirm the number of vCPUs and Memory, click Create new accounts, and then click Next



Number of virtual machines to create: 600

Master image: W7SP1-GI1

vCPUs: 1 | 1

Memory: 1536 MB | 1536 MB

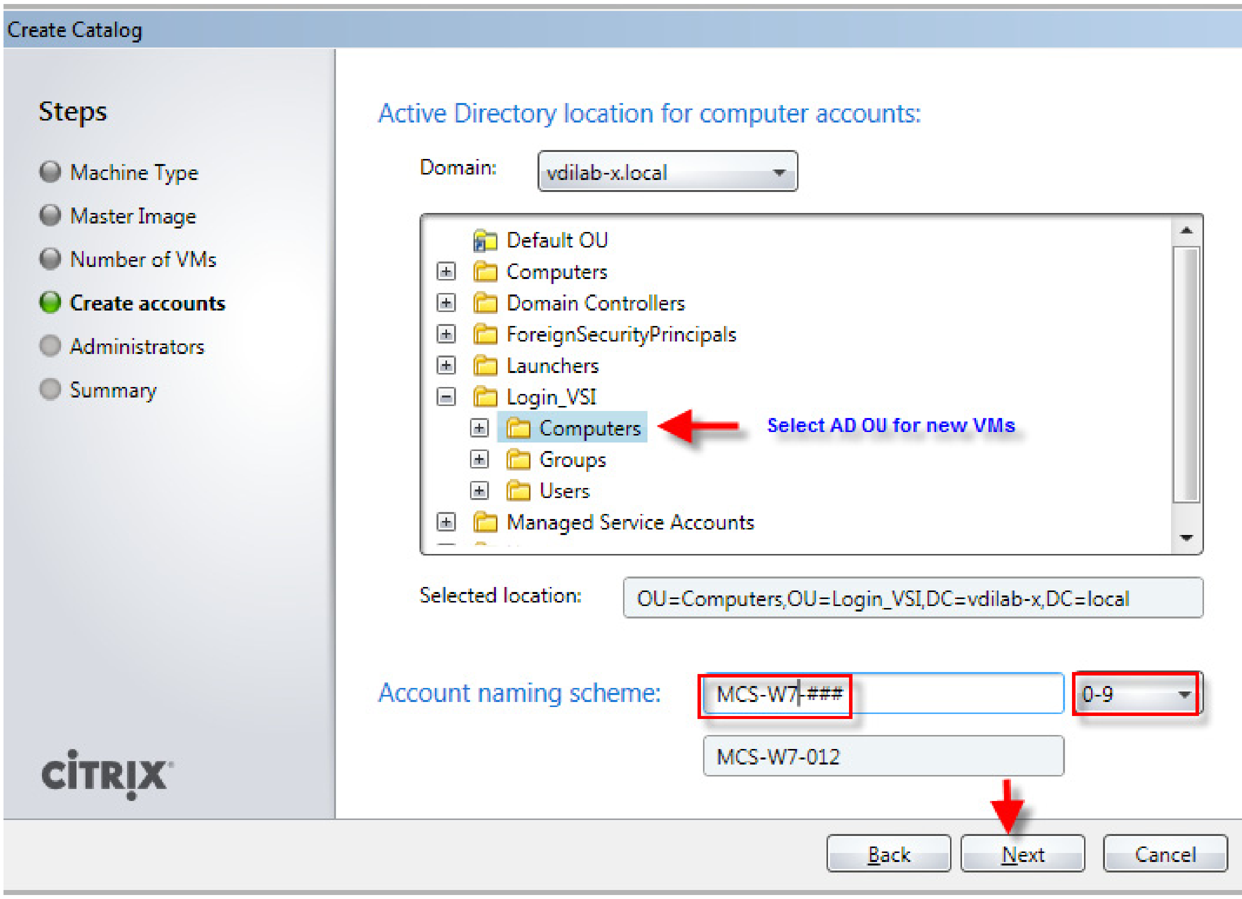
Hard disk: 17 GB | 17 GB

Active Directory computer accounts:

● Create new accounts

○ Use existing accounts

6. Select the Active Directory Domain, the location and a provide naming scheme, then click Next



Active Directory location for computer accounts:

Domain: vdilab-x.local

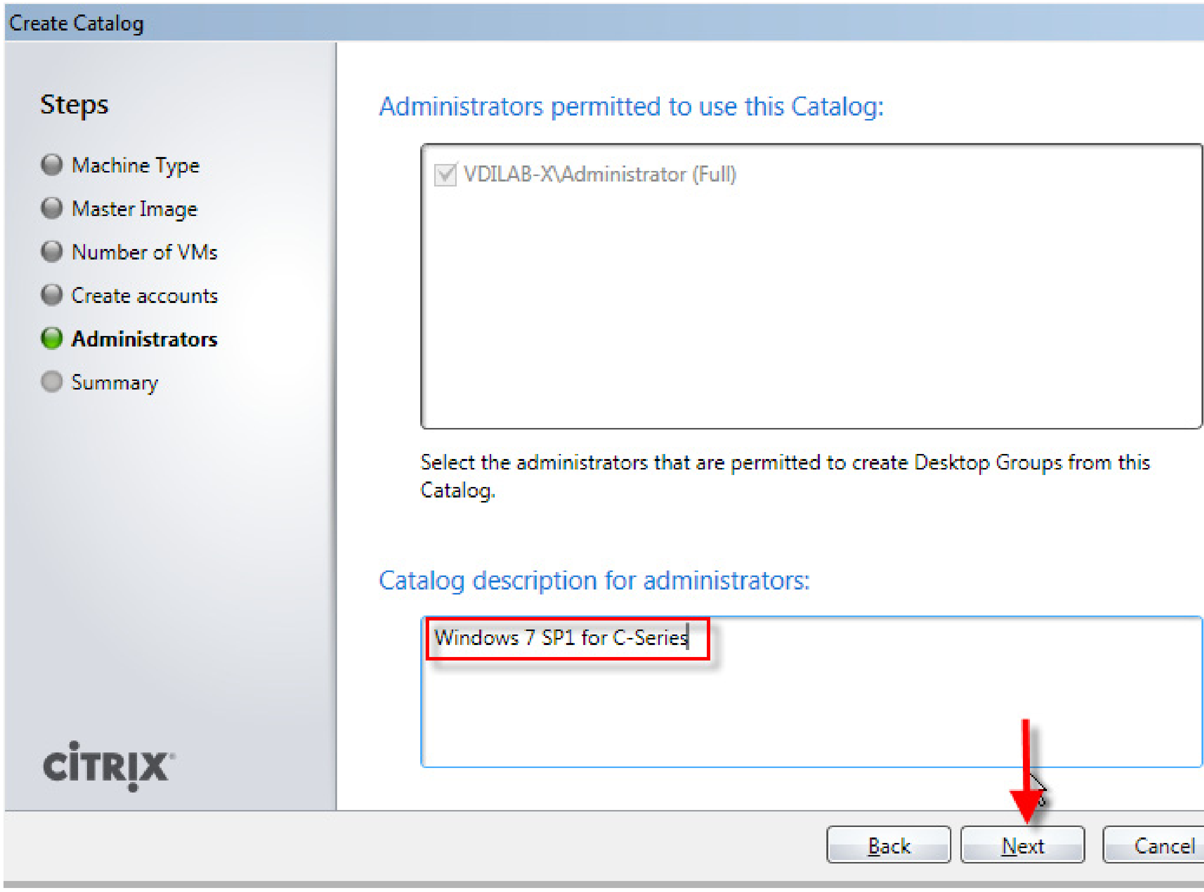
Select AD OU for new VMs

Selected location: OU=Computers,OU=Login_VSI,DC=vdilab-x,DC=local

Account naming scheme: MCS-W7-### 0-9

MCS-W7-012

7. Add an optional description for the Catalog administrators, then click Next



Administrators permitted to use this Catalog:

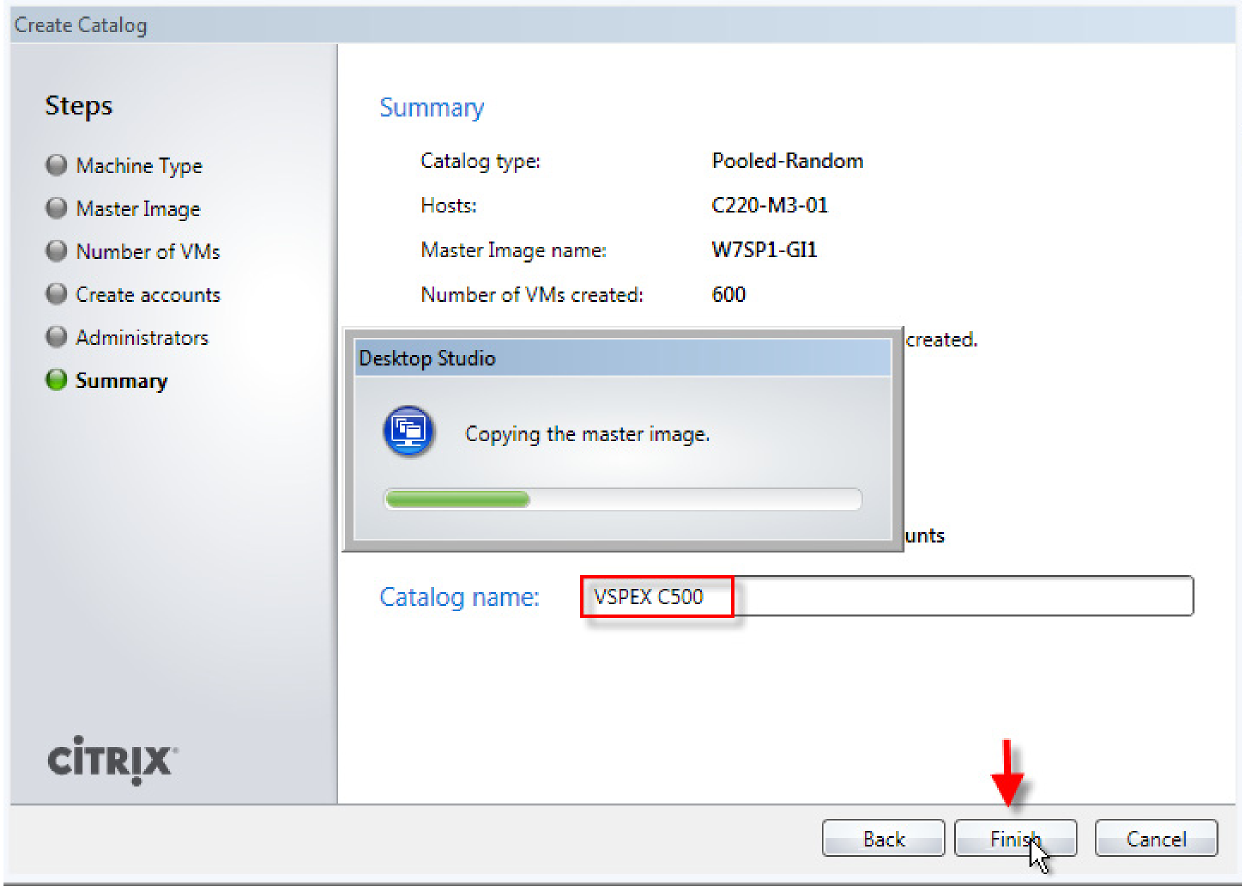
☑ VDILAB-X\Administrator (Full)

Select the administrators that are permitted to create Desktop Groups from this Catalog.

Catalog description for administrators:

Windows 7 SP1 for C-Series

8. Provide a unique Catalog name, then click Next. Machine Creation Services copies the master image and provisions 600 virtual desktops.



Summary

Catalog type: Pooled-Random

Hosts: C220-M3-01

Master Image name: W7SP1-GI1

Number of VMs created: 600

created.

unts

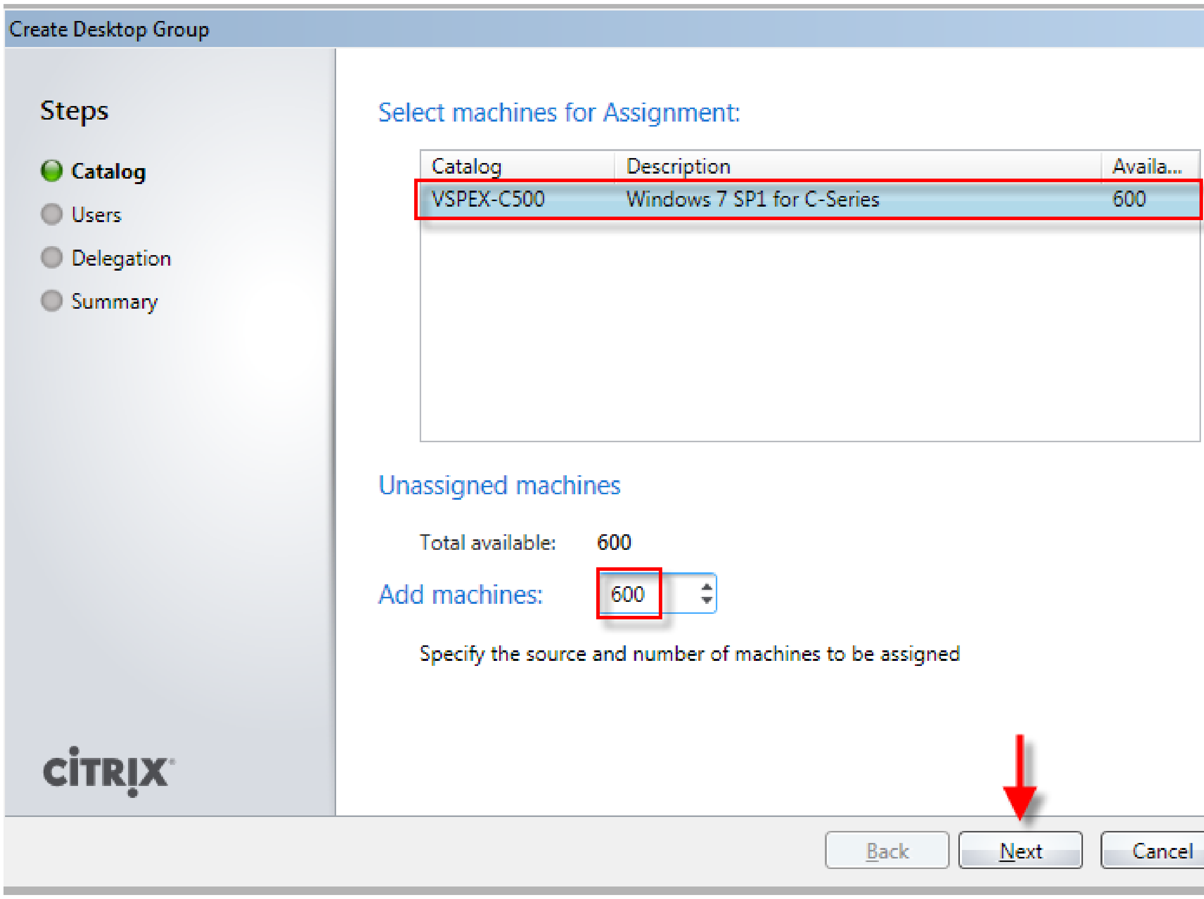
Desktop Studio

Copying the master image.

Catalog name: VSPEX C500

9. After the Catalog and its machines are created, click the Assignments node in the navigation pane, then Create Desktop Group in the action pane.

10. Click the Catalog that was created previously and enter 600 in the Add machines input field, then click Next



Create Desktop Group

Steps

- Catalog
- Users
- Delegation
- Summary

Select machines for Assignment:

Catalog	Description	Availa...
VSPEX-C500	Windows 7 SP1 for C-Series	600

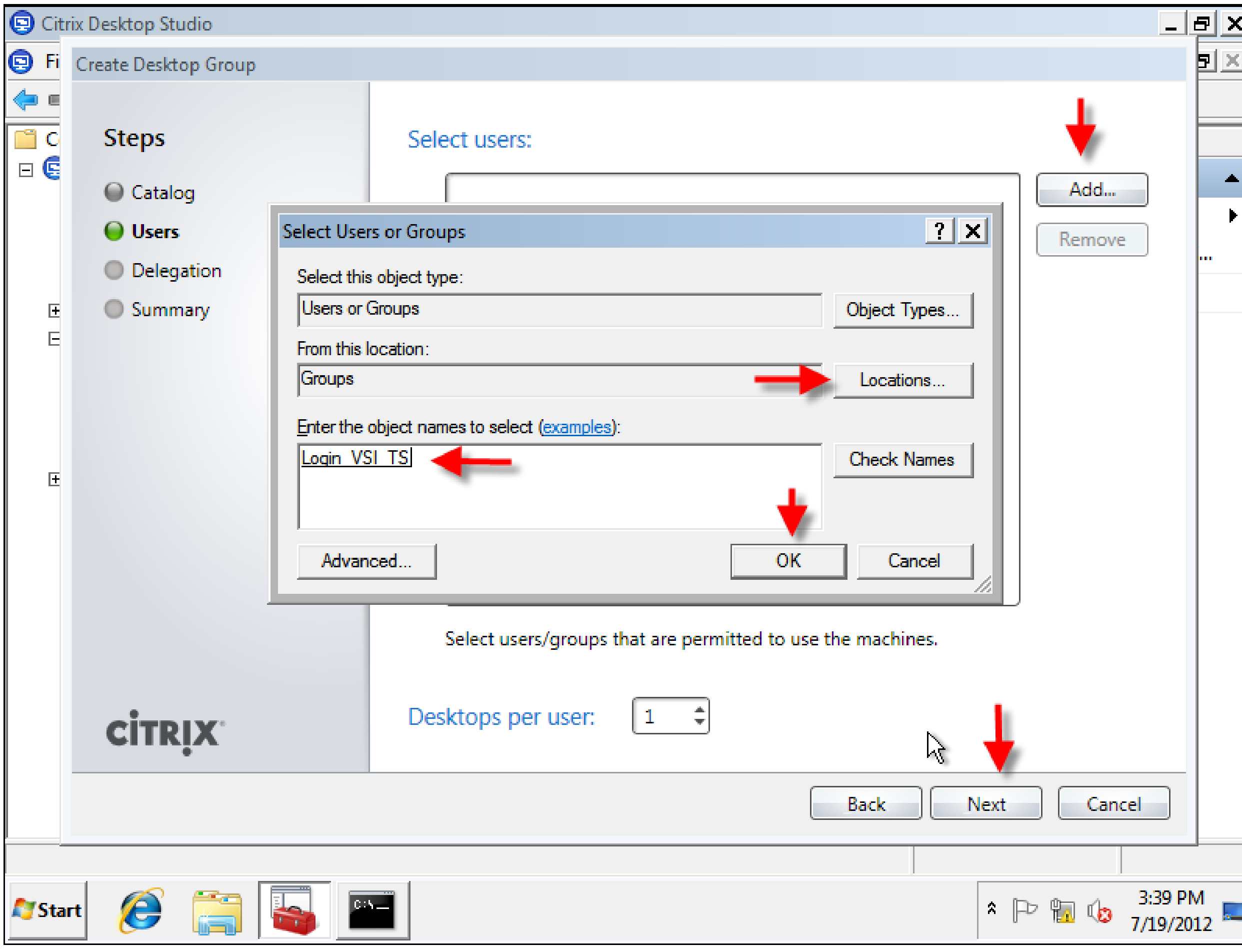
Unassigned machines

Total available: 600

Add machines: 600

Specify the source and number of machines to be assigned

11. Click the Add button, select the users or groups to be authorized to use the Desktop Group and click Ok, select the number of Desktops per user to allocate, then click Next



Select this object type:
Users or Groups

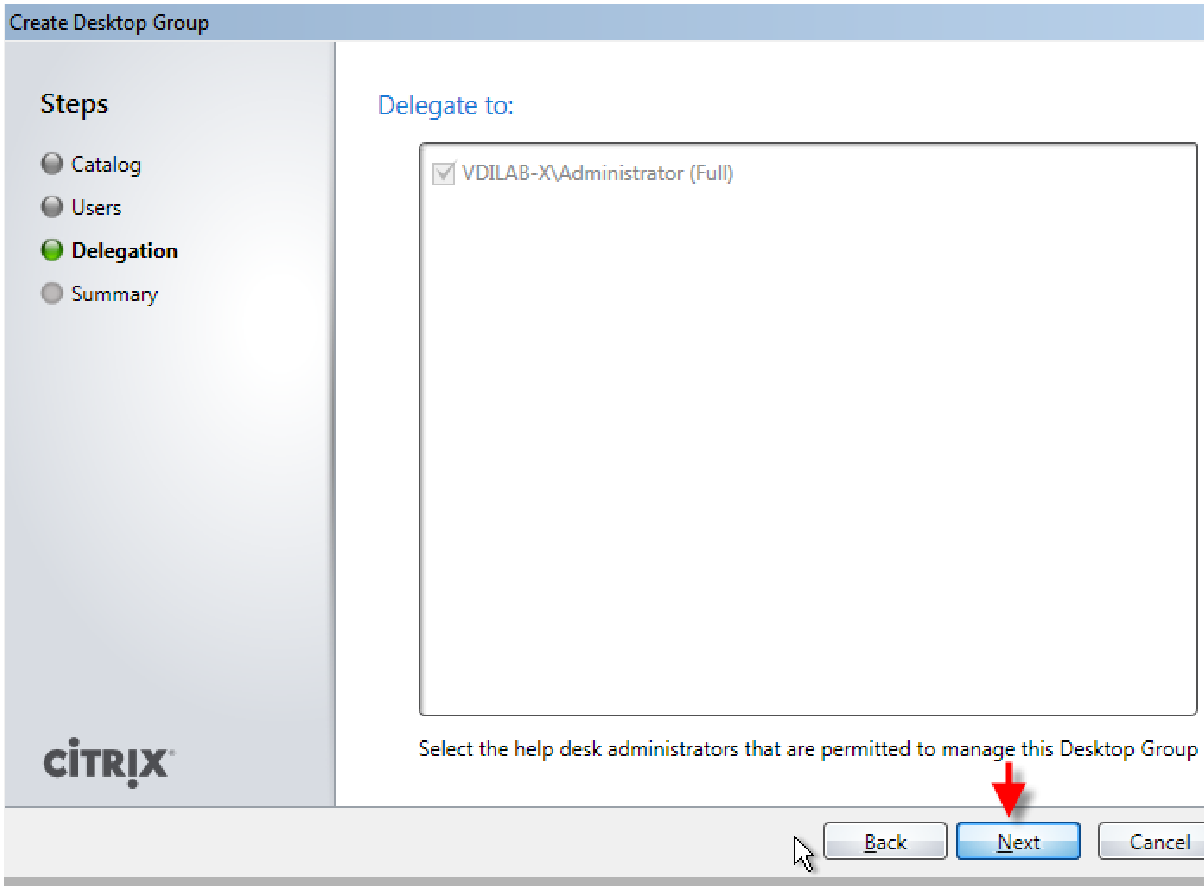
From this location:
Groups

Enter the object names to select (examples):
Login_VSI_TS

Select users/groups that are permitted to use the machines.

Desktops per user: 1

12. Click Next on the Delegate to page. (If there were multiple Administrators created, you could assign one or more as administrators of this Desktop Group)



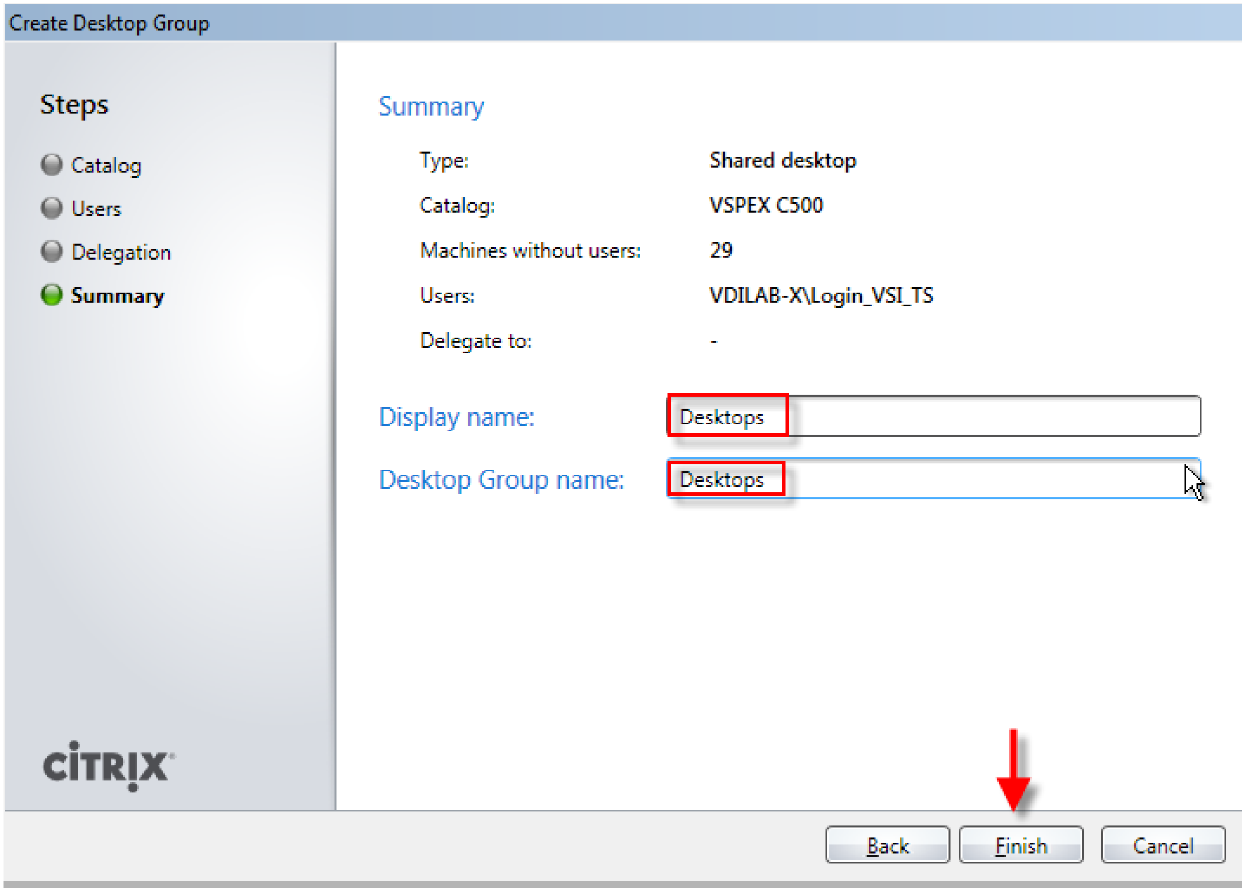
Create Desktop Group

Delegate to:

☑ VDILAB-X\Administrator (Full)

Select the help desk administrators that are permitted to manage this Desktop Group

13. Enter a Display name and a Desktop Group name and click Finish



Create Desktop Group

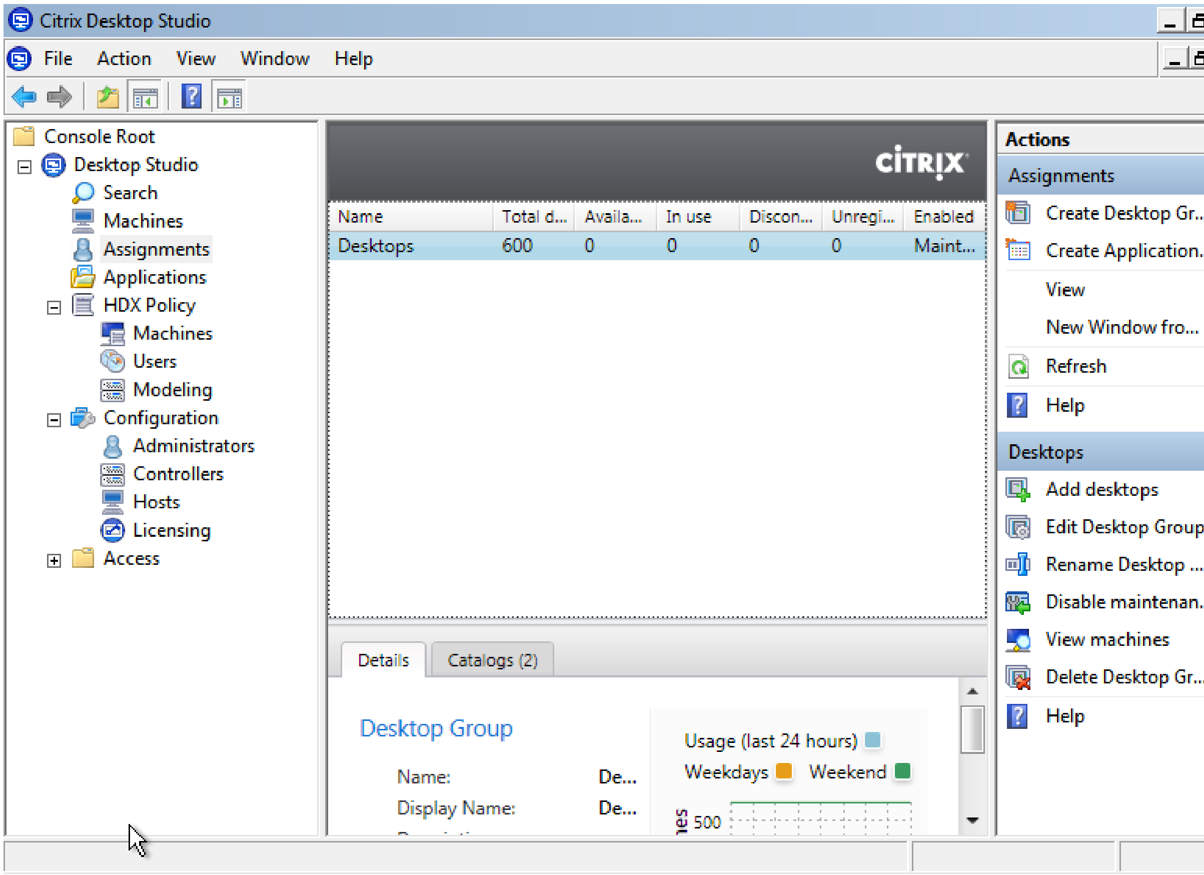
Summary

Type:	Shared desktop
Catalog:	VSPEX C500
Machines without users:	29
Users:	VDILAB-X\Login_VSI_TS
Delegate to:	-

Display name: Desktops

Desktop Group name: Desktops

14. Your Desktop Group is created and you can use the XenDesktop Studio to control the behavior of your XenDesktop environment



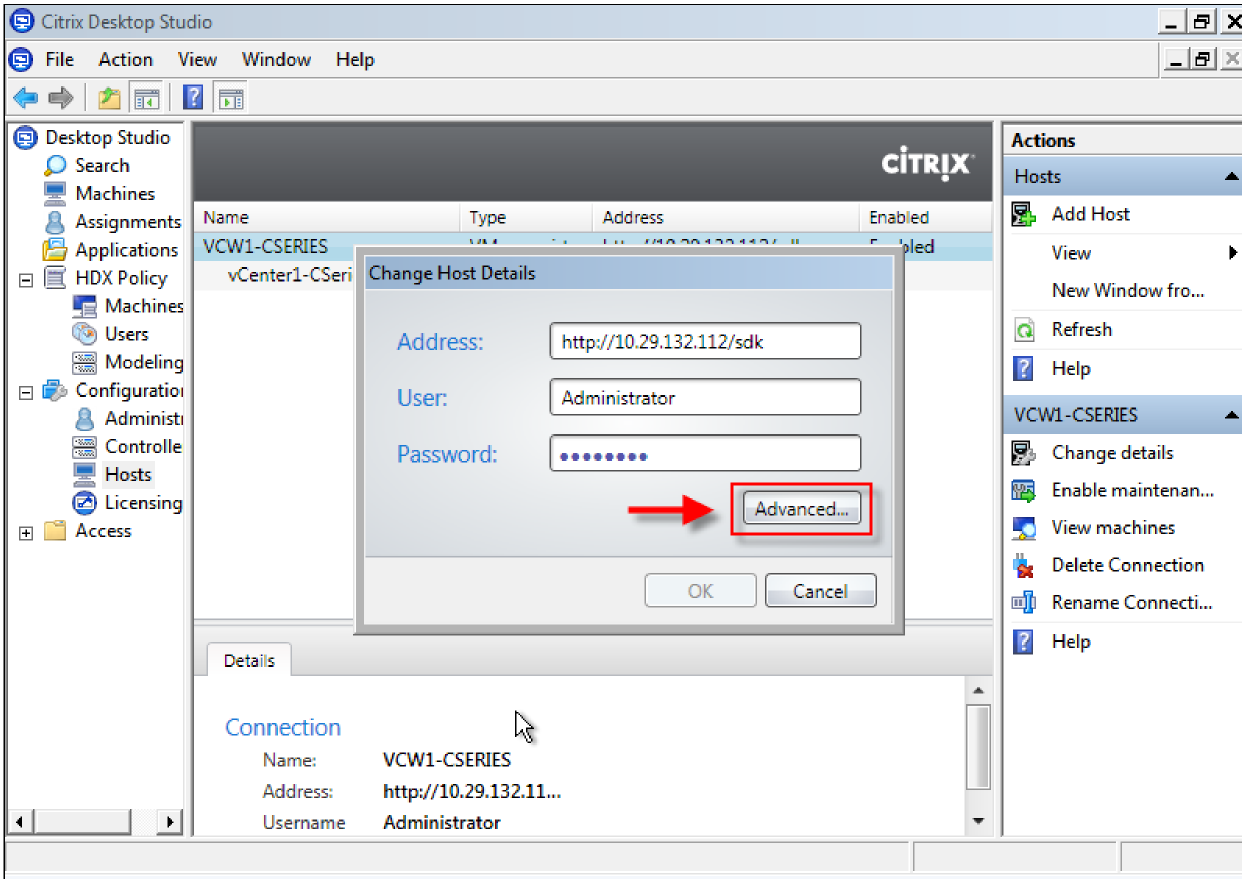
Name	Total d...	Availa...	In use	Discon...	Unregi...	Enabled
Desktops	600	0	0	0	0	Maint...

Desktop Group

Name: De...

Display Name: De...

15. (Optional) You can configure your Hosts launch rate details. Rt-click the Hos in Configuration>Hosts. Select Change Details, Click Advanced



Address: http://10.29.132.112/sdk

User: Administrator

Password: ••••••••

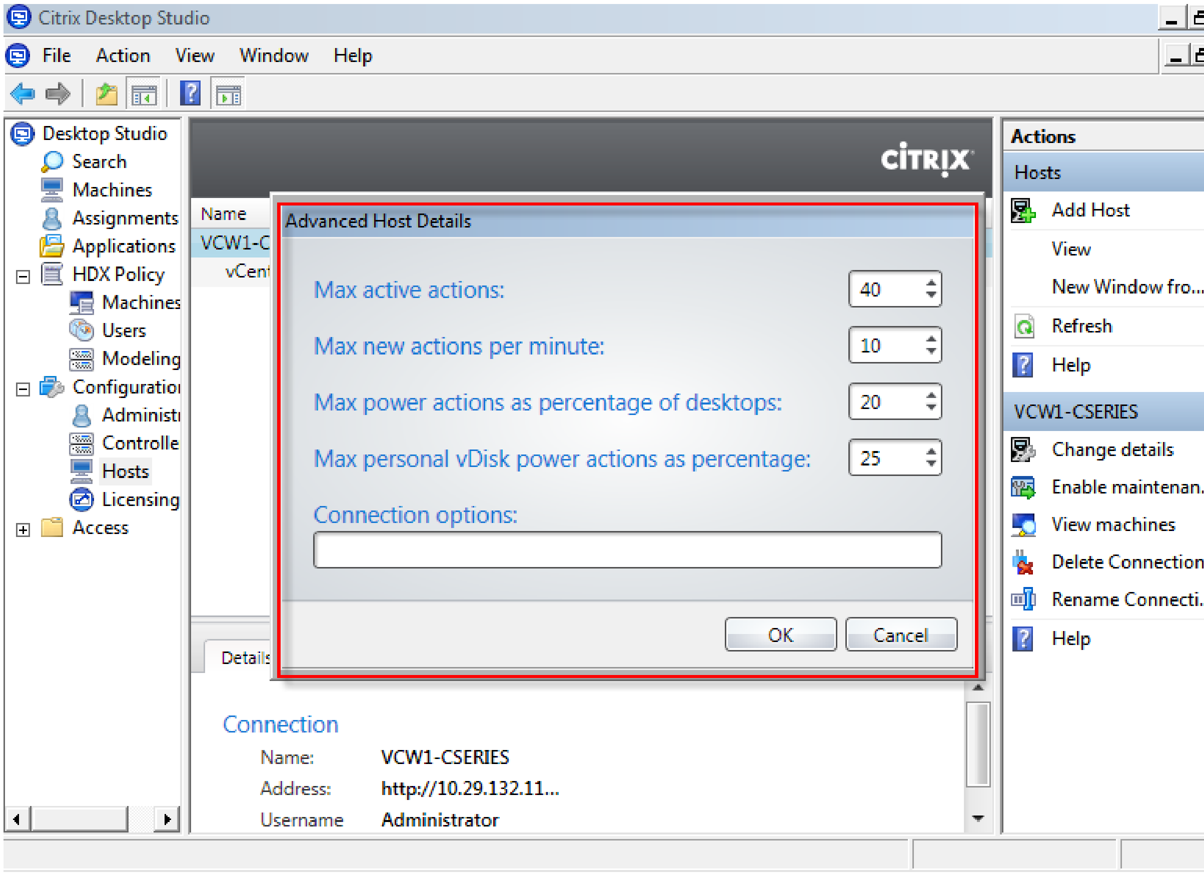
Connection

Name: VCW1-CSERIES

Address: http://10.29.132.11...

Username Administrator

16. (Optional) You can modify how actions are taken by the desktop controller based on these settings using these controls. The default actions will start 10 desktops per minute. In the 600 desktop, 5 UCS C220 M3 VDI host environment, we set the Max new actions per minute to 50 and the Max active actions to 100. Click OK when you are finished.



Advanced Host Details

Max active actions: 40

Max new actions per minute: 10

Max power actions as percentage of desktops: 20

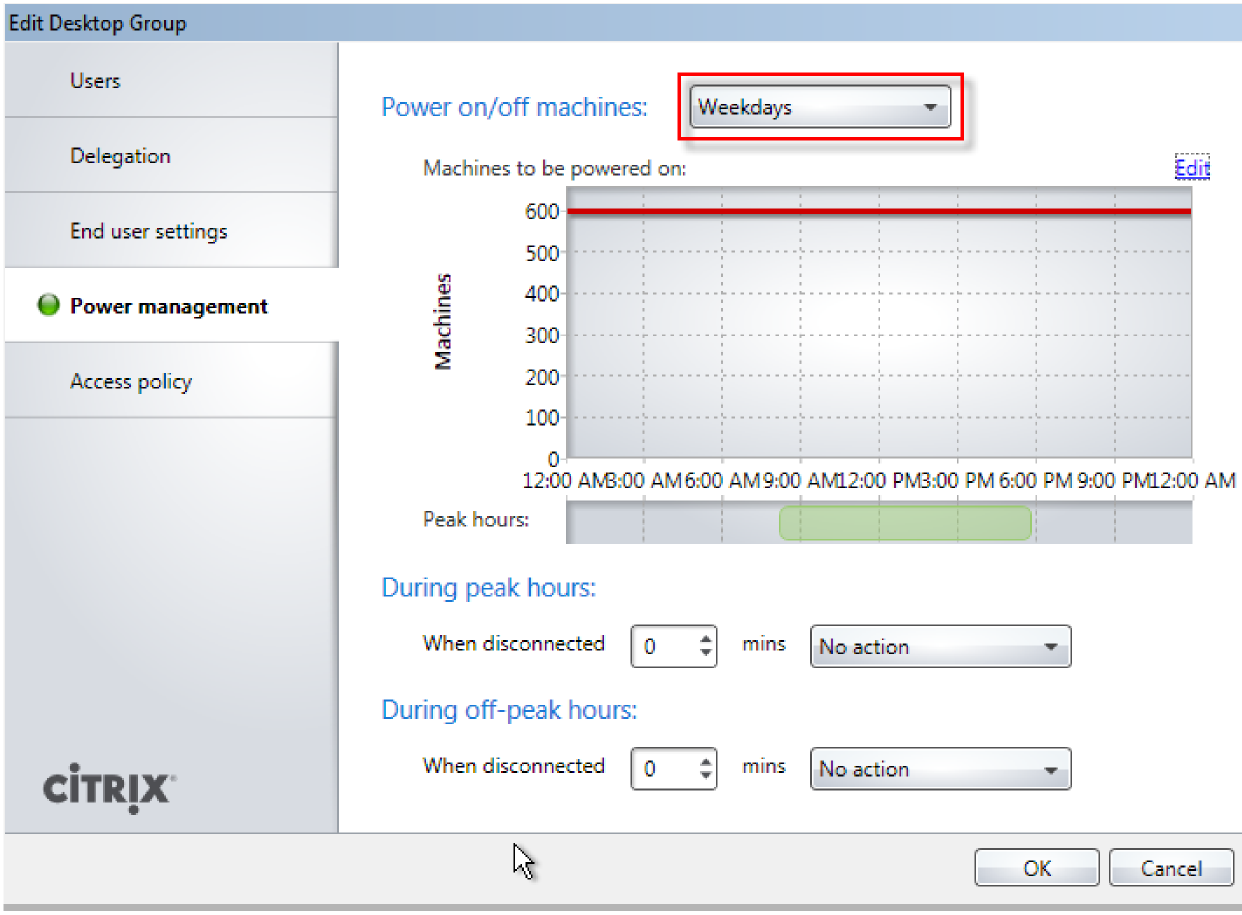
Max personal vDisk power actions as percentage: 25

Connection options:

Connection

Name:	VCW1-CSERIES
Address:	http://10.29.132.11...
Username	Administrator

17. You should adjust the minimum number of desktops available for Weekdays and Weekends. You can do so by right-clicking the Desktop Group, selecting Edit Desktop Group, and click on the Power Management node. In our test environment, we wanted all 600 desktops powered on at all times during working hours.



Power on/off machines: Weekdays

Machines to be powered on:

Peak hours:

During peak hours:

When disconnected 0 mins No action

During off-peak hours:

When disconnected 0 mins No action

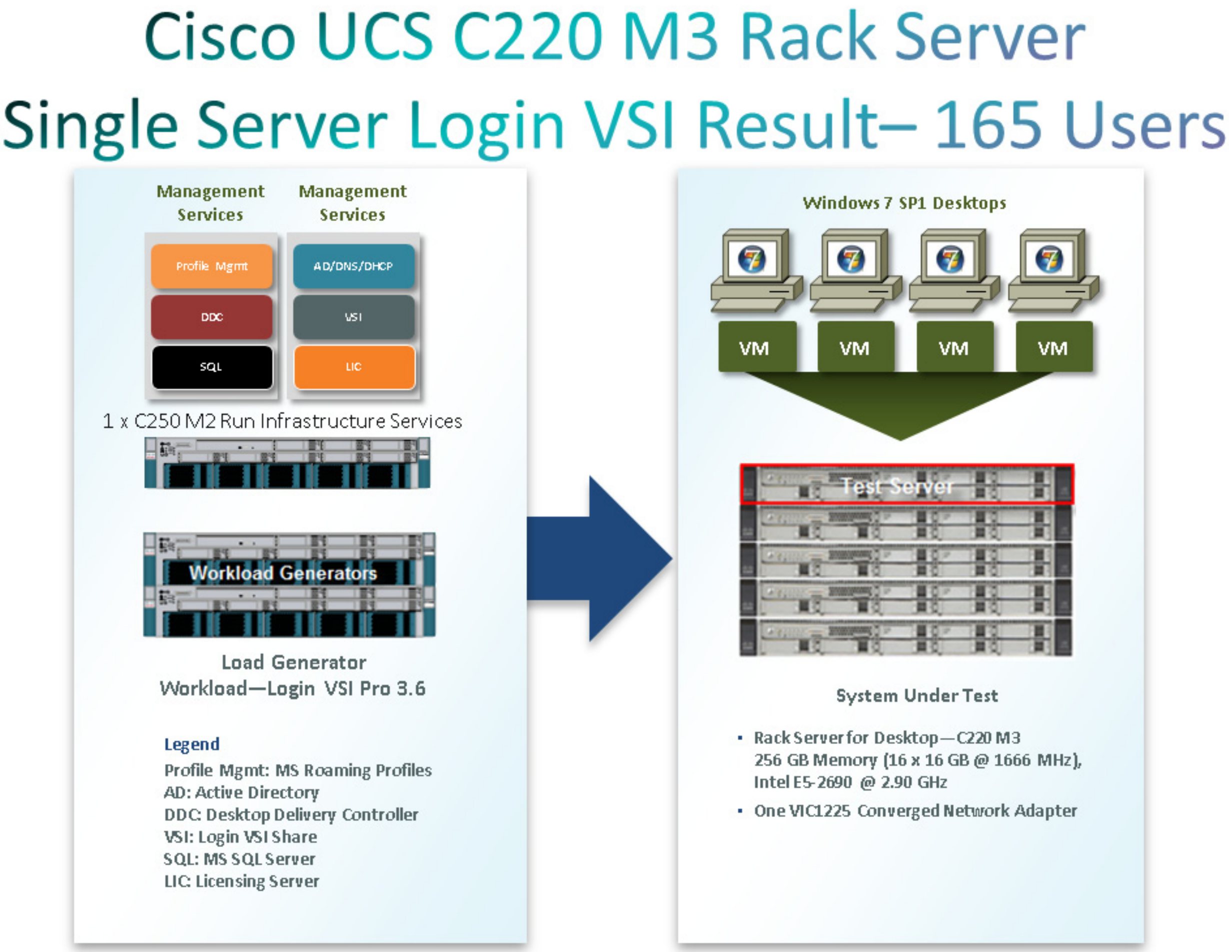
- (Optional) If you do not want your desktops to shut down after a user logs off which is the default behavior, follow the procedure, outlined in CTX127842.

8 Test Setup and Configurations

In this project, we tested a single Cisco UCS C220 M3 Rack-Mount server and five Cisco UCS C220 M3 Rack-Mount servers to illustrate linear scalability in a 600 User configuration with N+1 Server Fault Tolerance.

8.1 Cisco UCS Test Configuration for Single Server Scalability

Figure 19 Cisco UCS C220 M3 Rack-Mount Server for Single Server Scalability



Cisco UCS C220 M3 Rack Server

Single Server Login VSI Result– 165 Users

Legend
Profile Mgmt: MS Roaming Profiles
AD: Active Directory
DDC: Desktop Delivery Controller
VSI: Login VSI Share
SQL: MS SQL Server
LIC: Licensing Server

- Rack Server for Desktop—C220 M3 256 GB Memory (16 x 16 GB @ 1666 MHz), Intel E5-2690 @ 2.90 GHz
- One VIC1225 Converged Network Adapter

Hardware components

- 1 X Cisco UCS C220 M3 (E5-2690 @ 2.90 GHz) blade server with 256GB of memory (16GB X 16 DIMMS @ 1333 MHz) Windows 7 SP1 Virtual Desktop hosts
- 1 X Cisco UCS C250 M2 (Xeon 5690 @ 3.47 GHz) blade servers with 96 GB of memory (4GB X 24 DIMMS @ 1333 MHz) Infrastructure Servers
- 2 X Cisco UCS C250 M2 (Xeon 5690 @ 3.47 GHz) blade servers with 96 GB of memory (4GB X 24 DIMMS @ 1333 MHz) Load Generators
- 1 X M81KR (Palo) Converged Network Adapter/Server (C250 M2)
- 1X VIC1225 Converged Network Adapter/Server (C220 M3)
- 2 X Cisco Fabric Interconnect 6248UPs(Managed FC Variant Only)
- 2 X Cisco Nexus 5548UP Access Switches (Unmanaged NFS Variant Only)
- 2 X Cisco Nexus 2232PP 10 GE Fabric Extenders (Managed FC Variant Only)

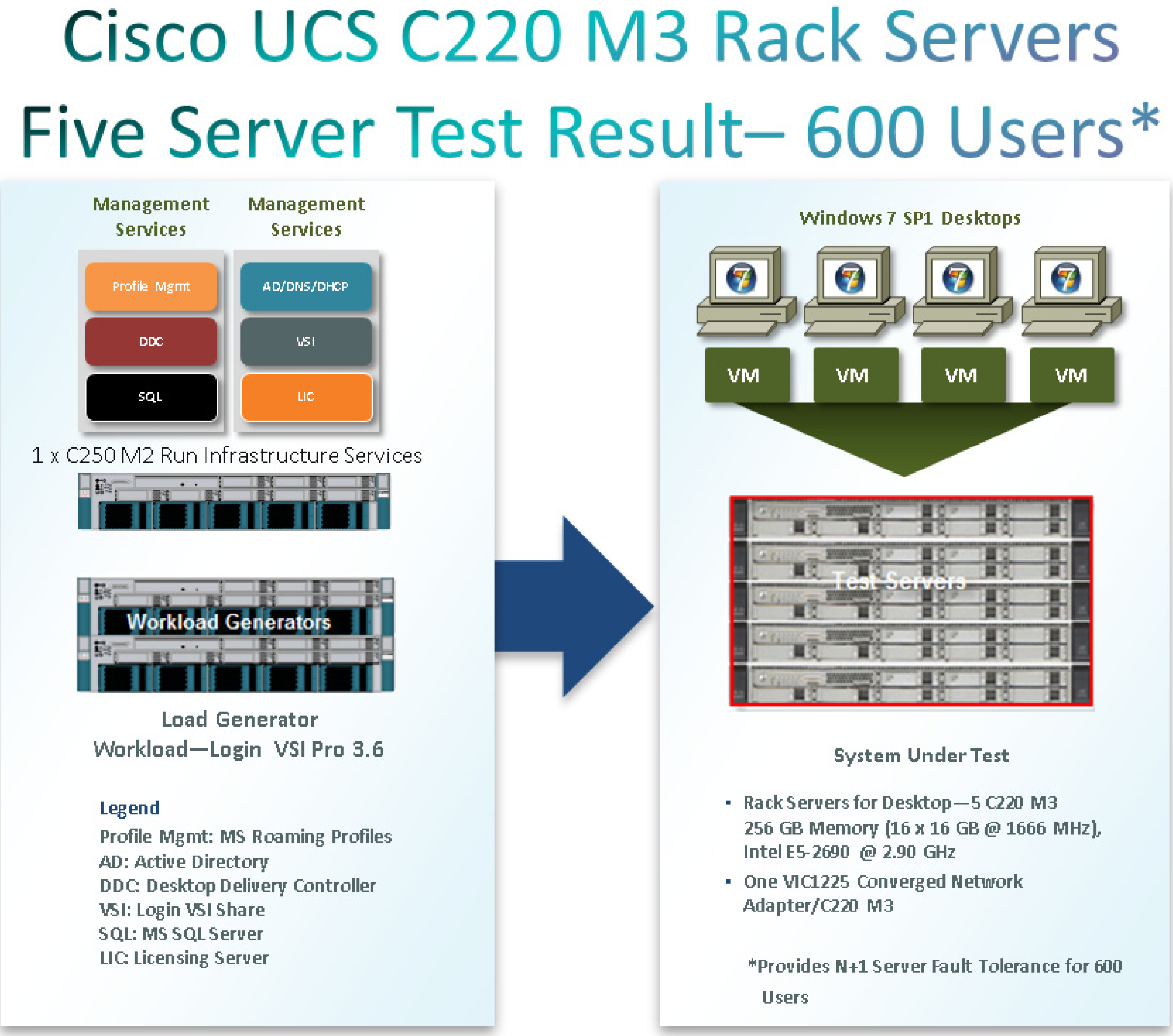
- 1 X EMC VNX5300 System storage array, two controllers, four Datamovers, 2 x dual port 8GB FC cards, 4 x dual port 10 GbE cards, 2 x 100GB Flash Drives for EMC Fast Cache, 10 x 600GB SAS drives for XenDesktop MCS disks, 5 x 600GB SAS Drives for Infrastructure and Boot LUNs, 1 x 100GB Flash Drive for hot spare and 1 x 600GB SAS drives for hot spare

Software components

- Cisco UCS firmware 2.1(1a) (Managed FC Variant Only)
- Cisco UCS C220 M3 firmware 1.4.7b
- VMware ESXi 5.0 Update 1 for VDI Hosts
- XenDesktop 5.6 Feature Pack 1
- Windows 7 SP1 32 bit, 1vCPU, 1.5 GB of memory, 17 GB/VM

8.2 Cisco UCS Configuration for Five Server Test

Figure 20 600 Desktop Test Configuration-5 x Cisco UCS C220 M3 Rack-Mount Servers



Cisco UCS C220 M3 Rack Servers

Five Server Test Result– 600 Users*

Legend
Profile Mgmt: MS Roaming Profiles
AD: Active Directory
DDC: Desktop Delivery Controller
VSI: Login VSI Share
SQL: MS SQL Server
LIC: Licensing Server

- Rack Servers for Desktop—5 C220 M3 256 GB Memory (16 x 16 GB @ 1666 MHz), Intel E5-2690 @ 2.90 GHz
- One VIC1225 Converged Network Adapter/C220 M3

*Provides N+1 Server Fault Tolerance for 600 Users

Hardware components

- 5 X Cisco UCS C220 M3 (E5-2690 @ 2.90 GHz) blade server with 256GB of memory (16GB X 16 DIMMS @ 1333 MHz) Windows 7 SP1 Virtual Desktop hosts
- 1 X Cisco UCS C250 M2 (Xeon 5690 @ 3.47 GHz) blade servers with 96 GB of memory (4GB X 24 DIMMS @ 1333 MHz) Infrastructure Servers
- 2 X Cisco UCS C250 M2 (Xeon 5690 @ 3.47 GHz) blade servers with 96 GB of memory (4GB X 24 DIMMS @ 1333 MHz) Load Generators
- 1 X M81KR (Palo) Converged Network Adapter/Server (C250 M2)
- 1X VIC1225 Converged Network Adapter/Server (C220 M3)
- 2 X Cisco Fabric Interconnect 6248UPs (Managed FC Variant Only)
- 2 X Cisco Nexus 5548UP Access Switches (Unmanaged NFS Variant Only)
- 2 X Cisco Nexus 2232PP 10 GE Fabric Extenders (Managed FC Variant Only)
- 1 X EMC VNX5300 System storage array, two controllers, four Datamovers, 2 x dual port 8GB FC cards, 4 x dual port 10 GbE cards, 2 x 100GB Flash Drives for EMC Fast Cache, 10 x 600GB SAS drives for XenDesktop MCS disks, 5 x 600GB SAS Drives for Infrastructure and Boot LUNs, 1 x 100GB Flash Drive for hot spare and 1 x 600GB SAS drives for hot spare

Software components

- Cisco UCS firmware 2.1(1a) (Managed FC Variant Only)
- Cisco UCS C220 M3 firmware 1.4.7b
- VMware ESXi 5.0 Update 1 for VDI Hosts
- XenDesktop 5.6 Feature Pack 1
- Windows 7 SP1 32 bit, 1vCPU, 1.5 GB of memory, 17 GB/VM

8.3 Testing Methodology and Success Criteria

All validation testing was conducted on-site within the Cisco Labs in San Jose, CA.

The testing results focused on the entire process of the virtual desktop lifecycle by capturing metrics during the desktop boot-up, user logon and virtual desktop acquisition (also referred to as ramp-up,) user workload execution (also referred to as steady state), and user logoff for the Hosted VDI model under test.

Test metrics were gathered from the hypervisor, virtual desktop, storage, and load generation software to assess the overall success of an individual test cycle. Each test cycle was not considered passing unless all of the planned test users completed the ramp-up and steady state phases (described below) and unless all metrics were within the permissible thresholds as noted as success criteria.

Three successfully completed test cycles were conducted for each hardware configuration and results were found to be relatively consistent from one test to the next.

8.3.1 Load Generation

Within each test environment, load generators were utilized to put demand on the system to simulate multiple users accessing the XenDesktop 5.6 environment and executing a typical end-user workflow. To generate load within the environment, an auxiliary software application was required to generate the end user connection to the XenDesktop environment, to provide unique user credentials, to initiate the workload, and to evaluate the end user experience.

In the Hosted VDI test environment, sessions launchers were used simulate multiple users making a direct connection to XenDesktop 5.6 via a Citrix HDX protocol connection.

8.3.2 User Workload SimulationLoginVSI From Login Consultants

One of the most critical factors of validating a XenDesktop deployment is identifying a real-world user workload that is easy for customers to replicate and standardized across platforms to allow customers to realistically test the impact of a variety of worker tasks. To accurately represent a real-world user workload, a third-party tool from Login Consultants was used throughout the Hosted VDI testing.

The tool has the benefit of taking measurements of the in-session response time, providing an objective way to measure the expected user experience for individual desktop throughout large scale testing, including login storms.

The Virtual Session Indexer (Login Consultants' Login VSI 3.6) methodology, designed for benchmarking Server Based Computing (SBC) and Virtual Desktop Infrastructure (VDI) environments is completely platform and protocol independent and hence allows customers to easily replicate the testing results in their environment. **NOTE:** In this testing, we utilized the tool to benchmark our VDI environment only.

Login VSI calculates an index based on the amount of simultaneous sessions that can be run on a single machine.

Login VSI simulates a medium workload user (also known as knowledge worker) running generic applications such as: Microsoft Office 2007 or 2010, Internet Explorer 8 including a Flash video applet and Adobe Acrobat Reader (Note: For the purposes of this test, applications were installed locally, not streamed nor hosted on XenApp).

Like real users, the scripted Login VSI session will leave multiple applications open at the same time. The medium workload is the default workload in Login VSI and was used for this testing. This workload emulated a medium knowledge working using Office, IE, printing and PDF viewing.

- When a session has been started the medium workload will repeat every 12 minutes.
- During each loop the response time is measured every 2 minutes.
- The medium workload opens up to 5 apps simultaneously.
- The type rate is 160ms for each character.
- Approximately 2 minutes of idle time is included to simulate real-world users.

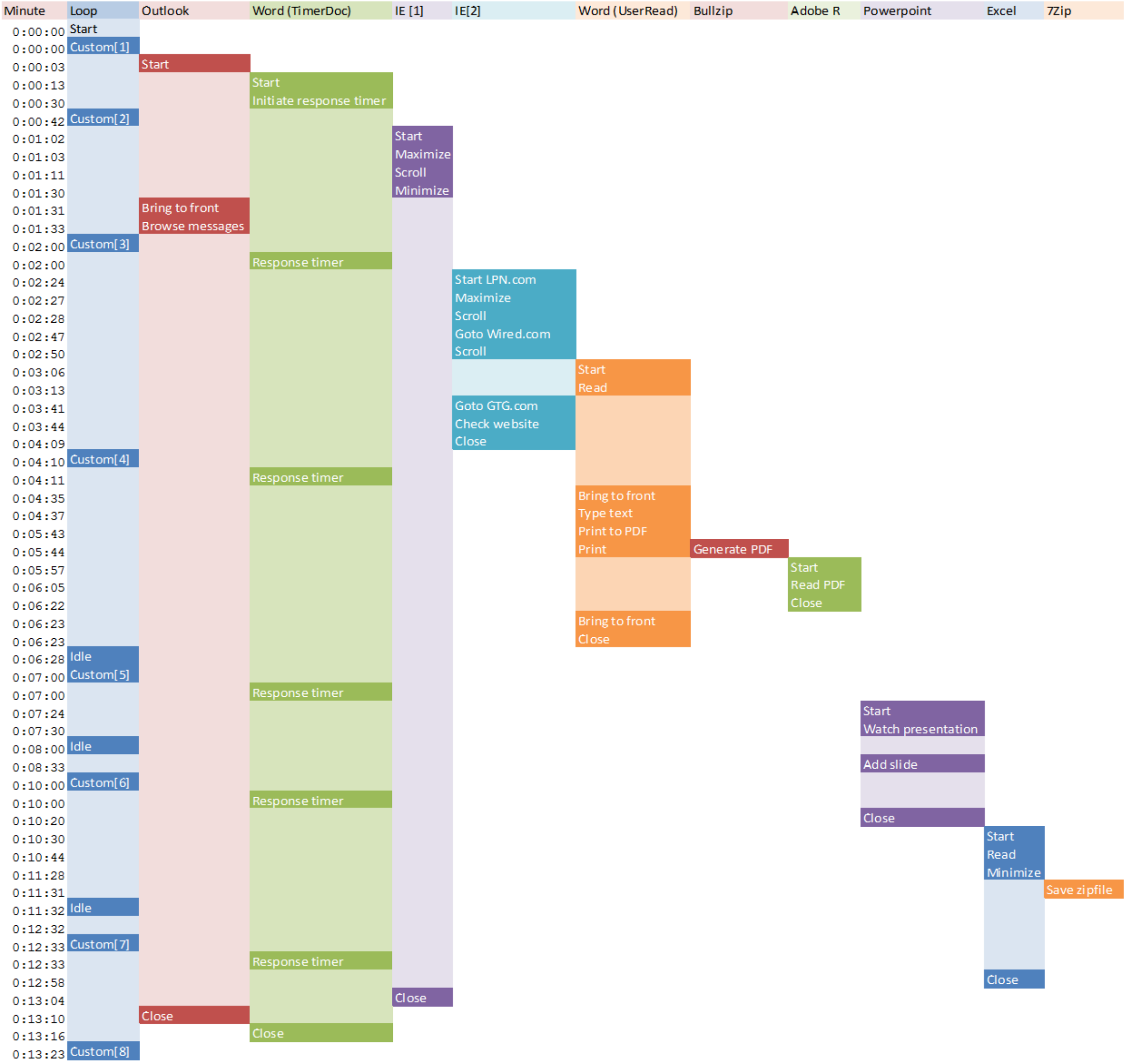
Each loop will open and use:

- Outlook 2007/2010, browse 10 messages.
- Internet Explorer, one instance is left open (BBC.co.uk), one instance is browsed to Wired.com, Lonelyplanet.com and heavy
- 480 p Flash application gettheglass.com.
- Word 2007/2010, one instance to measure response time, one instance to review and edit document.
- Bullzip PDF Printer & Acrobat Reader, the word document is printed and reviewed to PDF.

- Excel 2007/2010, a very large randomized sheet is opened.
- PowerPoint 2007/2010, a presentation is reviewed and edited.
- 7-zip: using the command line version the output of the session is zipped.

A graphical representation of the medium workload is shown below.

Graphical overview



Minute	Loop	Outlook	Word (TimerDoc)	IE [1]	IE[2]	Word (UserRead)	Bullzip	Adobe R	Powerpoint	Excel	7Zip
0:00:00	Start										
0:00:00	Custom[1]										
0:00:03		Start									
0:00:13			Start								
0:00:30			Initiate response timer								
0:00:42	Custom[2]										
0:01:02				Start							
0:01:03				Maximize							
0:01:11				Scroll							
0:01:30				Minimize							
0:01:31		Bring to front									
0:01:33		Browse messages									
0:02:00	Custom[3]										
0:02:00			Response timer								
0:02:24					Start LPN.com						
0:02:27					Maximize						
0:02:28					Scroll						
0:02:47					Goto Wired.com						
0:02:50					Scroll						
0:03:06						Start					
0:03:13						Read					
0:03:41					Goto GTG.com						
0:03:44					Check website						
0:04:09					Close						
0:04:10	Custom[4]										
0:04:11			Response timer								
0:04:35						Bring to front					
0:04:37						Type text					
0:05:43						Print to PDF					
0:05:44						Print	Generate PDF				
0:05:57								Start			
0:06:05								Read PDF			
0:06:22								Close			
0:06:23						Bring to front					
0:06:23						Close					
0:06:28	Idle										
0:07:00	Custom[5]										
0:07:00			Response timer								
0:07:24									Start		
0:07:30									Watch presentation		
0:08:00	Idle										
0:08:33									Add slide		
0:10:00	Custom[6]										
0:10:00			Response timer								
0:10:20									Close		
0:10:30										Start	
0:10:44										Read	
0:11:28										Minimize	
0:11:31											Save zipfile
0:11:32	Idle										
0:12:32											
0:12:33	Custom[7]										
0:12:33			Response timer								
0:12:58										Close	
0:13:04				Close							
0:13:10		Close									
0:13:16			Close								
0:13:23	Custom[8]										

You can obtain additional information on Login VSI from http://www.loginvsi.com.

8.3.3 Testing Procedure

The following protocol was used for each test cycle in this study to insure consistent results.

8.3.3.1 Pre-Test Setup for Single and Multi-Blade Testing

All virtual machines were shut down utilizing the Citrix XenDesktop 5.6 Desktop Studio.

All Launchers for the test were shut down. They were then restarted in groups of 10 each minute until the required number of launchers was running with the Login VSI Agent at a “waiting for test to start” state.

All VMware ESXi 5.0 VDI host blades to be tested were restarted prior to each test cycle.

8.3.3.2 Test Run Protocol

To simulate severe, real-world environments, Cisco requires the log-on and start-work sequence, known as Ramp Up, to complete in 30 minutes. Additionally, we require all sessions started, whether 195 single server users or 600 full scale test users to become active within 2 minutes after the last session is launched.

In addition, Cisco requires that the Login VSI Parallel Launching method is used for all single server and scale testing. This assures that our tests represent real-world scenarios. (**NOTE:** The Login VSI Sequential Launching method allows the CPU, storage and network components to rest between each logins. This does not produce results that are consistent with the real-world scenarios that our Customers run in.)

For each of the three consecutive runs on single server (195 User) and 4 and 5 server (500 and 600 User) tests, the same process was followed:

1. Time 0:00:00 Started ESXtop Logging on the following systems:
   oVDI Host Blades used in test run

   oDDCs used in test run

   oProfile Server(s) used in test run

   oSQL Server(s) used in test run

   o3 Launcher VMs

1. Time 0:00:10 Started EMC Basic Performance Logging on SPs
2. Time 0:00:15 Started EMC NFS Performance Logging on Datamovers (Unmanaged NFS Variant Only)
3. Time 0:05 Take 195, 500 or 600 desktops out of maintenance mode on XenDesktop Studio
4. Time 0:06 First machines boot
5. Time 0:26 195, 500 or 600 desktops booted on 1 or 5 servers
6. Time 0:28 195, 500 or 600 desktops available on 1 or 5 servers
7. Time 1:28 Start Login VSI 3.6 Test with 195, 500 or 600 desktops utilizing 7, 17 or 20 Launchers
8. Time 1:58 195, 500 or 600 sessions launched
9. Time 2:00 195, 500 or 600 sessions active
10. Time 2:15 Login VSI Test Ends
11. Time 2:30 195, 500 or 600 sessions logged off
12. Time 2:35 All logging terminated.

8.3.4 Success Criteria

There were multiple metrics that were captured during each test run, but the success criteria for considering a single test run as pass or fail was based on the key metric, VSI Max. The Login VSI Max evaluates the user response time during increasing user load and assesses the successful start-to-finish execution of all the initiated virtual desktop sessions.

8.3.4.1 Login VSI Max

VSI Max represents the maximum number of users the environment can handle before serious performance degradation occurs. VSI Max is calculated based on the response times of individual users as indicated during the workload execution. The user response time has a threshold of 4000ms and all users response times are expected to be less than 4000ms in order to assume that the user interaction with the virtual desktop is at a functional level. VSI Max is reached when the response times reaches or exceeds 4000ms for 6 consecutive occurrences. If VSI Max is reached, that indicates the point at which the user experience has significantly degraded. The response time is generally an indicator of the host CPU resources, but this specific method of analyzing the user experience provides an objective method of comparison that can be aligned to host CPU performance.

Note In the prior version of Login VSI, the threshold for response time was 2000ms. The workloads and the analysis have been upgraded in Login VSI 3 to make the testing more aligned to real-world use. In the medium workload in Login VSI 3.0, a CPU intensive 480p flash movie is incorporated in each test loop. In general, the redesigned workload would result in an approximate 20% decrease in the number of users passing the test versus Login VSI 2.0 on the same server and storage hardware.

8.3.4.2 Calculating VSIMax

Typically the desktop workload is scripted in a 12-14 minute loop when a simulated Login VSI user is logged on. After the loop is finished it will restart automatically. Within each loop the response times of seven specific operations is measured in a regular interval: six times in within each loop. The response times if these seven operations are used to establish ***VSImax***. The seven operations from which the response times are measured are:

- Copy new document from the document pool in the home drive
  - This operation will refresh a new document to be used for measuring the response time. This activity is mostly a file-system operation.
- Starting Microsoft Word with a document
  - This operation will measure the responsiveness of the Operating System and the file system. Microsoft Word is started and loaded into memory, also the new document is automatically loaded into Microsoft Word. When the disk I/O is extensive or even saturated, this will impact the file open dialogue considerably.
- Starting the “File Open” dialogue
  - This operation is handled for small part by Word and a large part by the operating system. The file open dialogue uses generic subsystems and interface components of the OS. The OS provides the contents of this dialogue.
- Starting “Notepad”
  - This operation is handled by the OS (loading and initiating notepad.exe) and by the Notepad.exe itself through execution. This operation seems instant from an end-user’s point of view.
- Starting the “Print” dialogue

  - This operation is handled for a large part by the OS subsystems, as the print dialogue is provided by the OS. This dialogue loads the print-subsystem and the drivers of the selected printer. As a result, this dialogue is also dependent on disk performance.
- Starting the “Search and Replace” dialogue \
  - This operation is handled within the application completely; the presentation of the dialogue is almost instant. Serious bottlenecks on application level will impact the speed of this dialogue.
- Compress the document into a zip file with 7-zip command line
  - This operation is handled by the command line version of 7-zip. The compression will very briefly spike CPU and disk I/O.

These measured operations with Login VSI do hit considerably different subsystems such as CPU (user and kernel), Memory, Disk, the OS in general, the application itself, print, GDI, etc. These operations are specifically short by nature. When such operations are consistently long: the system is saturated because of excessive queuing on any kind of resource. As a result, the average response times will then escalate. This effect is clearly visible to end-users. When such operations consistently consume multiple seconds the user will regard the system as slow and unresponsive.

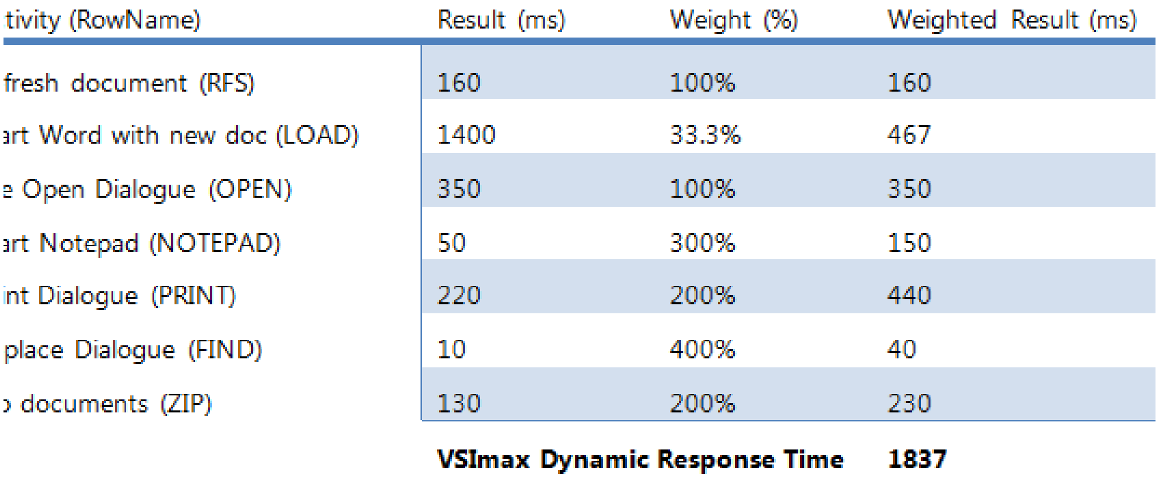
With Login VSI 3.0 and later it is now possible to choose between ‘VSImax Classic’ and 'VSImax Dynamic’ results analysis. For these tests, we utilized VSImax Dynamic analysis.

8.3.4.3 VSIMax Dynamic

VSImax Dynamic is calculated when the response times are consistently above a certain threshold. However, this threshold is now dynamically calculated on the baseline response time of the test. The following individual measurements are weighted to better support this approach:

- Copy new doc from the document pool in the home drive: 100%
- Microsoft Word with a document: 33.3%
- Starting the “File Open” dialogue: 100%
- Starting “Notepad”: 300%
- Starting the “Print” dialogue: 200%
- Starting the “Search and Replace” dialogue: 400%
- Compress the document into a zip file with 7-zip command line 200%

A sample of the VSImax Dynamic response time calculation is displayed below:



tivity (RowName)	Result (ms)	Weight (%)	Weighted Result (ms)
fresh document (RFS)	160	100%	160
art Word with new doc (LOAD)	1400	33.3%	467
e Open Dialogue (OPEN)	350	100%	350
art Notepad (NOTEPAD)	50	300%	150
int Dialogue (PRINT)	220	200%	440
place Dialogue (FIND)	10	400%	40
p documents (ZIP)	130	200%	230
	VSImax Dynamic Response Time		**1837**

Then the average VSImax response time is calculated based on the amount of active Login VSI users logged on to the system. For this the average VSImax response times need to consistently higher than a dynamically calculated threshold.

To determine this dynamic threshold, first the average baseline response time is calculated. This is done by averaging the baseline response time of the first 15 Login VSI users on the system.

The formula for the dynamic threshold is: Avg. Baseline Response Time x 125% + 3000. As a result, when the baseline response time is 1800, the VSImax threshold will now be 1800 x 125% + 3000 = 5250ms.

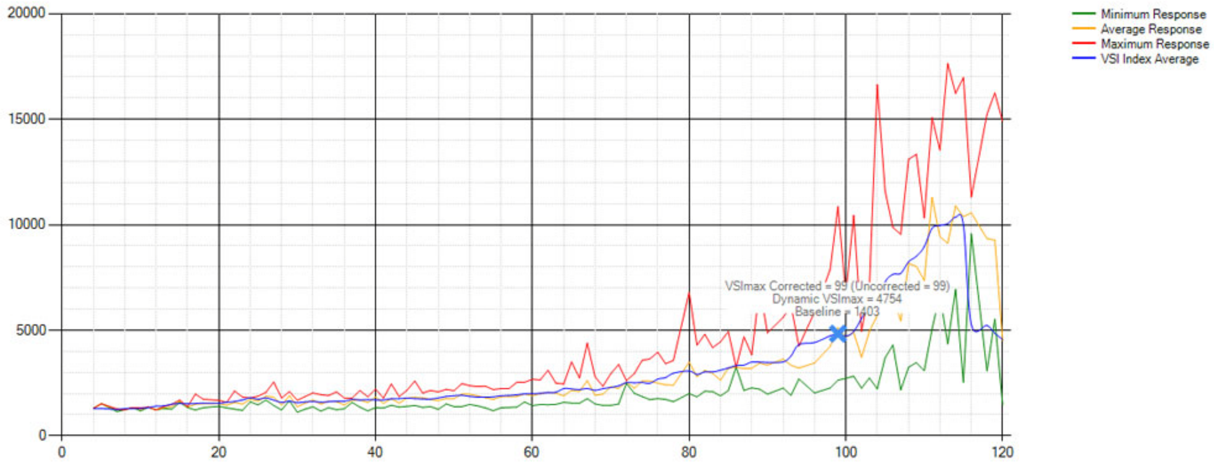
Especially when application virtualization is used, the baseline response time can wildly vary per vendor and streaming strategy. Therefore it is recommend to use VSImax Dynamic when comparisons are made with application virtualization or anti-virus agents. The resulting VSImax Dynamic scores are aligned again with saturation on a CPU, Memory or Disk level, also when the baseline response time are relatively high.

8.3.4.5 Determining VSIMax

The Login VSI analyzer will automatically identify the “VSImax”. In the example below the VSImax is 98. The analyzer will automatically determine “stuck sessions” and correct the final VSImax score.

- Vertical axis: Response Time in milliseconds
- Horizontal axis: Total Active Sessions

Figure 21 Sample Login VSI Analyzer Graphic Output



- Red line: Maximum Response (worst response time of an individual measurement within a single session)
- Orange line: Average Response Time within for each level of active sessions
- Blue line: the VSImax average.
- Green line: Minimum Response (best response time of an individual measurement within a single session)

In our tests, the total number of users in the test run had to login, become active and run at least one test loop and log out automatically without reaching the VSI Max to be considered a success.

Note We discovered a technical issue with the VSIMax dynamic calculation in our testing on Cisco B230 M2 blades where the VSIMax Dynamic was not reached during extreme conditions. Working with Login Consultants, we devised a methodology to validate the testing without reaching VSIMax Dynamic until such time as a new calculation is available.

Our Login VSI “pass” criteria, accepted by Login Consultants for this testing follows:

- Cisco will run tests at a session count level that effectively utilizes the blade capacity measured by CPU
- utilization, Memory utilization, Storage utilization and Network utilization.
- We will use Login VSI to launch version 3.6 medium workloads, including flash.
- Number of Launched Sessions must equal Active Sessions within two minutes of the last session launched in a test.
- The Citrix Desktop Studio will be monitored throughout the steady state to insure that:
  - All running sessions report In Use throughout the steady state
  - No sessions move to Unregistered or Available state at any time during Steady State
- Within 20 minutes of the end of the test, all sessions on all Launchers must have logged out automatically and the Login VSI Agent must have shut down.

- We will publish our CVD with our recommendation following the process above and will note that we did not reach a VSIMax dynamic in our testing due to a technical issue with the analyzer formula that calculates VSIMax.

9 VDI Test Results

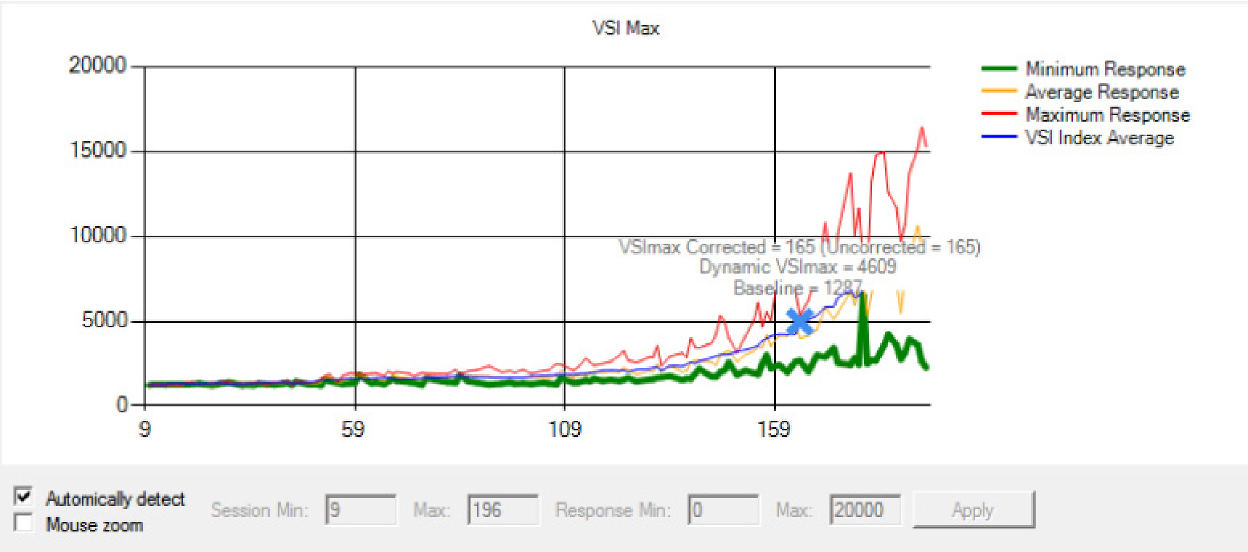
The purpose of this testing is to provide the data needed to validate Citrix XenDesktop 5.6 FP1 Hosted VDI FlexCast model and Citrix XenDesktop with Machine Creation Services using ESXi 5.0 Update 1 and vCenter 5.0 Update 1B to virtualize Microsoft Windows 7 SP1 desktops on Cisco UCS C220 M3 blade servers using a EMC VNX5300 storage system.

The information contained in this section provides data points that a customer may reference in designing their own implementations. These validation results are an example of what is possible under the specific environment conditions outlined here, and do not represent the full characterization of XenDesktop with VMware vSphere.

Two test sequences, each containing three consecutive test runs generating the same result, were performed to establish single server performance and multi-server, linear scalability.

One additional series of stress tests on a single blade server was conducted to establish the official Login VSI Max Score. To reach the Login VSI Max, we ran 195 Medium Workload (with flash) Windows 7 SP1 sessions on a single server. The Login VSI score was achieved on three consecutive runs and is shown below.

Figure 22 Login VSIMax Reached: 165 Users



☑ Automically detect
□ Mouse zoom
Session Min: 9 Max: 196 Response Min: 0 Max: 20000

9.1 Cisco UCS Test Configuration for Single-Server Scalability Test Results

This section details the results from the XenDesktop Hosted VDI single blade server validation testing. The primary success criteria used to validate the overall success of the test cycle is an output chart from Login Consultants' VSI Analyzer Professional Edition, VSIMax Dynamic for the Medium workload (with Flash.)

Note We did not reach a VSIMax Dynamic in our testing due to a technical issue with the analyzer formula that calculates VSIMax. See Section 8.3.4.5 Determining VSIMax for a discussion of this issue.

We ran the single server test at approximately 10 percent lower user density than prescribed by the Login VSI Max to achieve a successful pass of the test with server hardware performance in a realistic range.

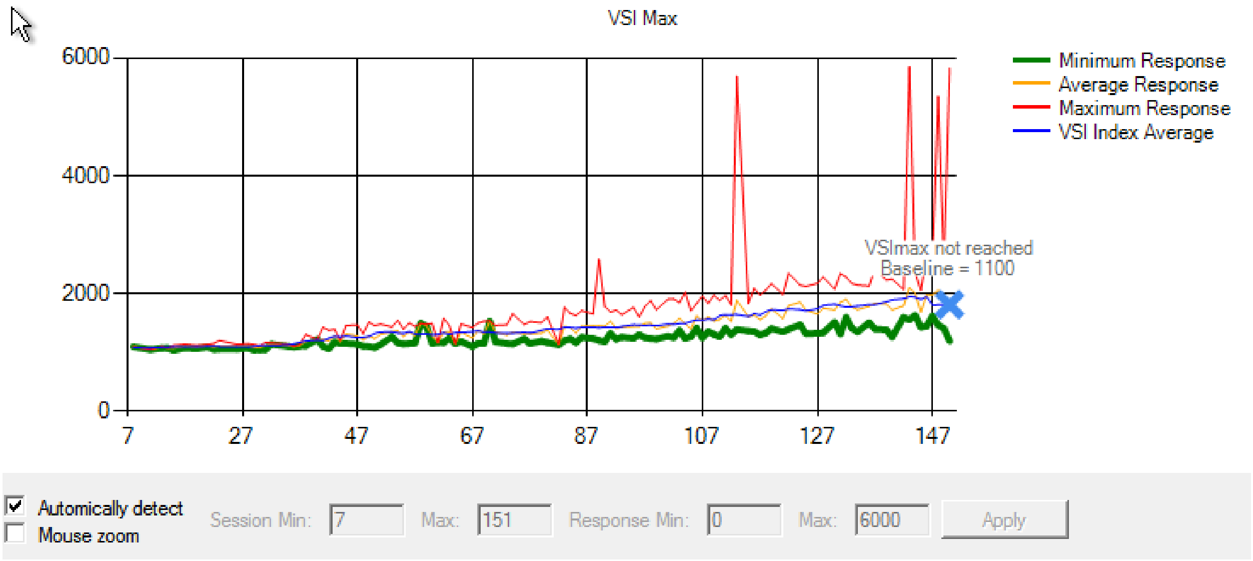
The data below demonstrates that a single Cisco UCS C220 M3 is able to host 150 users sessions with average end user response times of under 2 seconds, well below the Login VSIMax Dynamic threshold for unacceptable performance.

This provides evidence that four Cisco UCS C220 M3s can handle the full 600 user compliment in the event that one of the five Cisco UCS C220 M3s prescribed for the 600 Users workload fails.

Similarly, for the alternate four Cisco UCS C220 500 User alternate solution, this data supports 450 Users can run on three Cisco UCS C220 M3s in the event that one of the four Cisco UCS C220 M3s fails.

Additionally, graphs detailing the CPU, Memory utilization and network throughput during peak session load are also presented. Given adequate storage capability, the CPU utilization determined the maximum VM density per blade.

Figure 23 150 Desktop Sessions on VMware ESXi 5.0U1 below 4000 ms



☑ Automically detect
□ Mouse zoom
Session Min: 7 Max: 151 Response Min: 0 Max: 6000

The following graphs detail CPU, Memory, Disk and Network performance on the Single Cisco UCS B230-M2 Blades

Figure 24 150 User Single Cisco UCS C220 M3 CPU Utilization Boot Phase

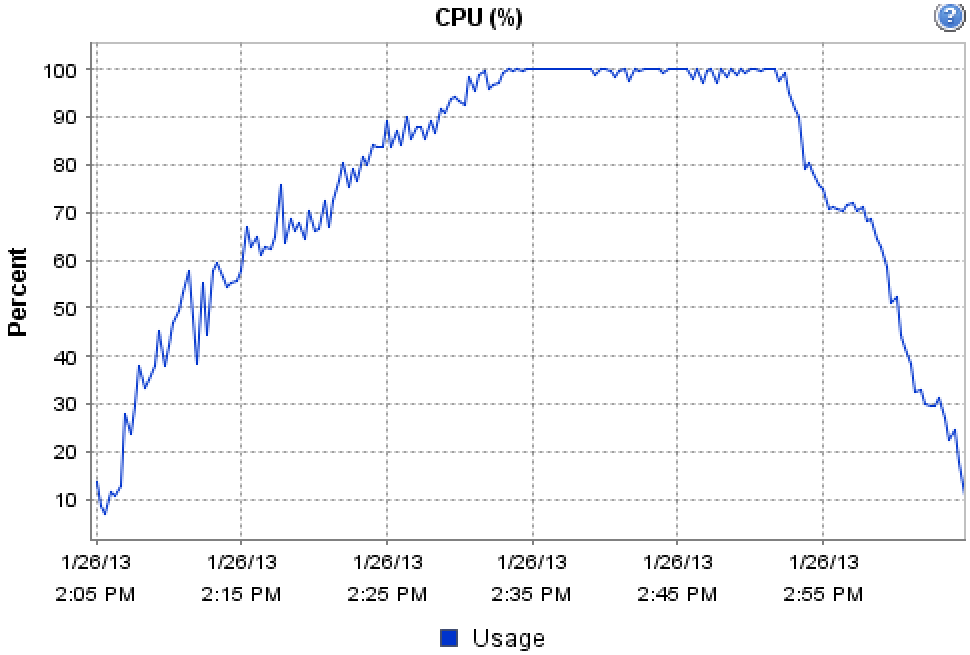


Figure 25 150 User Single Cisco UCS C220 M3 Available Memory

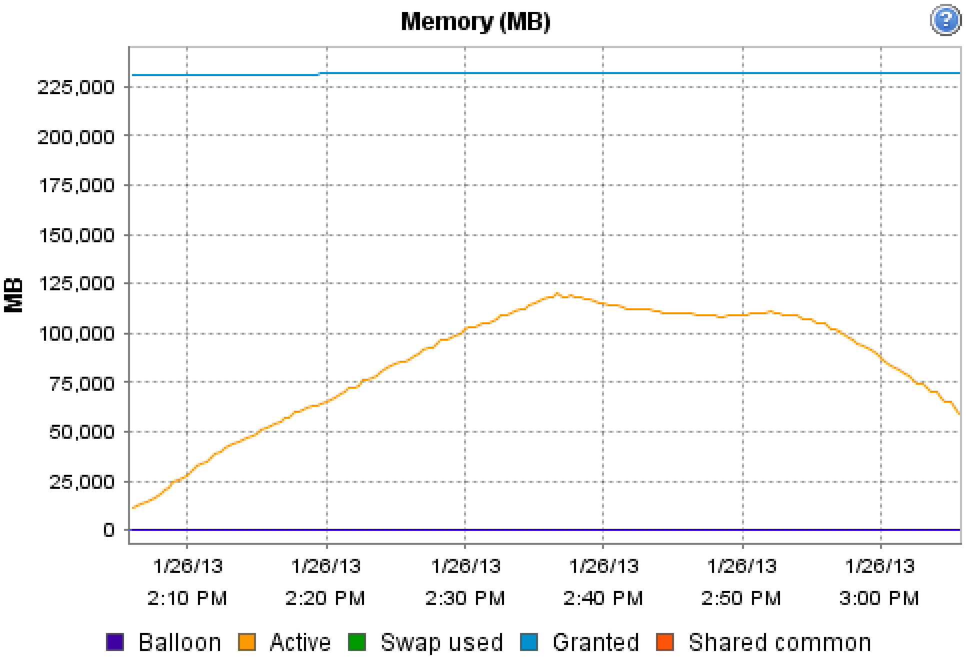
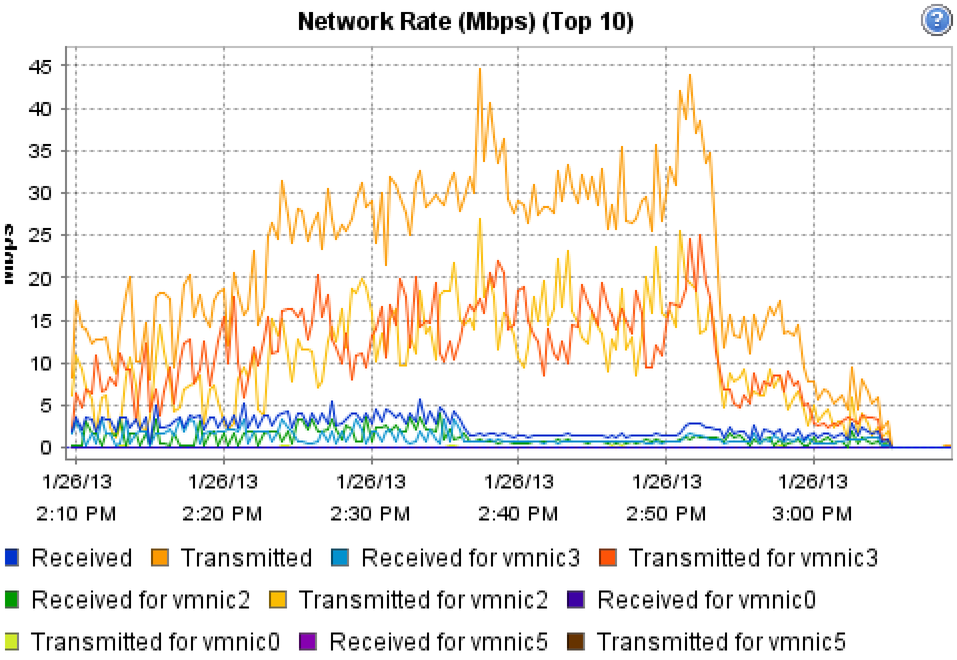


Figure 26 User Single Cisco UCS C220 M3 Cisco VIC1225 VIC Network Rates



The following graphs detail performance of the EMC VNX 7500 during the single blade, 139 user test.

9.2 Cisco UCS Test Configuration for 600 Desktop Scalability Test Results

This section details the results from the XenDesktop Hosted VDI five rack server 600 user validation testing. It demonstrates linear scalability for the system. The primary success criteria used to validate the overall success of the test cycle is an output chart from Login Consultants' VSI Analyzer Professional Edition, VSIMax Dynamic for the Medium workload (with Flash.)

Note We did not reach a VSIMax Dynamic in our testing due to a technical issue with the analyzer formula that calculates VSIMax. See Section 8.3.4.5 Determining VSIMax for a discussion of this issue.

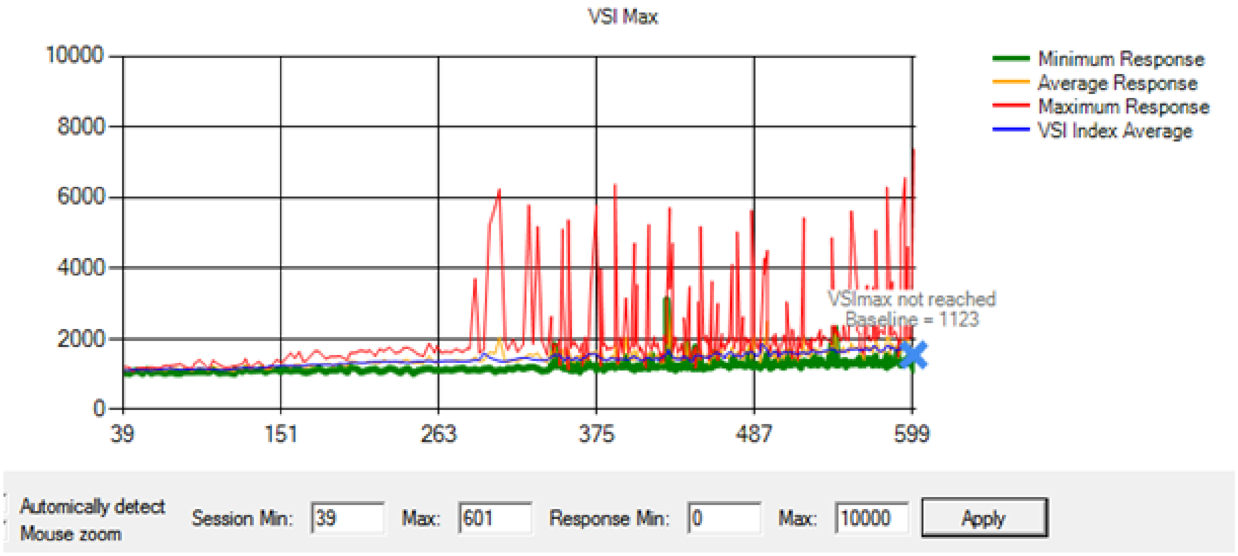
We ran the multi-server test at an average user density slightly higher than 120 users per server across the system. One ESX Cluster containing 5 UCS C220 M3 servers ran the entire workload. This configuration provides N+1 fault tolerance on a cluster basis to achieve a successful pass of the test with server hardware performance in a realistic range.

Additionally, graphs detailing the CPU, Memory utilization and network throughput during peak session load are also presented for a representative blade running 120 user sessions. The single server graphs for blades running 120 user sessions are essentially the same. We have provided the remaining 4 UCS C220 M3 servers' performance charts in Appendix D to illustrate this point.

Given adequate storage capability, the CPU utilization determined the maximum recommended VM density per blade for the 600 user environment.

For the largest scale test, we are including the EMC VNX5300 performance metrics as well.

Figure 27 600 Desktop Sessions on 5 Cisco UCS C220 M3s running VMware ESXi 5.0 U1 below 4000 ms



Automically detect
Mouse zoom

Session Min: 39 Max: 601 Response Min: 0 Max: 10000

The following graphs detail CPU, Memory, Disk and Network performance on a representative Cisco UCS C220 M3 server during the five server, 600 User test. (Representative results for all five servers in one vCenter clusters can be found in Appendix C.)

Figure 28 600 Desktop Sessions on 5 Cisco UCS C220 M3 CPU Utilization Boot Phase

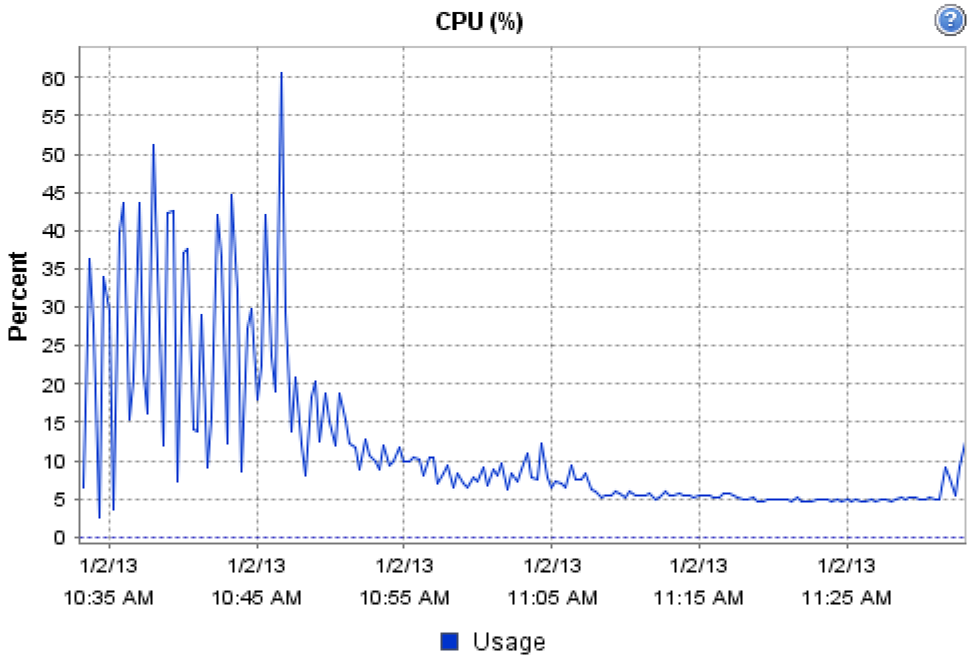


Figure 29 600 Desktop Sessions on 5 Cisco UCS C220 M3 Memory Utilization Boot Phase

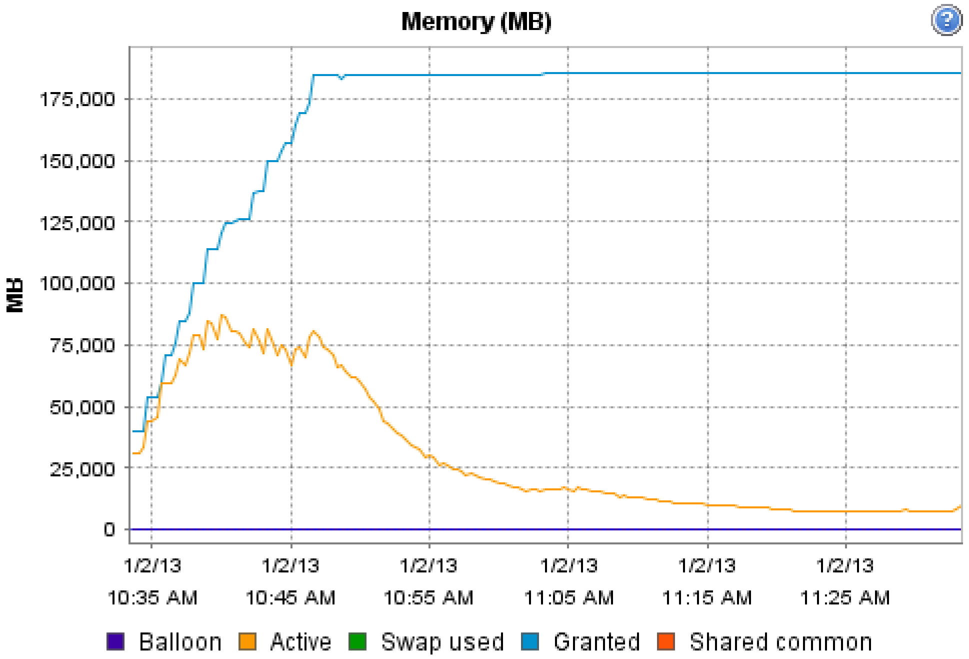


Figure 30 600 Desktop Sessions on 5 Cisco UCS C220 M3 Cisco VIC1225 Mbps Receive/Transmit Boot Phase

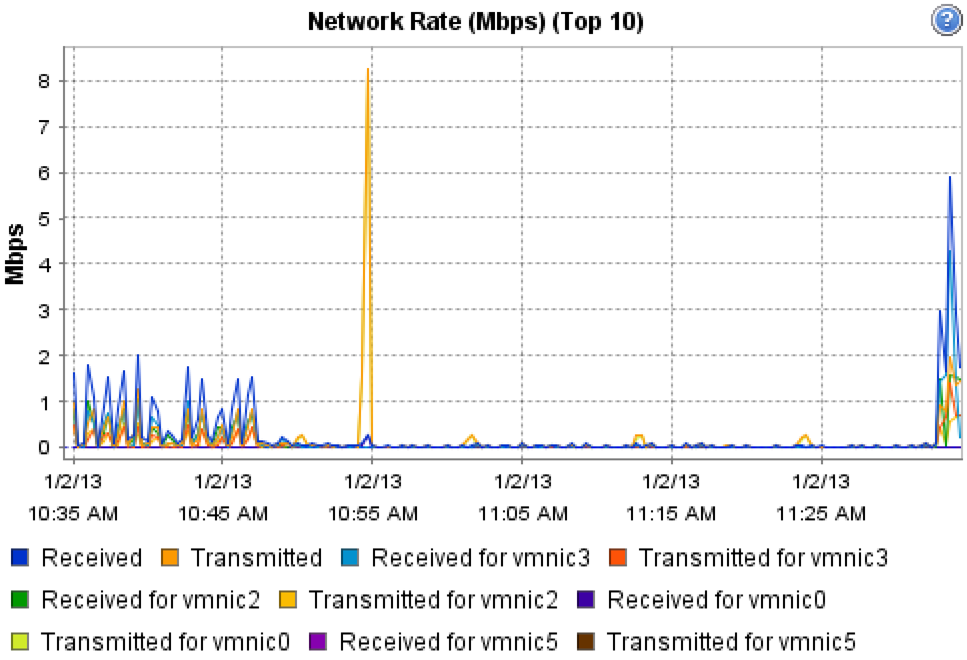


Figure 31 600 Desktop Sessions on 5 Cisco UCS C220 M3 CPU Utilization Test Phase

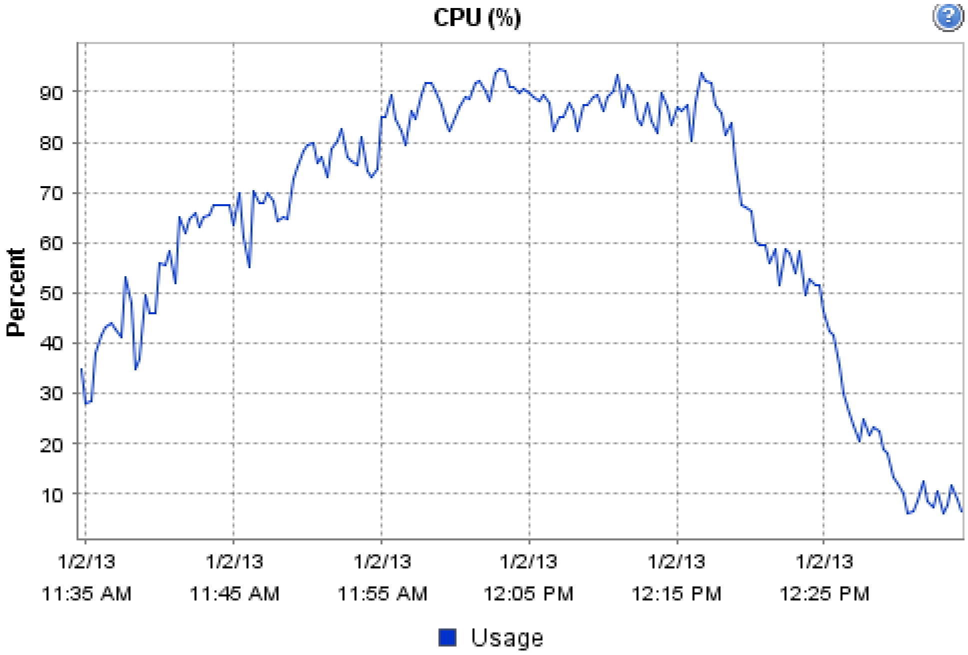


Figure 32 600 Desktop Sessions on 5 Cisco UCS C220 M3 CPU Utilization Test Phase

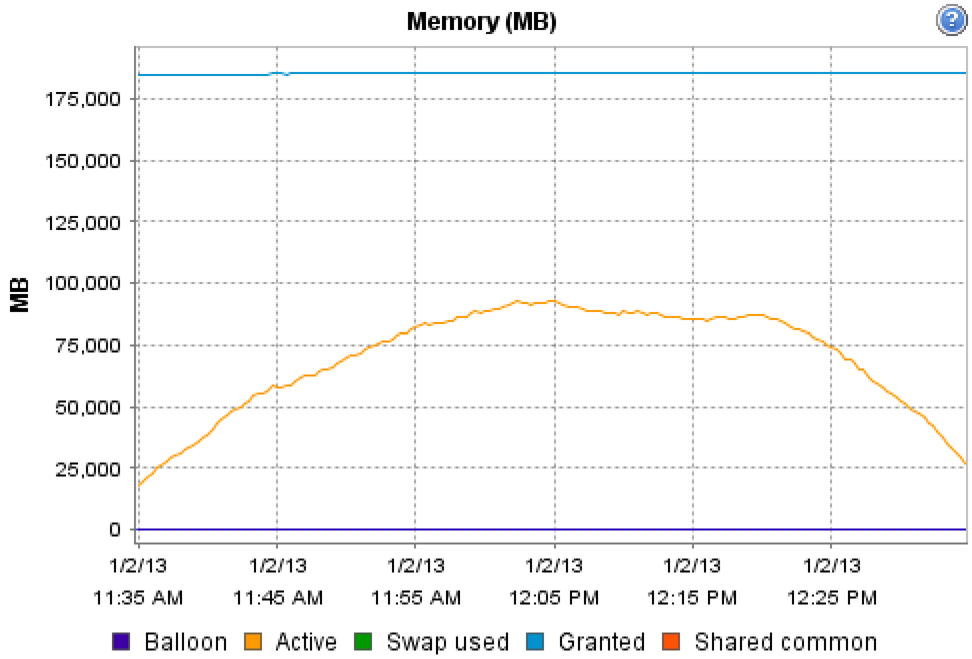


Figure 33 600 Desktop Sessions on 5 Cisco UCS C220 M3 Cisco VIC1225 Mbps Receive/Transmit Test Phase

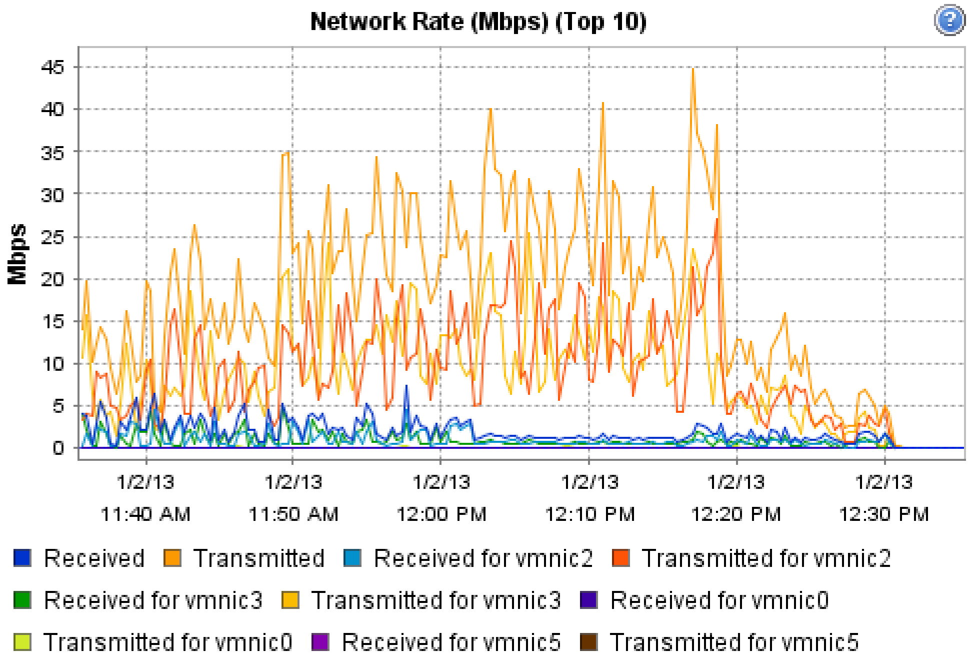


Figure 34 *600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Utilization Boot Phase*

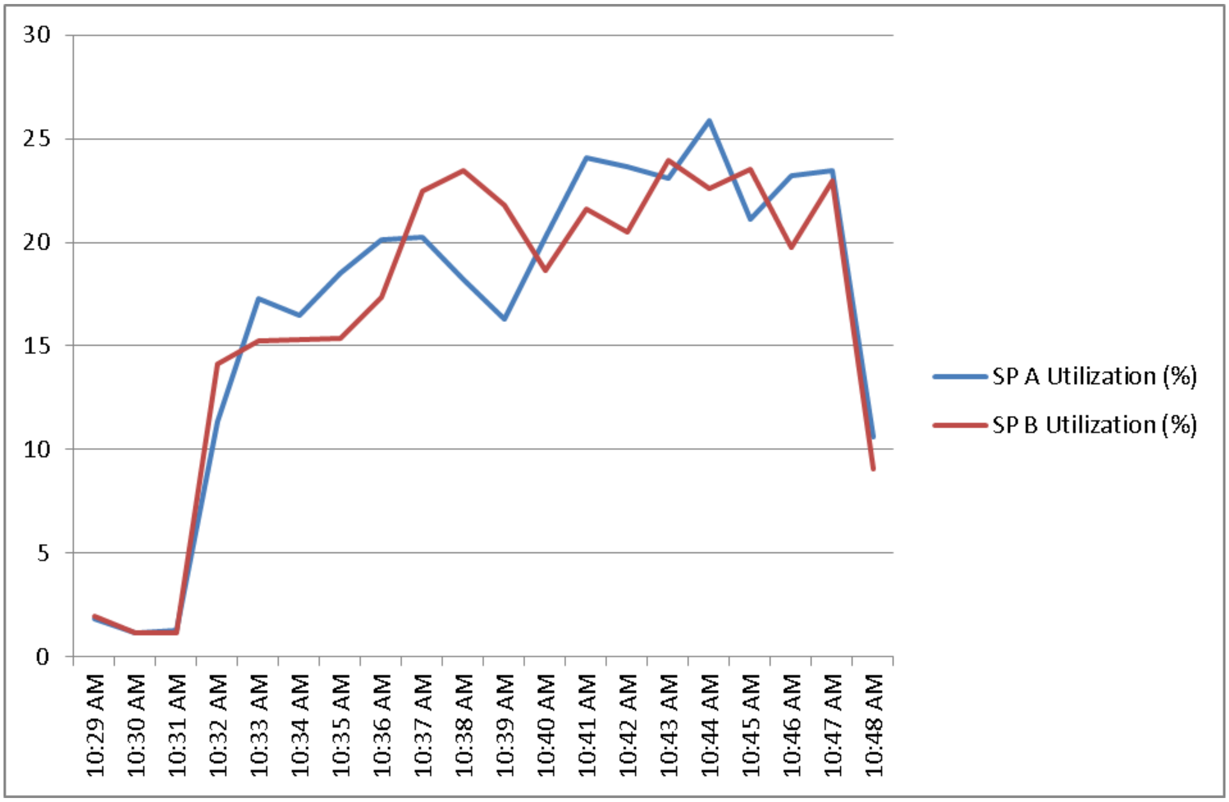


Figure 35 *600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Queue Lengths Boot Phase*

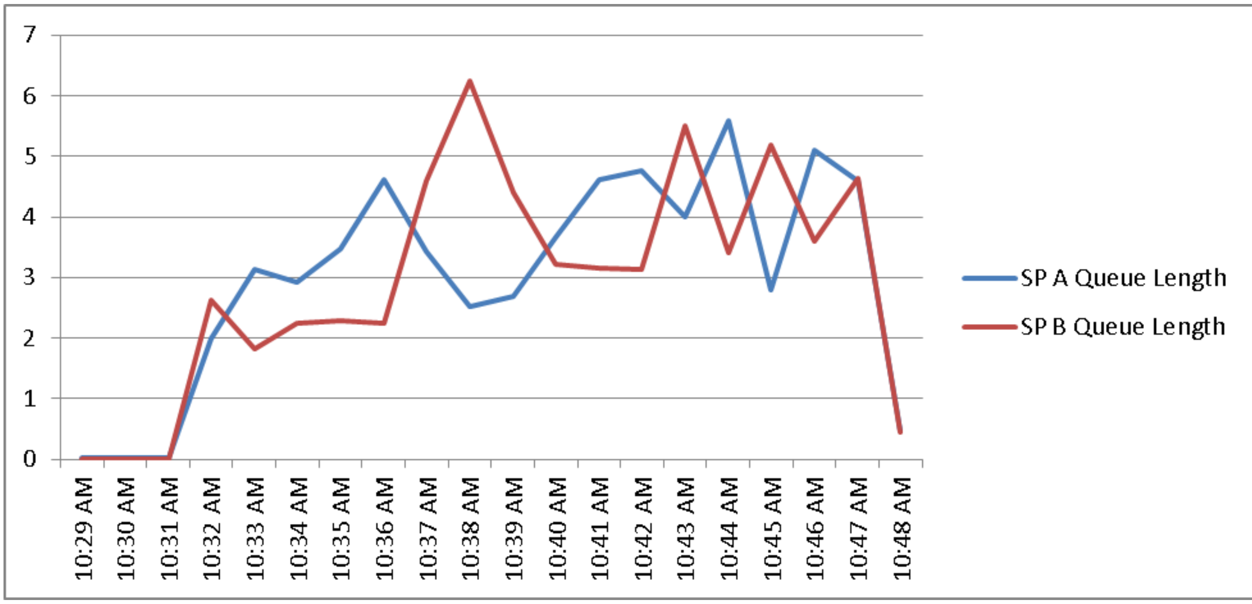


Figure 36 600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Total Throughput Boot Phase

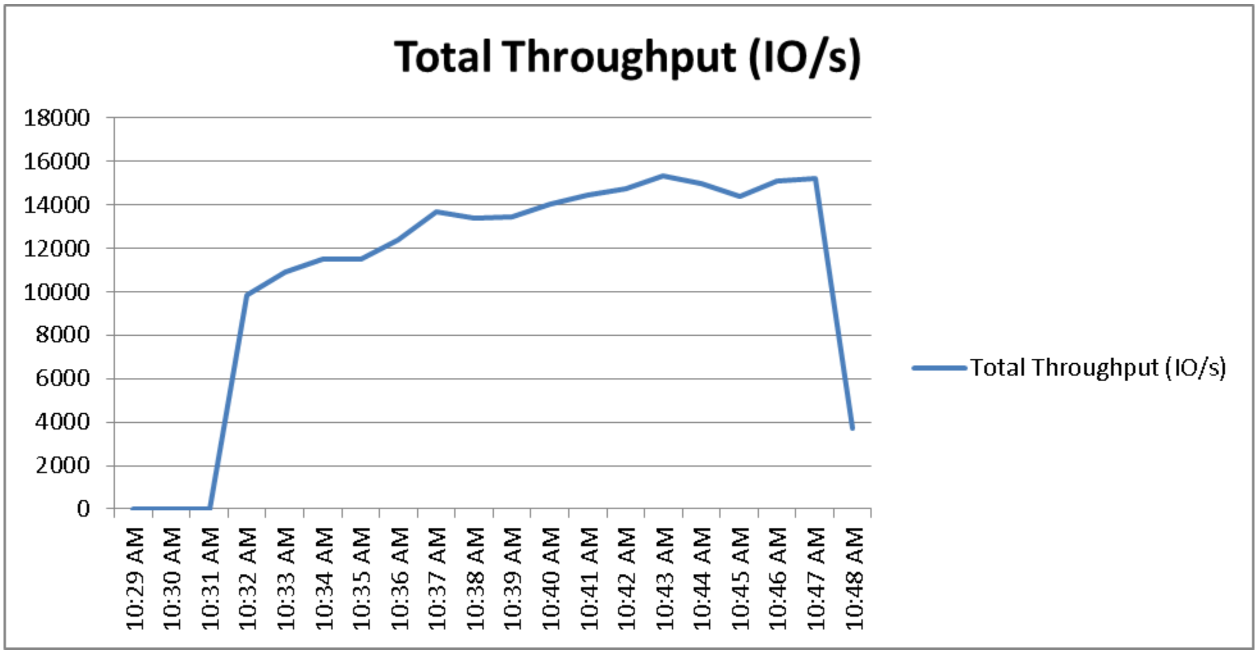


Figure 37 600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Utilization Test Phase

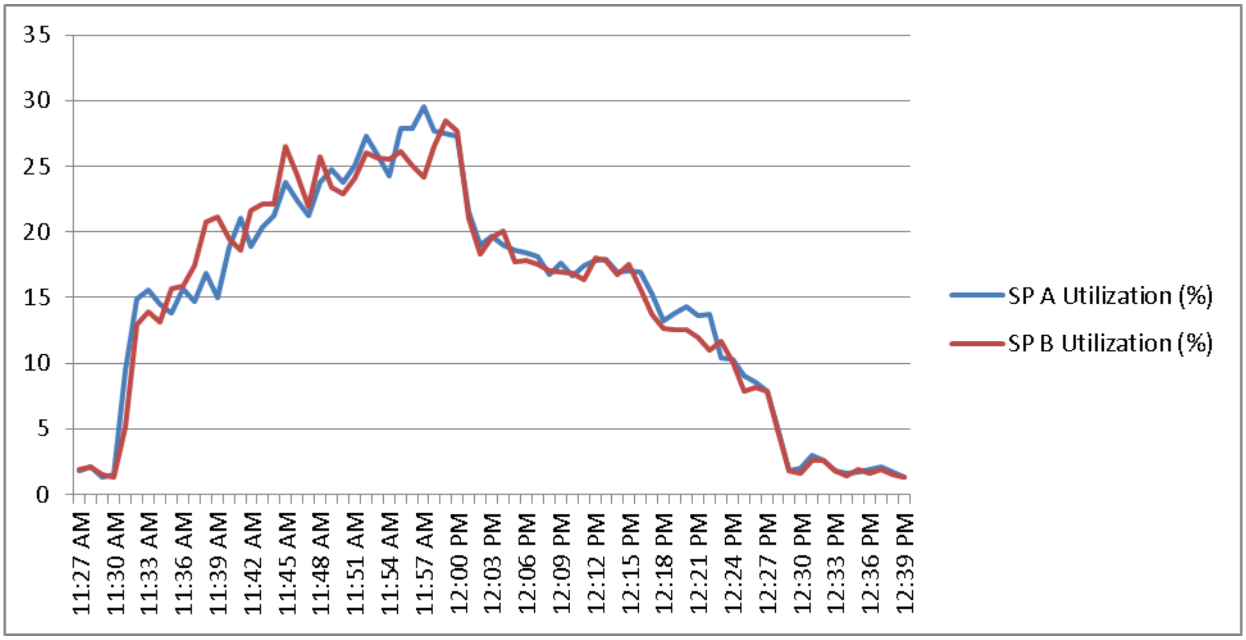


Figure 38 600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Queue Lengths Test Phase

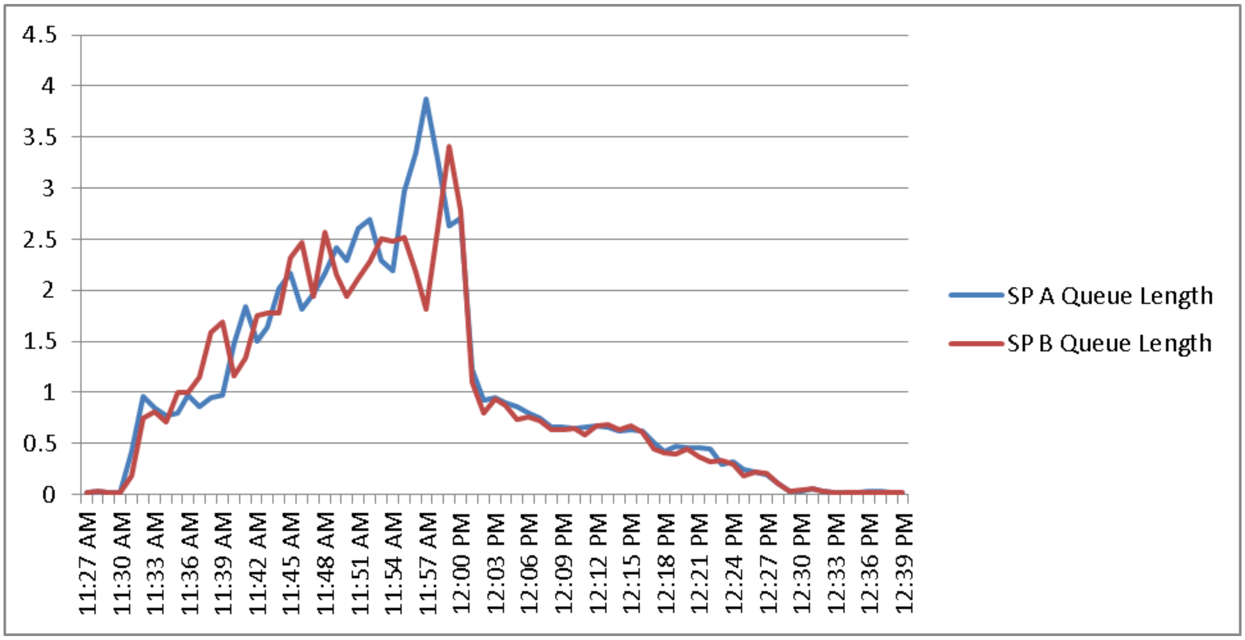
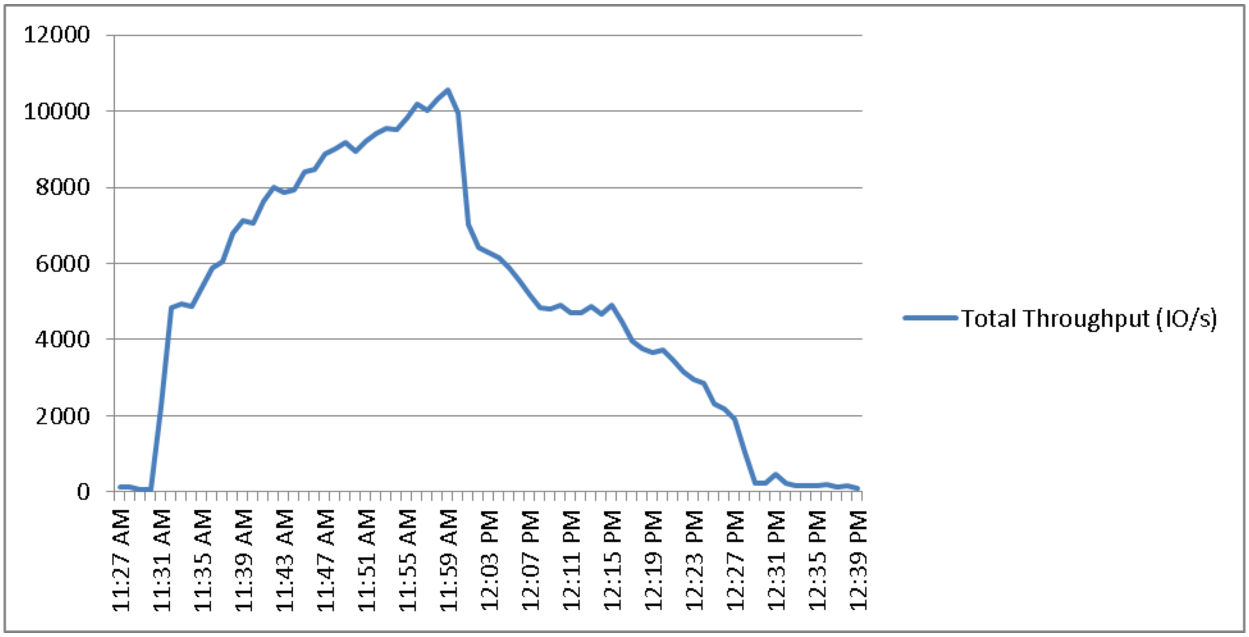


Figure 39 600 Desktop Sessions on 5 Cisco UCS C220 M3 EMC VNX5300 SP Total Throughput Test Phase



9.3 Cisco UCS Test Configuration for 500 Desktop Scalability Test Results

This section details the results from the XenDesktop Hosted VDI four rack server 500 user validation testing. It demonstrates linear scalability for the system. The primary success criteria used to validate the overall success of the test cycle is an output chart from Login Consultants' VSI Analyzer Professional Edition, VSIMax Dynamic for the Medium workload (with Flash.)

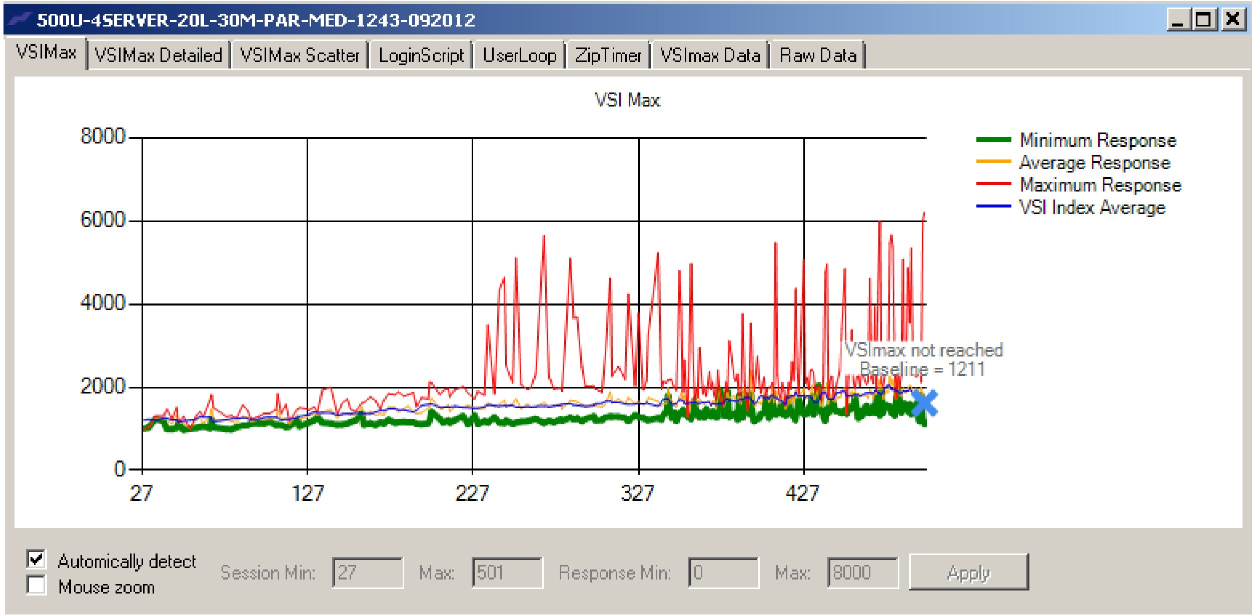
Note We did not reach a VSIMax Dynamic in our testing due to a technical issue with the analyzer formula that calculates VSIMax. See Section 8.3.4.5 Determining VSIMax for a discussion of this issue.

We ran the multi-server test at an average user density of 125 users per server across the system. One ESX Cluster containing 4 Cisco UCS C220 M3 servers ran the entire workload. This configuration provides N+1 fault tolerance for 450 users to achieve a successful pass of the test with server hardware performance in a realistic range.

Additionally, graphs detailing the CPU, Memory utilization and network throughput during peak session load are also presented for a representative server running 125 user sessions. The single server graphs for blades running 125 user sessions are essentially the same. We have provided the remaining 3 UCS C220 M3 servers' performance charts in Appendix D to illustrate this point.

Given adequate storage capability, the CPU utilization determined the maximum recommended VM density per blade for the 500 user environment.

Figure 40 *500 Desktop Sessions on 4 Cisco UCS C220 M3s running VMware ESXi 5.0U1 below 4000 ms*



500U-4SERVER-20L-30M-PAR-MED-1243-092012

☑ Automically detect
□ Mouse zoom

Session Min: 27 Max: 501 Response Min: 0 Max: 8000

Figure 41 500 Desktop Sessions on 4 C220 M3 CPU Utilization Boot Phase

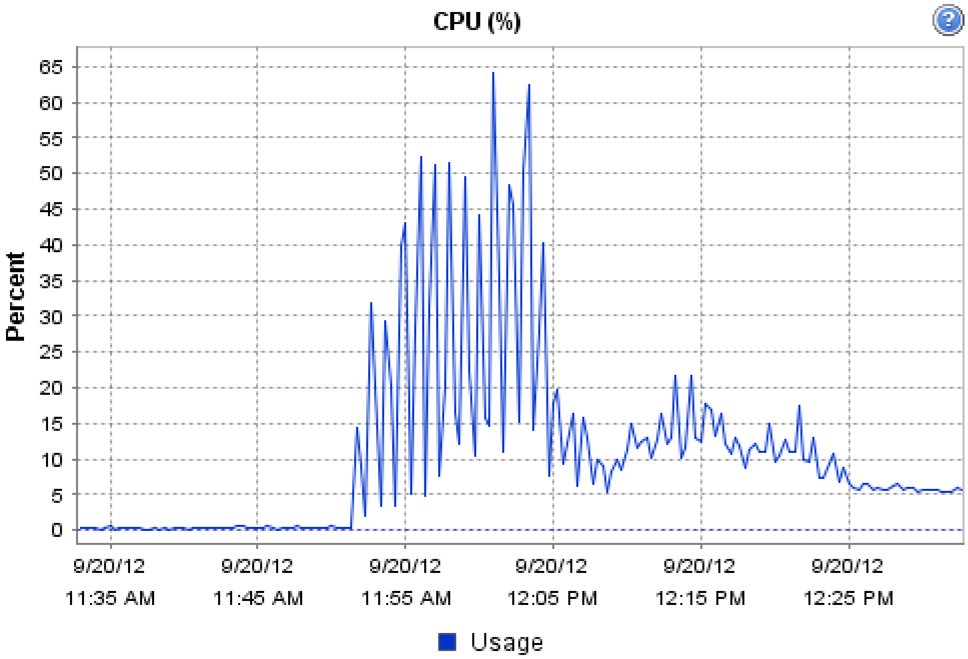


Figure 42 500 Desktop Sessions on 5 C220 M3 Memory Utilization Boot Phase

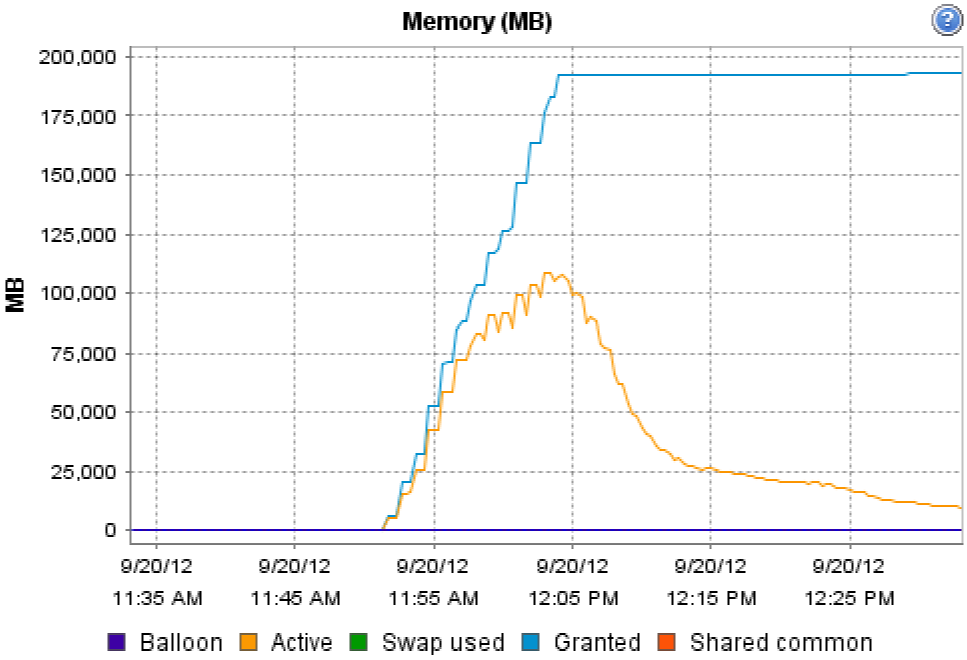


Figure 43 500 Desktop Sessions on 5 C220 M3 Network Utilization Boot Phase

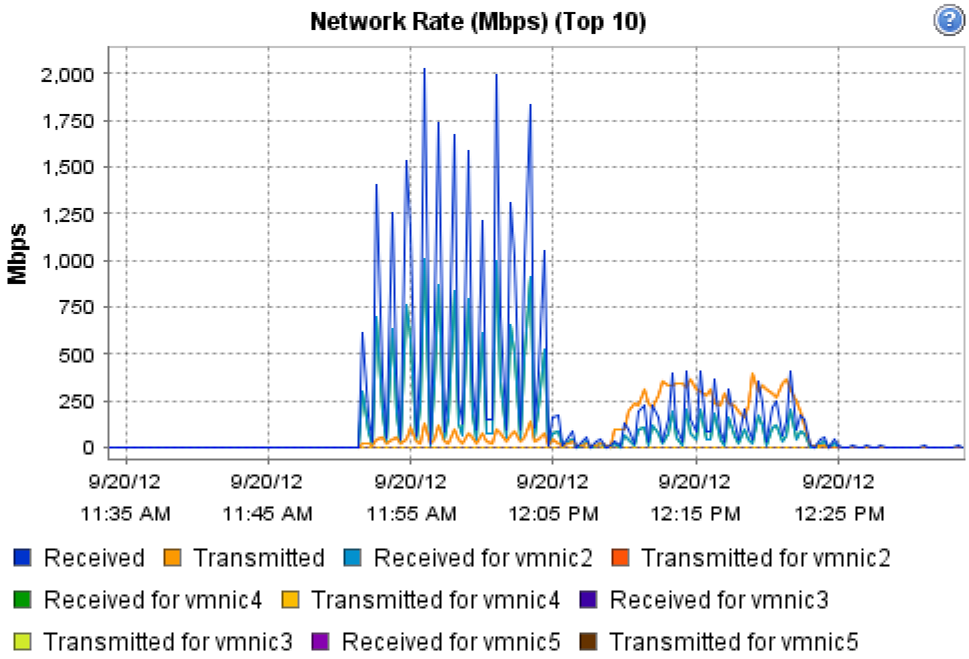


Figure 44 500 Desktop Sessions on 4 C220 M3 CPU Utilization Test Phase

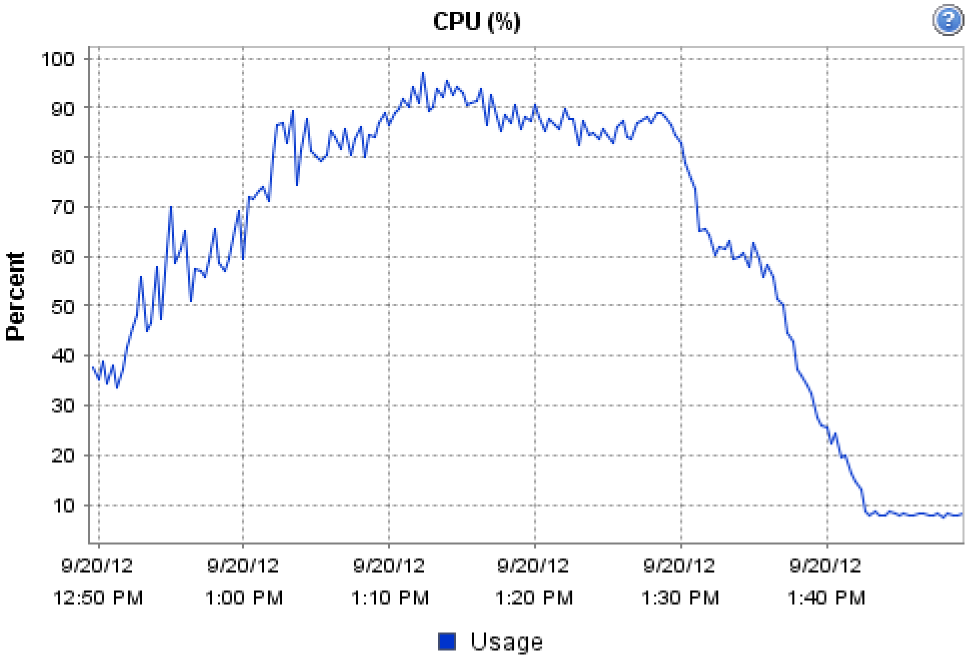


Figure 45 500 Desktop Sessions on 4 C220 M3 Memory Utilization Test Phase

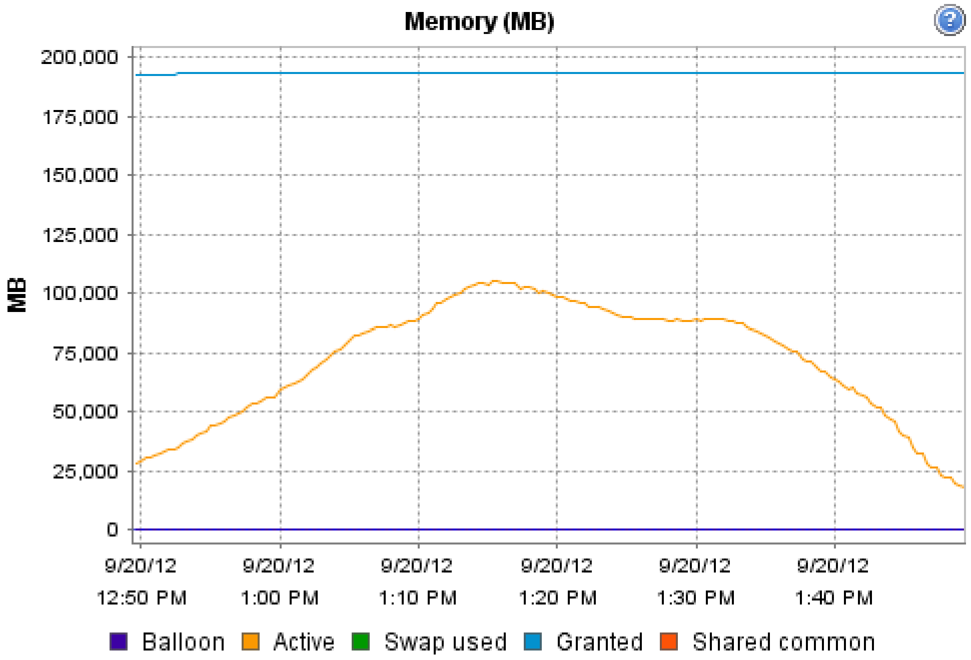
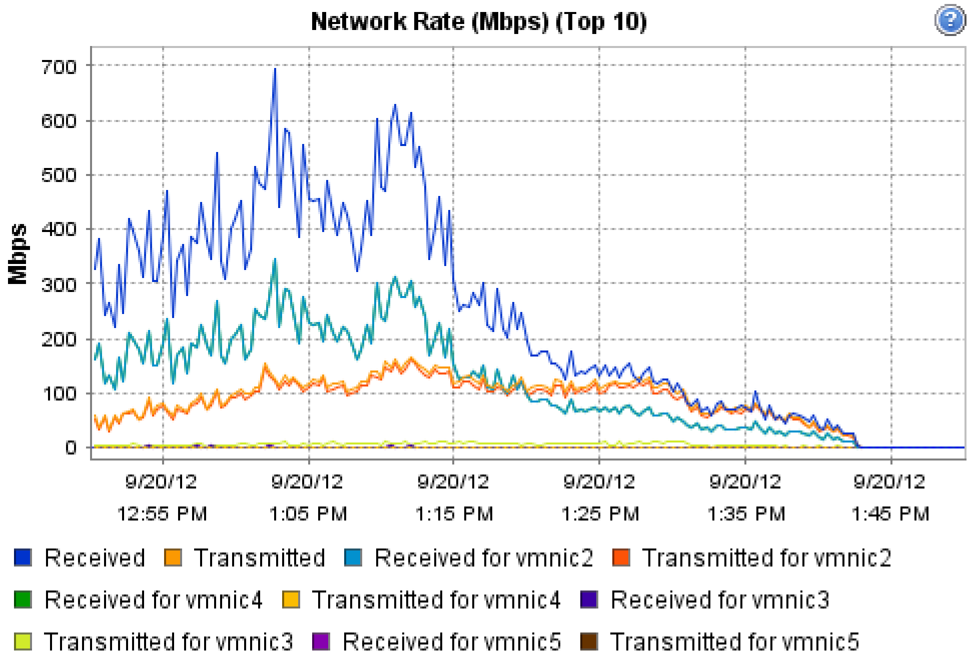


Figure 46 500 Desktop Sessions on 4 C220 M3 Network Utilization Test Phase



10 Scalability Considerations and Guidelines

There are many factors to consider when you begin to scale beyond a 500-600 User, four to five Cisco UCS C220 host server configuration, which this reference architecture has successfully tested. In this section we give guidance to scale beyond the 500-600 user system.

10.1 Cisco UCS System Configuration

As our results indicate, we have proven linear scalability in the Cisco UCS Reference Architecture as tested.

- Cisco UCS 2.1 management software supports up to 20 chassis within a single Cisco UCS domain on our second generation Cisco UCS Fabric Interconnect 624UP8 and 6296UP models. Our single UCS domain can grow to 160 blades or rack servers or any combination of the two totaling 160.
- With Cisco UCS 2.1 management software, released late in November 2012, each UCS 2.1 Management domain is extensibly manageable by UCS Central, our new manager of managers, vastly increasing the reach of the UCS system.
- As scale grows, the value of the combined UCS fabric, Nexus physical switches and Nexus virtual switches increases dramatically to define the Quality of Services required to deliver excellent end user experience 100% of the time.
- To accommodate the Cisco Nexus 5500 upstream connectivity in the way we describe in the LAN and SAN Configuration section, we need four Ethernet uplinks and two Fibre Channel uplinks to be configured on the Cisco UCS Fabric interconnect. And based on the number of uplinks from each chassis, we can calculate number of desktops can be hosted in a single UCS domain. Assuming eight links per chassis, four to each 6248, scaling beyond 10 chassis would require a pair of Cisco UCS 6296 fabric interconnects. A 20,000 virtual desktop building block, with its support infrastructure services can be built out of the RA described in this study with eight links per chassis and 20 Cisco UCS chassis comprised of seven B230 M2 and one B200 M3 blades servers in each chassis.

Of course, the backend storage has to be scaled accordingly, based on the IOP considerations as described in the EMC scaling section. Please refer the EMC section that follows this one for scalability guidelines.

10.2 Citrix XenDesktop 5.6 Hosted VDI

XenDesktop environments can scale to large numbers. When implementing Citrix XenDesktop hosted VDI considerations include but not limited to:

- Types of Storage in your environment
- Types of desktops that will be deployed
- Data protection requirements
- For Citrix Provisioning Server pooled desktops write cache size and placement

These and other various aspects of scalability considerations described in greater detail in “XenDesktop - Modular Reference Architecture” document and should be a part of any VDI design.

Designing and deploying our test environment we followed best practices whenever possible.

The following are in particular worth mentioning here.

Citrix always recommends using N+1 schema for VDI servers, to accommodate resiliency. In our test environment, this was applied to all infrastructure servers.

For larger scale deployments, Provisioning Server Network Adapters were configured to have a static IP and management and streaming traffic was separated between different Network adapters.

For larger scale deployments, all the PVS services are set to start as: Automatic (Delayed Start).

For larger scale deployments, we use the XenDesktop Setup Wizard in PVS. Wizard does an excellent job of creating the desktops automatically and it's possible to run multiple instances of the wizard provided the deployed desktops are placed in different catalogs and have different naming conventions.

To run wizard at a minimum you need to install the Provisioning Server, the XenDesktop Controller, and configure hosts, as well as create VM templates on all datastores were desktops will be deployed.

10.3 EMC VNX Storage Guidelines for XenDesktop Virtual Machines

Sizing VNX storage system to meet virtual desktop IOPS requirement is a complicated process. When an I/O reaches the VNX storage, it is served by several components such as Data Mover (NFS), backend dynamic random access memory (DRAM) cache, FAST Cache, and disks. To reduce the complexity, EMC recommends using a building block approach to scale to thousands of virtual desktops.

For more information on storage sizing guidelines to implement virtual desktop infrastructure in VNX unified storage systems, refer to the EMC white paper “Sizing EMC VNX Series for VDI workload – An Architectural Guideline.”

10.4 VMware ESXi 5 Guidelines for Virtual Desktop Infrastructure

In our test environment two adjustments were performed to support our scale:

The amount of memory configured for the Tomcat Maximum memory pool was increased to 3072.

The cost threshold for parallelism was increased to 15.

For further explanations on a basis for these adjustments and details on how to perform them refer to the VMware documentation sited in References section of this document.

11 References

This section provides links to additional information for each partner’s solution component of this document.

11.1 Cisco Reference Documents

Third-Generation Fabric Computing: The Power of Unification webcast replay

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=W&LANGUAGE_ID=E&PRIORITY_CODE=215011_15&SEMINAR_CODE=S15897&CAMPAIGN=UCS+Momentum&COUNTRY_SITE=us&POSITION=banner&REFERRING_SITE=go+unified+computing&CREATIVE=carousel+banner+event+replay

Cisco Unified Computing System Manager Home Page

http://www.cisco.com/en/US/products/ps10281/index.html

Cisco UCS C220 M3 Rack Server Resources

http://www.cisco.com/en/US/partner/products/ps12369/index.html

Cisco UCS 6200 Series Fabric Interconnects http://www.cisco.com/en/US/partner/products/ps11544/index.html

Cisco Nexus 2232PP 10GE Fabric Extender

http://www.cisco.com/en/US/partner/products/ps10784/index.html

Cisco Nexus 5500 Series Switches Resources

http://www.cisco.com/en/US/products/ps9670/index.html

Download Software for UCS C220 M3 Rack Server

http://software.cisco.com/download/type.html?mdfid=284296253&i=rs

Download Cisco UCS Manager and Blade Software Version 2.0(4d)

http://software.cisco.com/download/release.html?mdfid=283612660&softwareid=283655658&release=1.4(4k)&relind=AVAILABLE&rellifecycle=&reltype=latest

Download Cisco UCS Central Software Version 1.0(1a)

http://software.cisco.com/download/cart.html?imageGuId=8CAAAD77B3A1DB35B157BE84ED109A4703849F53&i=rs

11.2 Citrix Reference Documents

XenDesktop 5.6

- Modular Reference Architecture - http://support.citrix.com/article/CTX133162

Virtual Desktop

- Windows 7 Optimization Guide: http://support.citrix.com/article/CTX127050
- Web Interface Best Practices for Avoiding Major Production Outages: http://support.citrix.com/article/CTX125715

11.3 EMC Reference Documents

- Sizing EMC VNX Series for VDI Workload – An Architectural Guideline
- EMC Infrastructure for Citrix XenDesktop 5.6, EMC VNX Series (NFS), VMware vSphere 5.0, Citrix XenDesktop 5.6, and Citrix Profile Manager 4.1—Reference Architecture
- EMC Infrastructure for Citrix XenDesktop 5.6, EMC VNX Series (NFS), VMware vSphere 5.0, Citrix XenDesktop 5.6, and Citrix Profile Manager 4.1—Proven Solutions Guide
- EMC Infrastructure for Citrix XenDesktop 5.5 (PVS), EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5 (PVS), Citrix XenApp 6.5, and XenServer 6—Reference Architecture
- EMC Infrastructure for Citrix XenDesktop 5.5 (PVS), EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5 (PVS), Citrix XenApp 6.5, and XenServer 6—Proven Solution Guide
- EMC Infrastructure for Citrix XenDesktop 5.5 , EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, Citrix XenApp 6.5, and XenServer 6—Reference Architecture

- EMC Infrastructure for Citrix XenDesktop 5.5, EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, Citrix XenApp 6.5, and XenServer 6—Proven Solution Guide

11.4 VMware Reference Documents

- Accessing a vCenter Server using Web access or vSphere Client fails with an SSL certificate error: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021514
- VMware vSphere ESXi and vCenter Server 5 Documentation: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021514
- VMware vCenter Management Webservices features do not function properly: - http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1039180
- VMware® vCenter Server™ 5.1 Database Performance Improvements and Best Practices for Large-Scale Environments: - http://www.vmware.com/files/pdf/techpaper/VMware-vCenter-DBPerfBestPractices.pdf
- Performance Best Practices for VMware vSphere™ 5.0: - http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf

Appendix A—Nexus 5548 Configuration (NFS Variant Only)

```
!Nexus 5548A NFS Variant VSPEX C500
!Command: show running-config
!Time: Sun Dec  6 23:15:29 2009

version 5.1(3)N1(1a)
hostname SJ2-B21-N5548-A

feature telnet
no feature http-server
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
feature fex
```

```
username admin password 5 $1$ZGA7bQiM$rD7QcH45.4ZOLIf2/J.ur1  role
network-adminno password strength-check

banner motd #Nexus 5000 Switch
#

ip domain-lookup
ip domain-name cisco.com
ip name-server 171.70.168.183 171.68.226.120
system jumbomtu 9000
logging event link-status default
class-map type qos class-fcoe
class-map type qos match-any class-platinum
  match cos 5
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-platinum
  match qos-group 2
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
policy-map type qos jumbo
  class class-default
    set qos-group 0
policy-map type qos system_qos_policy
  class class-platinum
    set qos-group 2
  class class-default
    set qos-group 0
policy-map type queuing system_q_in_policy
  class type queuing class-platinum
    bandwidth percent 50
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 30
policy-map type queuing system_q_out_policy
```

```
  class type queuing class-platinum
    bandwidth percent 50
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 30
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-platinum
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos system_nq_policy
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos system_nq_policy
  class type network-qos class-platinum
    pause no-drop
    mtu 9000
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    mtu 9000
    multicast-optimize
system qos
  service-policy type qos input system_qos_policy
  service-policy type queuing input system_q_in_policy
  service-policy type queuing output system_q_out_policy
  service-policy type network-qos system_nq_policy
fex 130
  pinning max-links 1
  description "FEX0130"
snmp-server user admin network-admin auth md5
0x0ae428b6495ff67f478fd90e941c15d7 priv

0x0ae428b6495ff67f478fd90e941c15d7 localizedkey
```

```
vrf context management
  ip route 0.0.0.0/0 10.29.132.1
vlan 1
vlan 47
  name N1K-Mgmt
vlan 48
  name N1K-Ctrl
vlan 49
  name N1K-Pckt
vlan 50
  name Storage
vlan 51
  name vMotion
vlan 52
  name VDIAB
vlan 100
  name VDI
vlan 132
  name ESXi_Management
spanning-tree vlan 1,10-20,50-52,100,132 priority 16384
vpc domain 30
  role priority 4000
  peer-keepalive destination 10.29.132.6


interface Vlan1

interface Vlan50
  no shutdown
  ip address 10.10.50.3/24
  hsrp version 2
  hsrp 50
    preempt
    priority 110
    ip 10.10.50.1

interface Vlan51
```

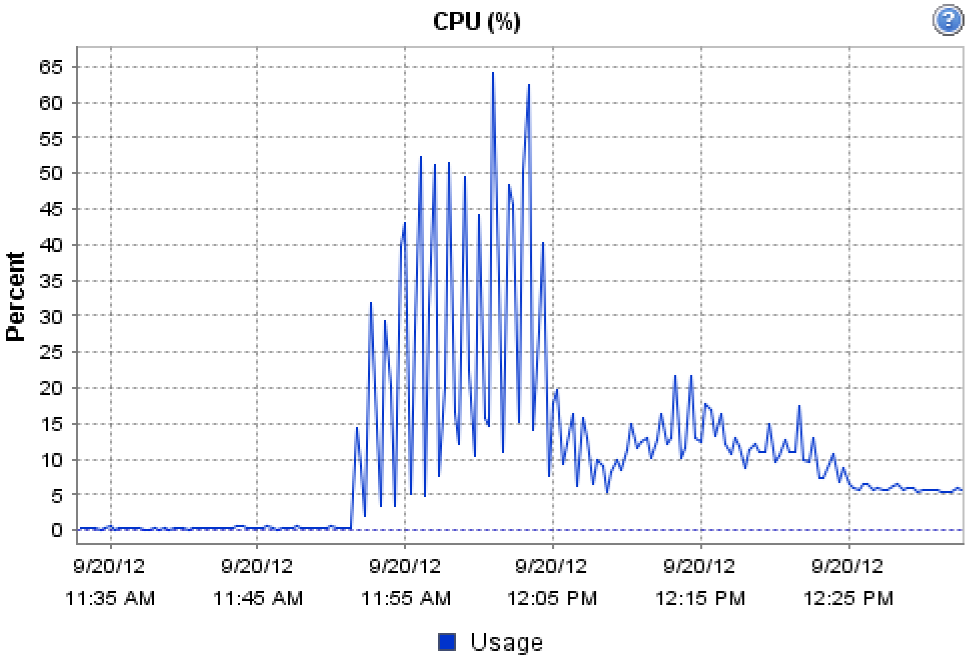
```
  no shutdown
  ip address 10.10.51.3/24
  hsrp version 2
  hsrp 51
    preempt
    priority 110
    ip 10.10.51.1

interface Vlan52
  no shutdown
  ip address 10.10.52.3/24
  hsrp version 2
  hsrp 52
    preempt
    priority 110
    ip 10.10.52.1

interface Vlan100
  no shutdown
  ip address 10.10.1.3/22
  hsrp version 2
  hsrp 100
    preempt
    priority 110
    ip 10.10.1.1

interface port-channel2
  untagged cos 5
  switchport access vlan 50
  vpc 2

interface port-channel30
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  spanning-tree port type network
  vpc peer-link

interface port-channel47
```

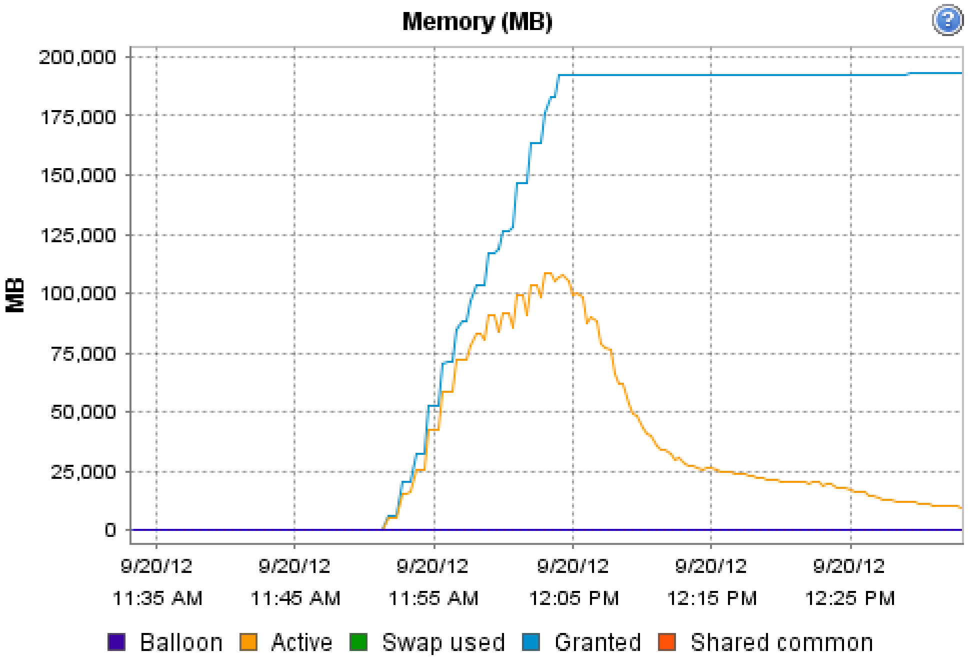
```
  description VPCforN1KVUplinks
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  spanning-tree port type edge trunk
  speed 10000
  vpc 47

interface Ethernet1/1
  switchport access vlan 132
  speed 1000

interface Ethernet1/2

interface Ethernet1/3
  description N1K-UplinkforInfraServers
  switchport access vlan 100

interface Ethernet1/4
  switchport mode trunk
  switchport access vlan 51
  switchport trunk allowed vlan 47-52,100,132
  speed 1000

interface Ethernet1/5
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/7
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/8
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
```

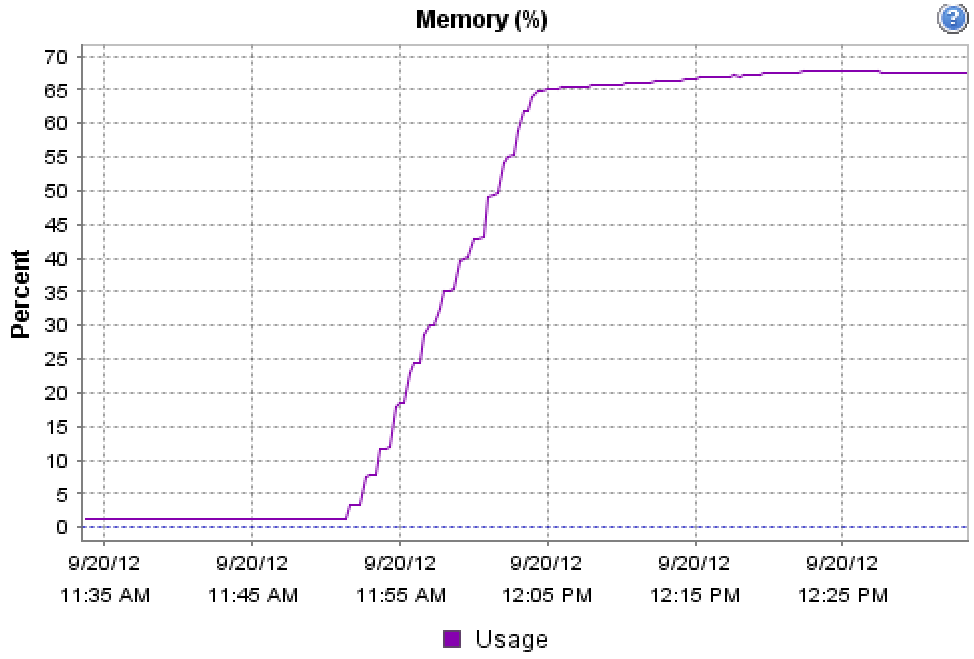
```
interface Ethernet1/9
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/10
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13
  switchport access vlan 100
  speed 1000

interface Ethernet1/14
  switchport access vlan 100
  speed 1000

interface Ethernet1/15
  switchport access vlan 100
  speed 1000

interface Ethernet1/16
  switchport access vlan 100
  speed 1000

interface Ethernet1/17
  switchport access vlan 100
  speed 1000

interface Ethernet1/18
  switchport access vlan 100
  speed 1000

interface Ethernet1/19
```

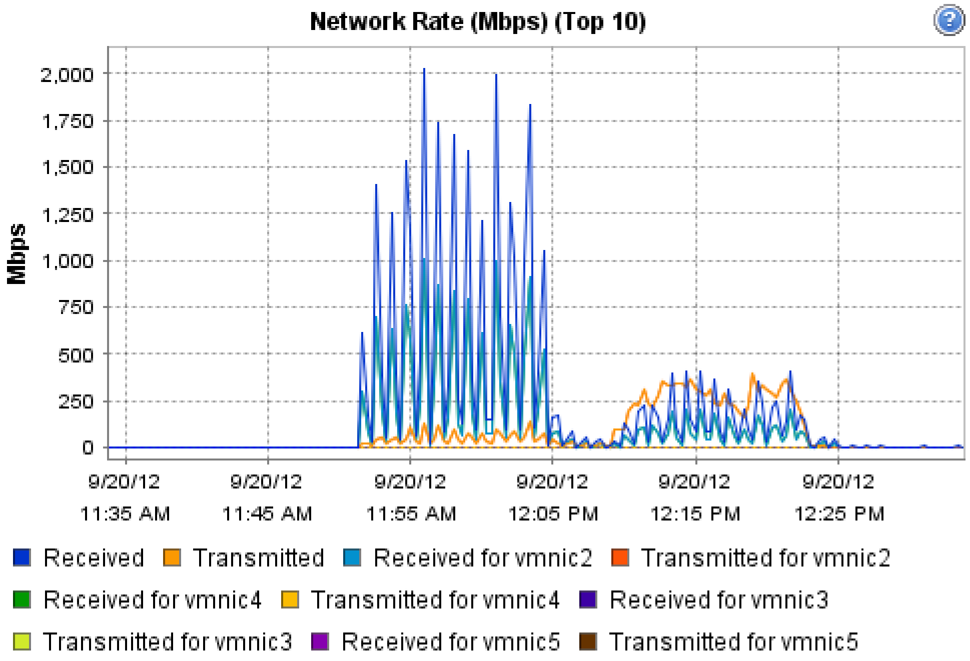
```
  switchport access vlan 100
  speed 1000

interface Ethernet1/20
  switchport access vlan 100
  speed 1000

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30
  shutdown
  switchport mode fex-fabric
  fex associate 130

interface Ethernet1/31
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  channel-group 30 mode active

interface Ethernet1/32
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  channel-group 30 mode active

interface Ethernet2/1
  description VNX-5300-10GB-UPLINK
  switchport access vlan 50
  channel-group 2 mode active

interface Ethernet2/2
  description VNX-5300-10GB-UPLINK
  switchport access vlan 50

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface mgmt0
  ip address 10.29.132.7/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

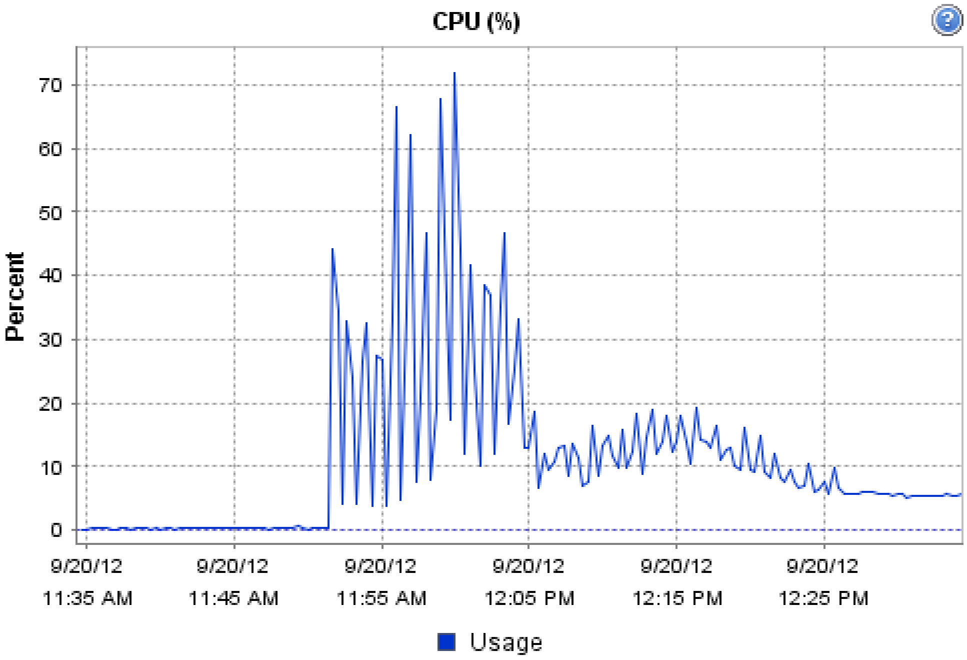
Appendix B—Server Performance Metrics for 500 Users on 4 Cisco UCS C220 M3 Servers

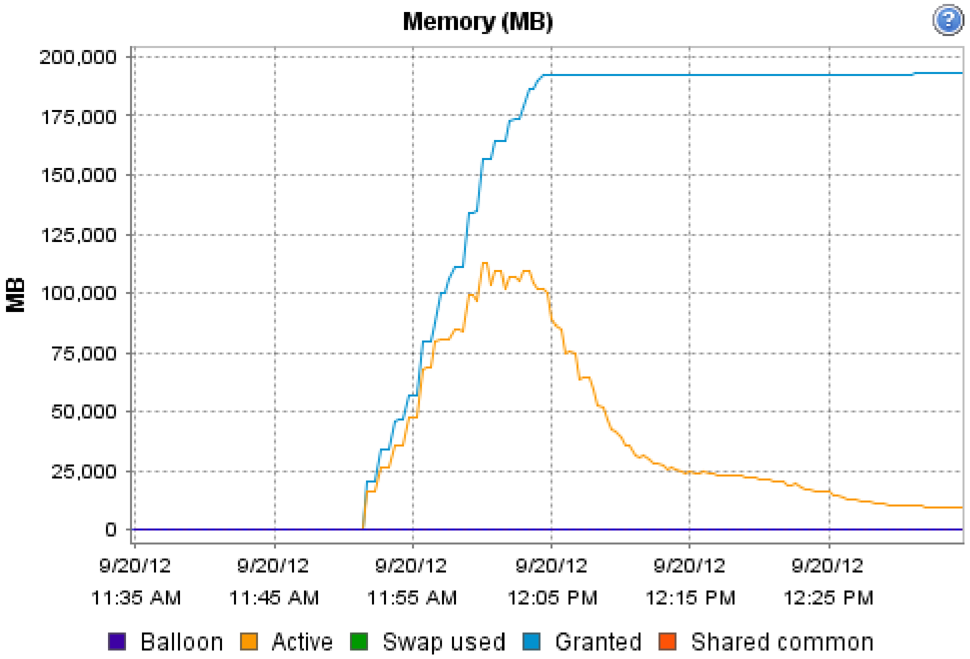


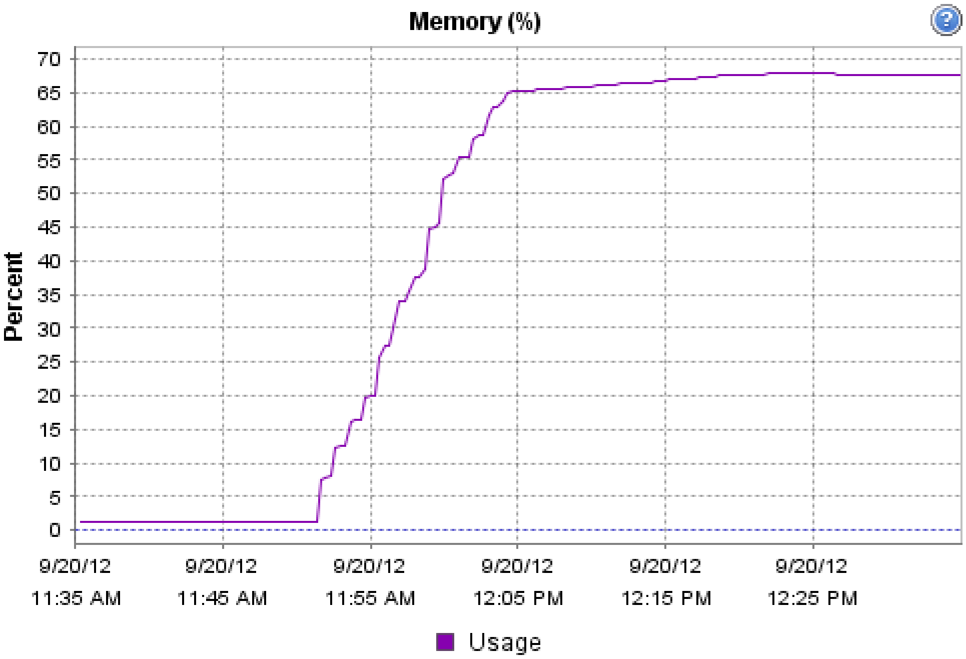


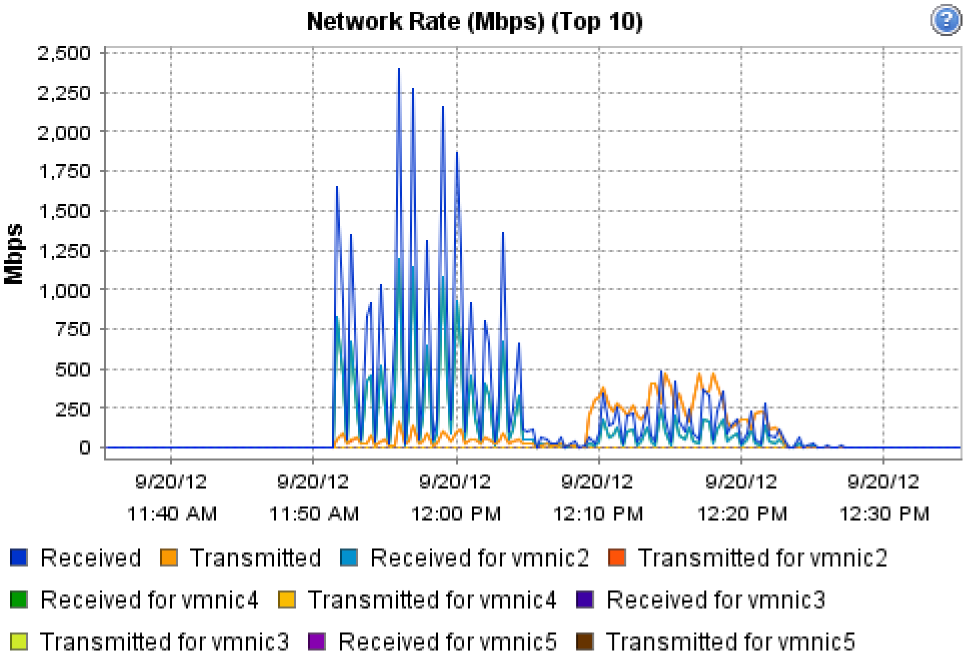

Memory (%)
Percent
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:35 AM
9/20/12 11:45 AM
9/20/12 11:55 AM
9/20/12 12:05 PM
9/20/12 12:15 PM
9/20/12 12:25 PM
Usage

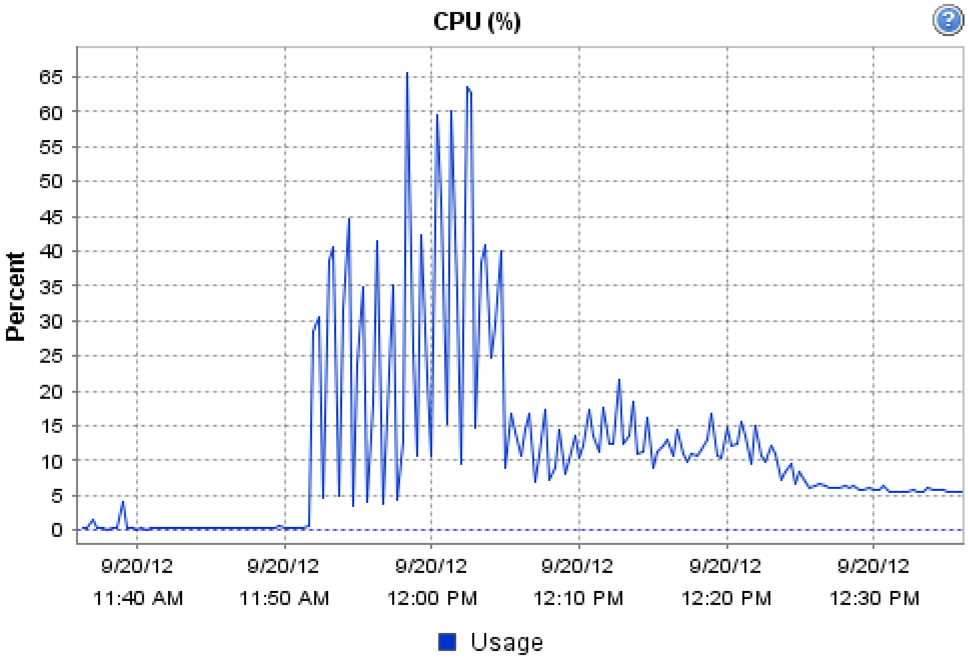

Network Rate (Mbps) (Top 10)
Mbps
2,000
1,750
1,500
1,250
1,000
750
500
250
0
9/20/12 11:35 AM
9/20/12 11:45 AM
9/20/12 11:55 AM
9/20/12 12:05 PM
9/20/12 12:15 PM
9/20/12 12:25 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

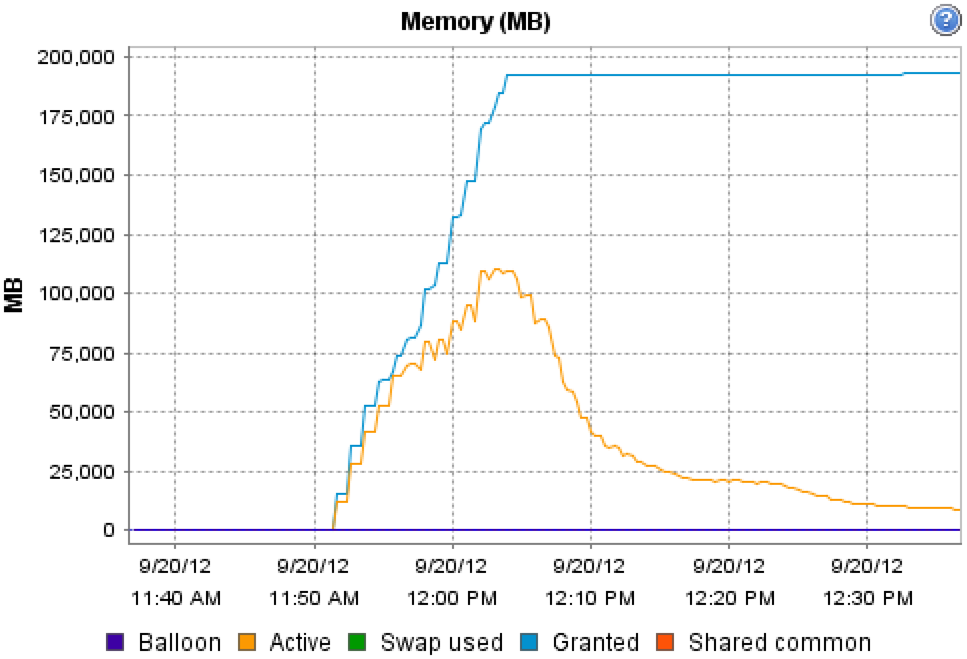

CPU (%)
Percent
70
60
50
40
30
20
10
0
9/20/12 11:35 AM
9/20/12 11:45 AM
9/20/12 11:55 AM
9/20/12 12:05 PM
9/20/12 12:15 PM
9/20/12 12:25 PM
Usage

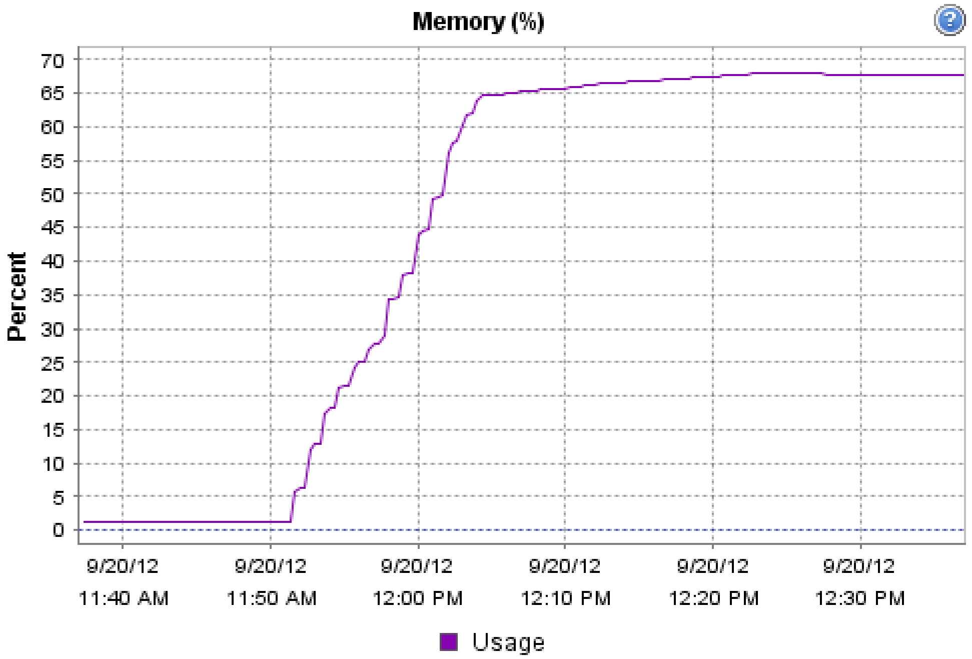

Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 11:35 AM
9/20/12 11:45 AM
9/20/12 11:55 AM
9/20/12 12:05 PM
9/20/12 12:15 PM
9/20/12 12:25 PM
Balloon
Active
Swap used
Granted
Shared common

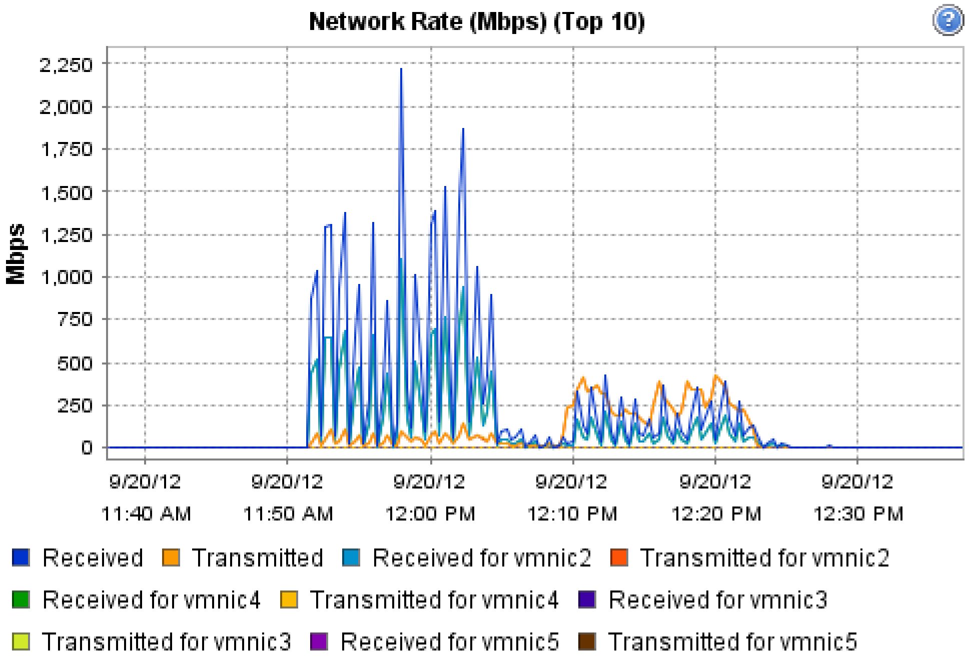

Memory (%)
Percent
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:35 AM
9/20/12 11:45 AM
9/20/12 11:55 AM
9/20/12 12:05 PM
9/20/12 12:15 PM
9/20/12 12:25 PM
Usage

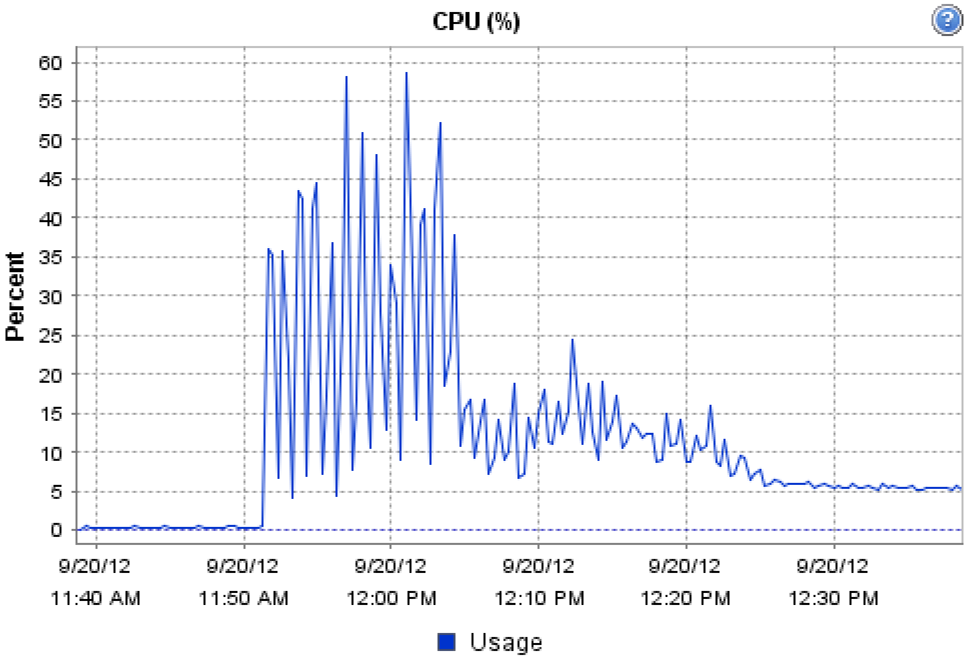

Network Rate (Mbps) (Top 10)
Mbps
2,500
2,250
2,000
1,750
1,500
1,250
1,000
750
500
250
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

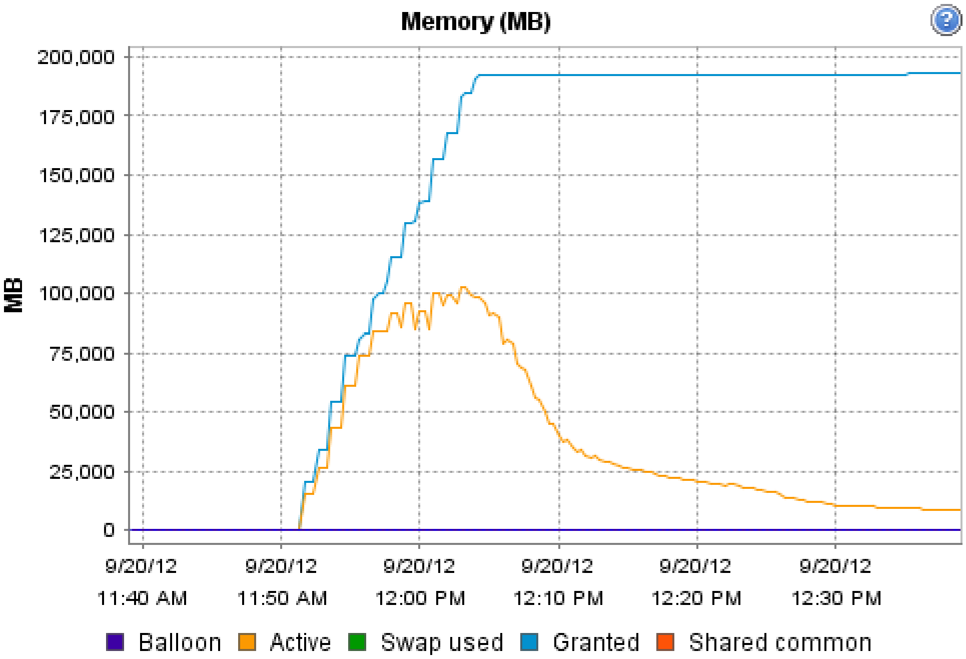

CPU (%)
Percent
65
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Usage

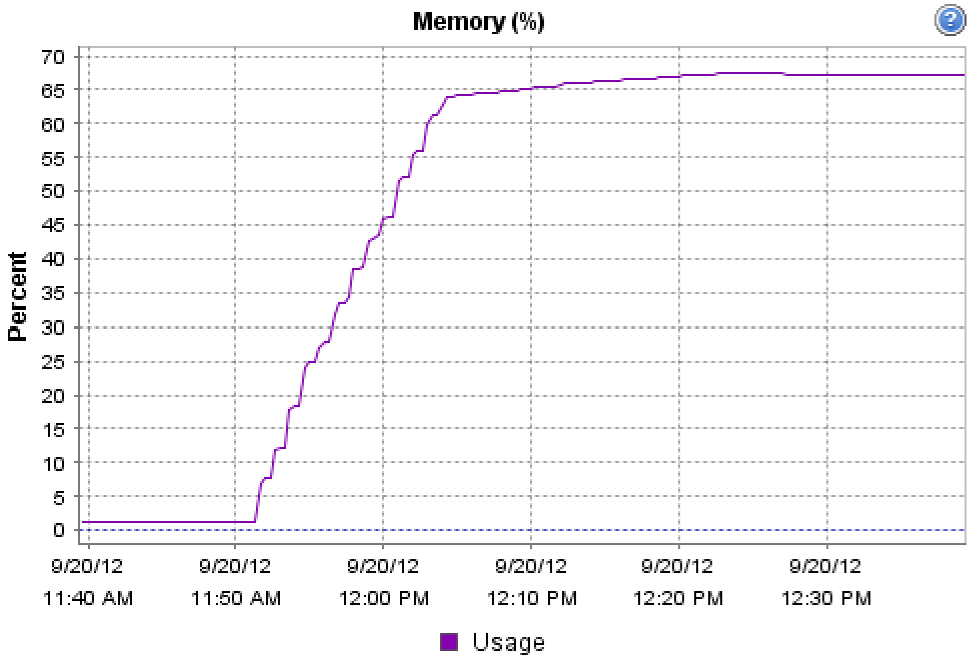

Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Balloon
Active
Swap used
Granted
Shared common

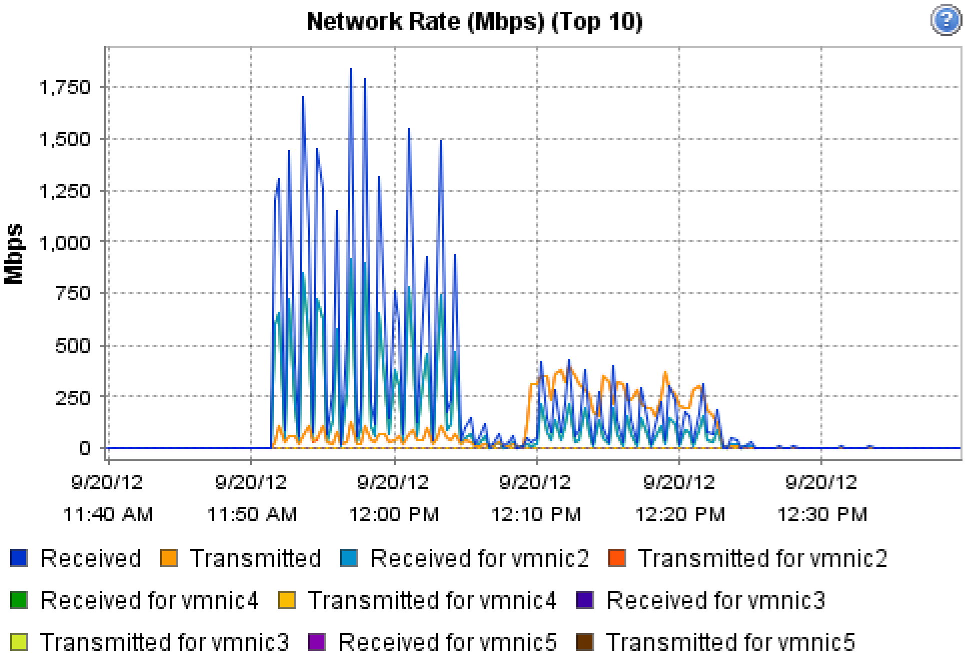

Memory (%)
Percent
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Usage

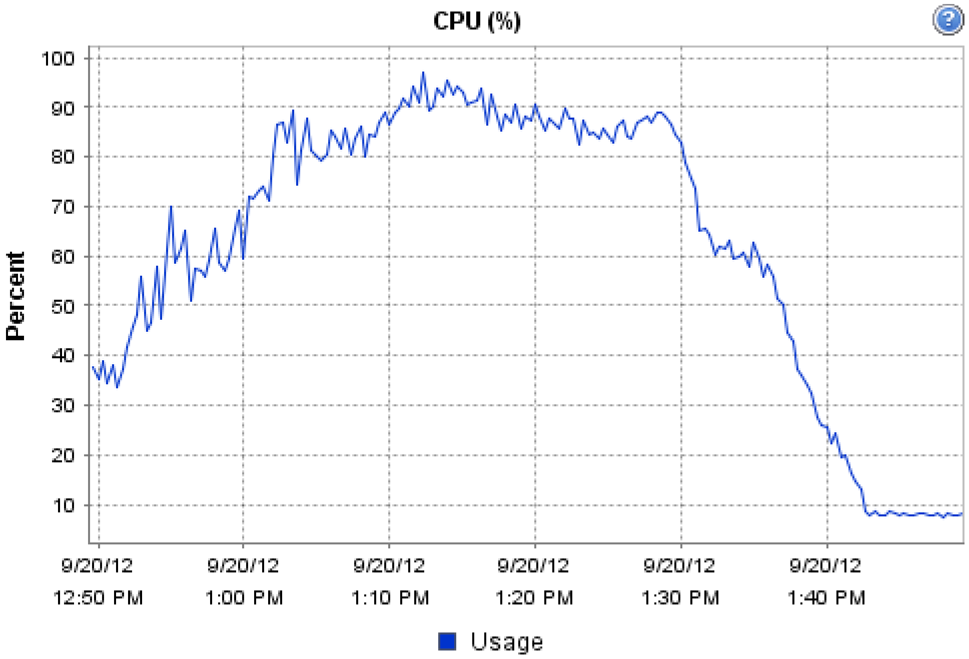

Network Rate (Mbps) (Top 10)
Mbps
2,250
2,000
1,750
1,500
1,250
1,000
750
500
250
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

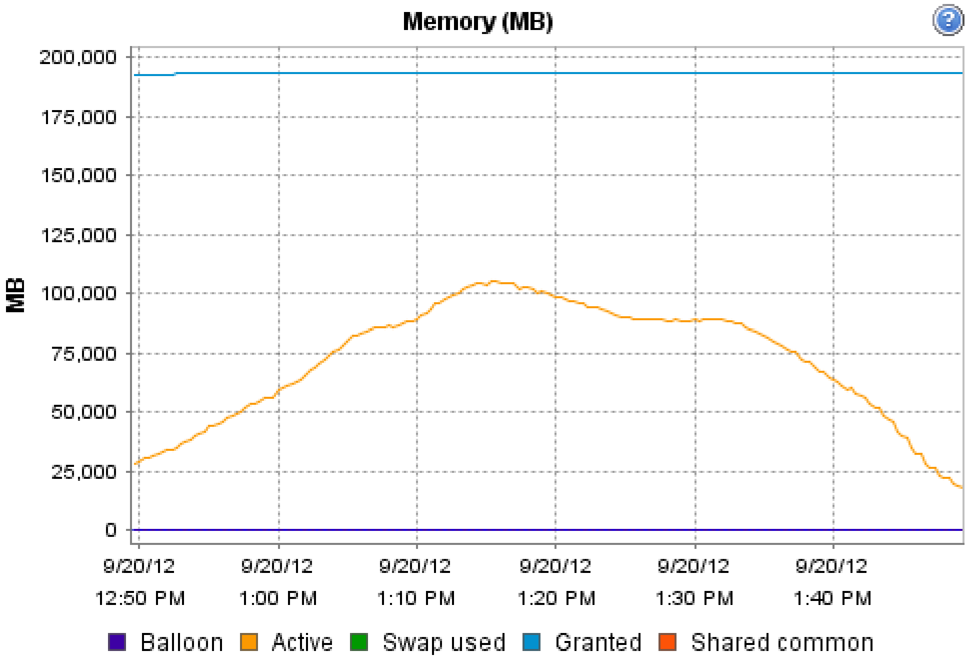

CPU (%)
Percent
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Usage

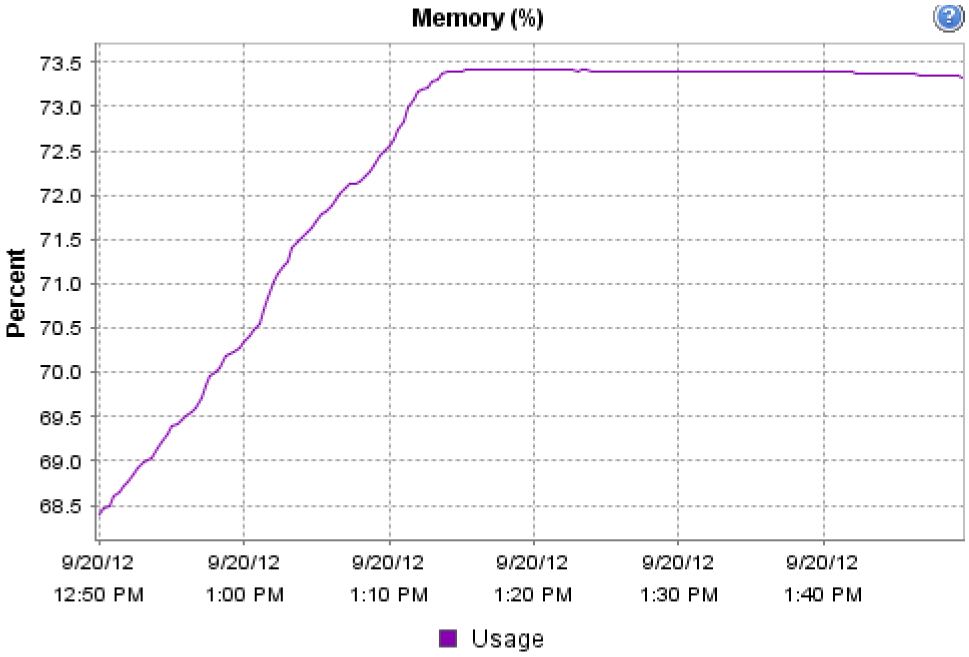

Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Balloon
Active
Swap used
Granted
Shared common

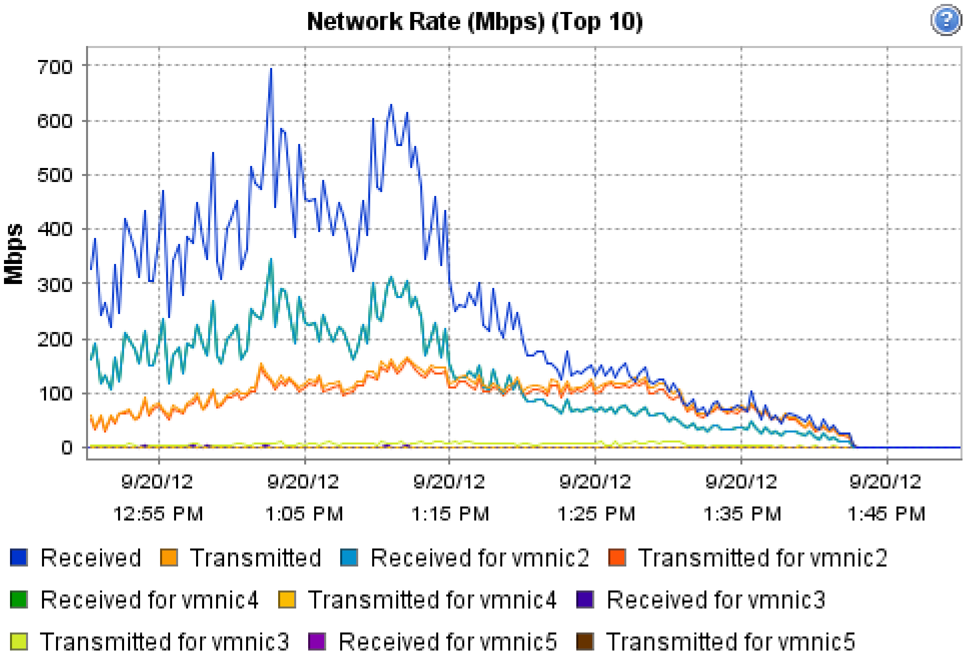

Memory (%)
Percent
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Usage

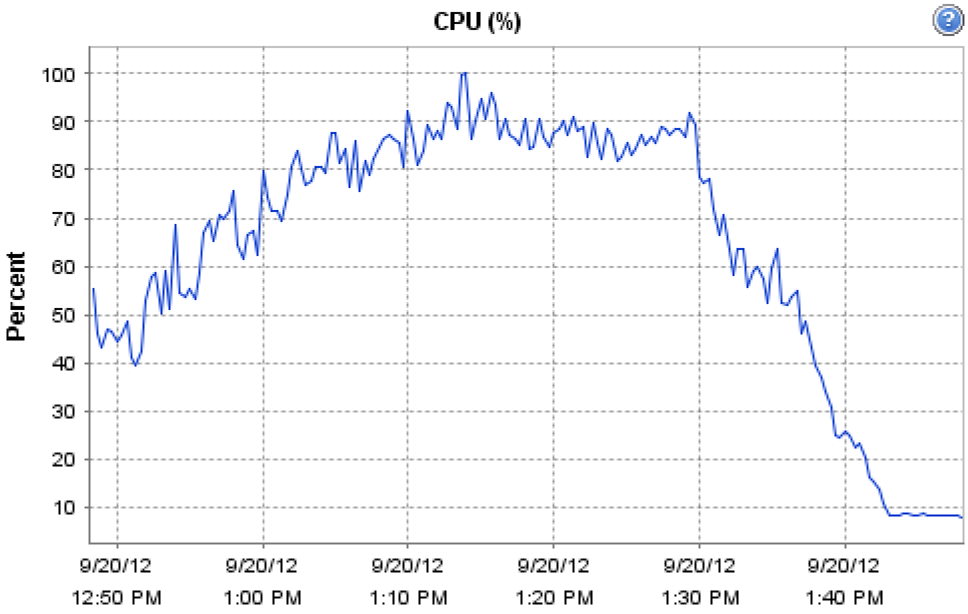

Network Rate (Mbps) (Top 10)
Mbps
1,750
1,500
1,250
1,000
750
500
250
0
9/20/12 11:40 AM
9/20/12 11:50 AM
9/20/12 12:00 PM
9/20/12 12:10 PM
9/20/12 12:20 PM
9/20/12 12:30 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

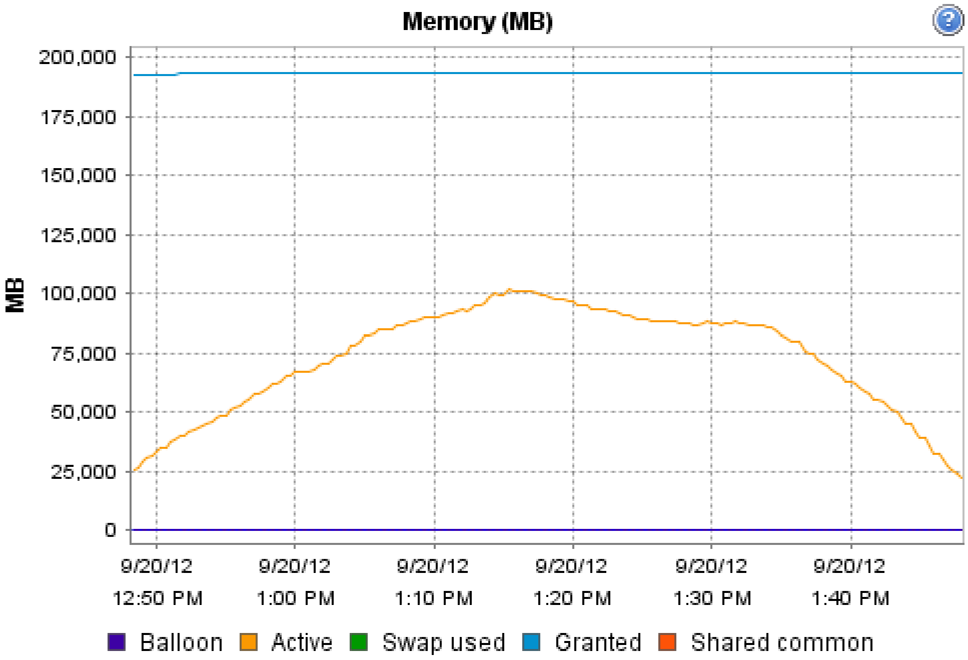

CPU (%)
Percent
100
90
80
70
60
50
40
30
20
10
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage

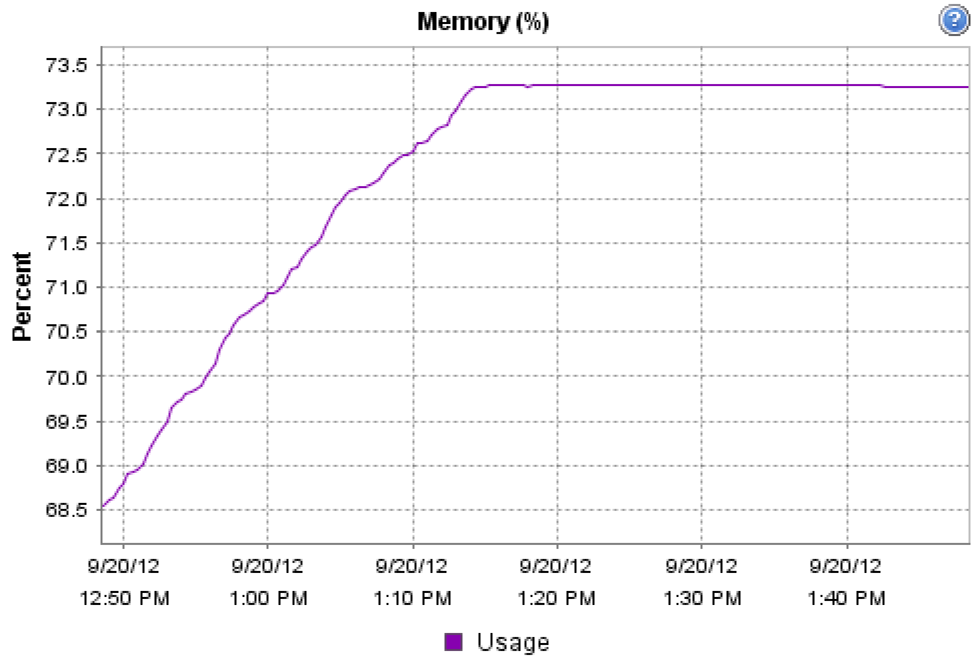

Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Balloon
Active
Swap used
Granted
Shared common

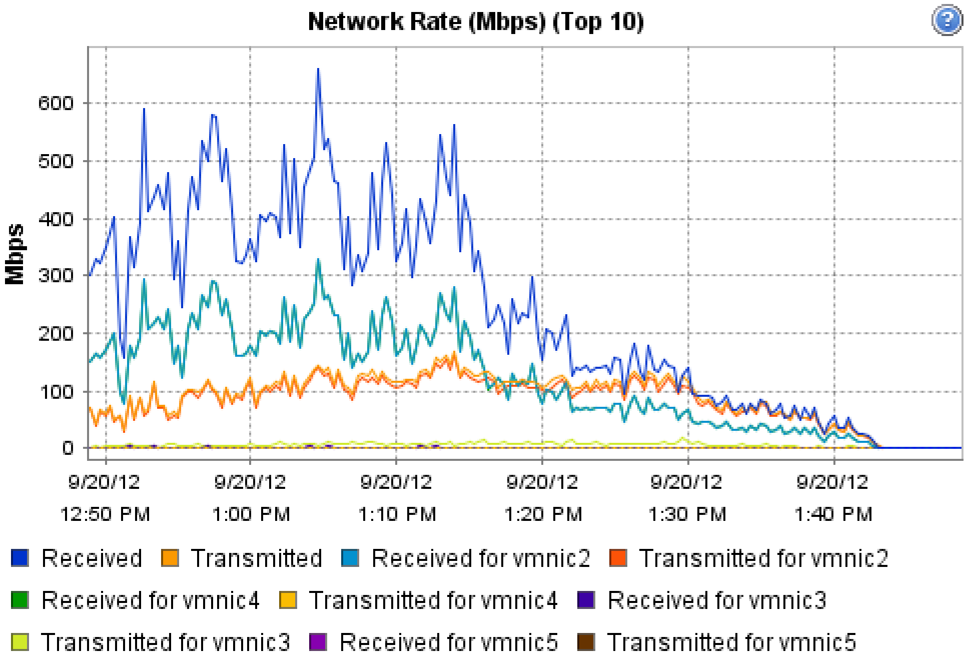

Memory (%)
Percent
73.5
73.0
72.5
72.0
71.5
71.0
70.5
70.0
69.5
69.0
68.5
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage

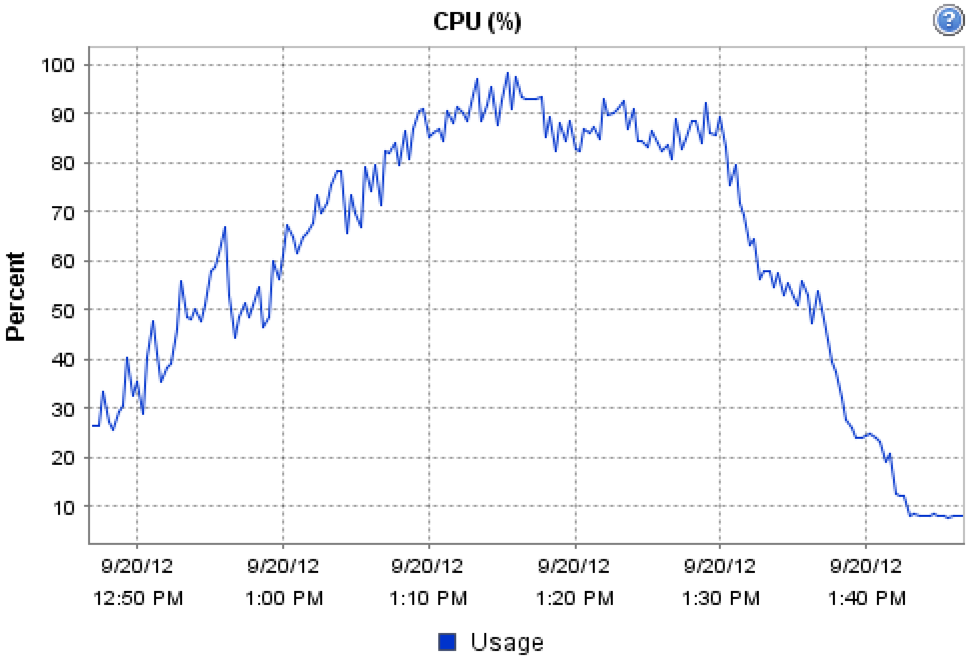

Network Rate (Mbps) (Top 10)
Mbps
700
600
500
400
300
200
100
0
9/20/12 12:55 PM
9/20/12 1:05 PM
9/20/12 1:15 PM
9/20/12 1:25 PM
9/20/12 1:35 PM
9/20/12 1:45 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

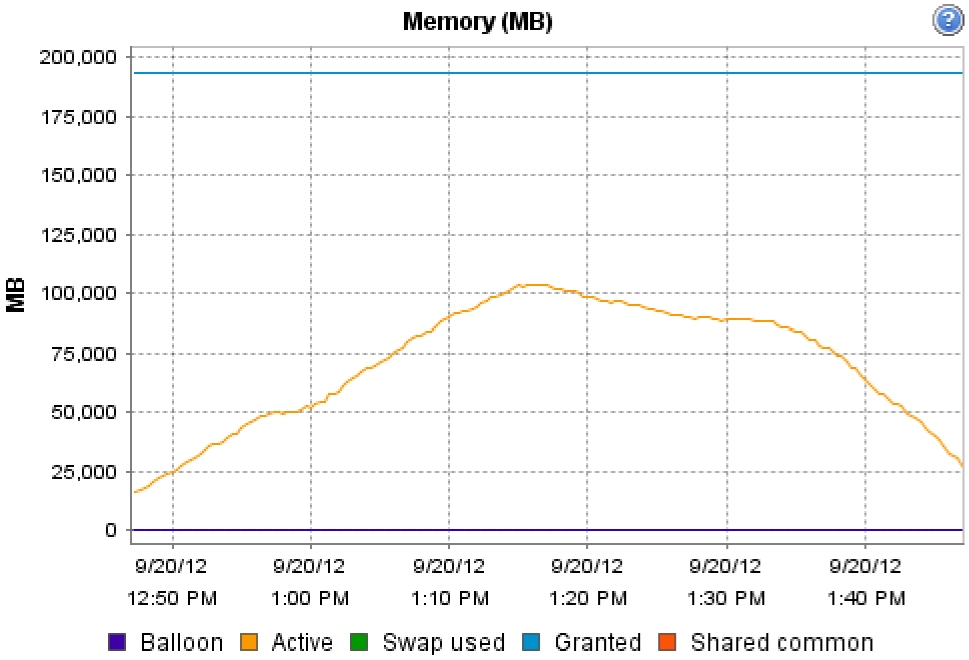

CPU (%)
?
Percent
100
90
80
70
60
50
40
30
20
10
9/20/12
12:50 PM
9/20/12
1:00 PM
9/20/12
1:10 PM
9/20/12
1:20 PM
9/20/12
1:30 PM
9/20/12
1:40 PM

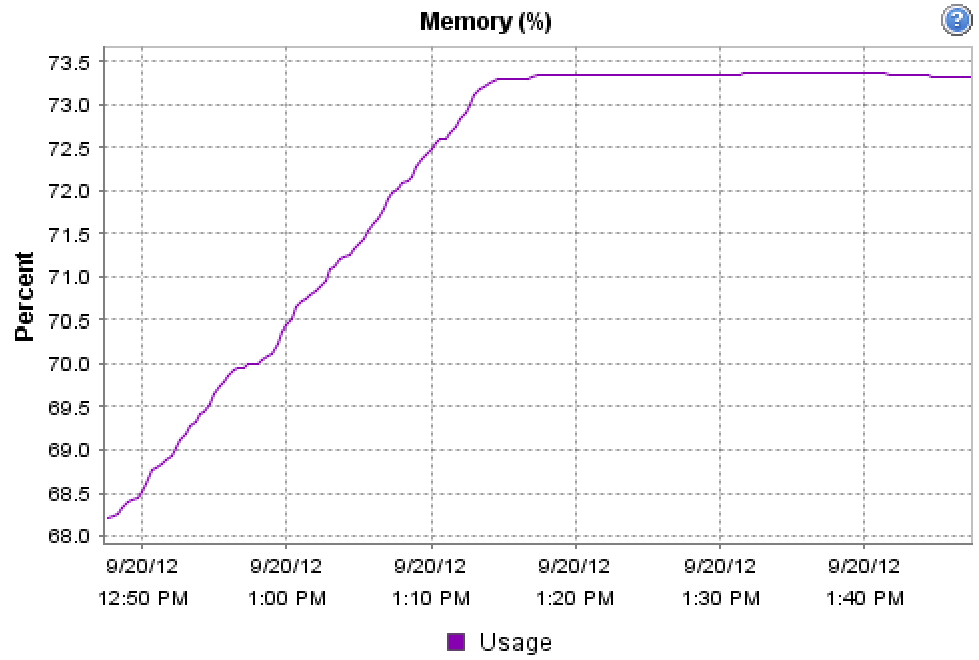

Memory (MB)
?
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12
12:50 PM
9/20/12
1:00 PM
9/20/12
1:10 PM
9/20/12
1:20 PM
9/20/12
1:30 PM
9/20/12
1:40 PM
Balloon
Active
Swap used
Granted
Shared common

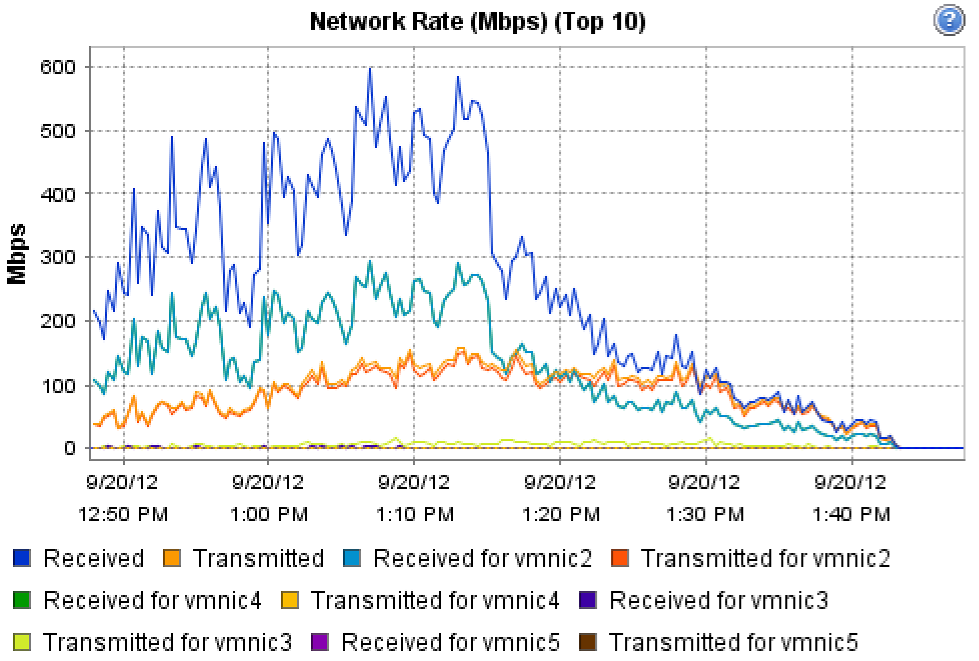

Memory (%)
Percent
73.5
73.0
72.5
72.0
71.5
71.0
70.5
70.0
69.5
69.0
68.5
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage

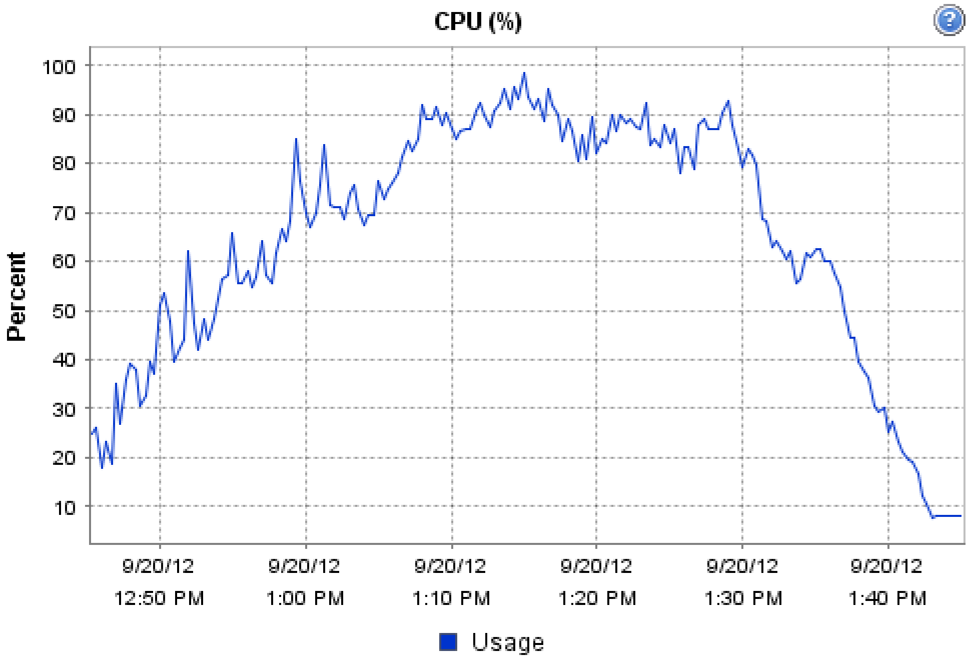

Network Rate (Mbps) (Top 10)
Mbps
600
500
400
300
200
100
0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5

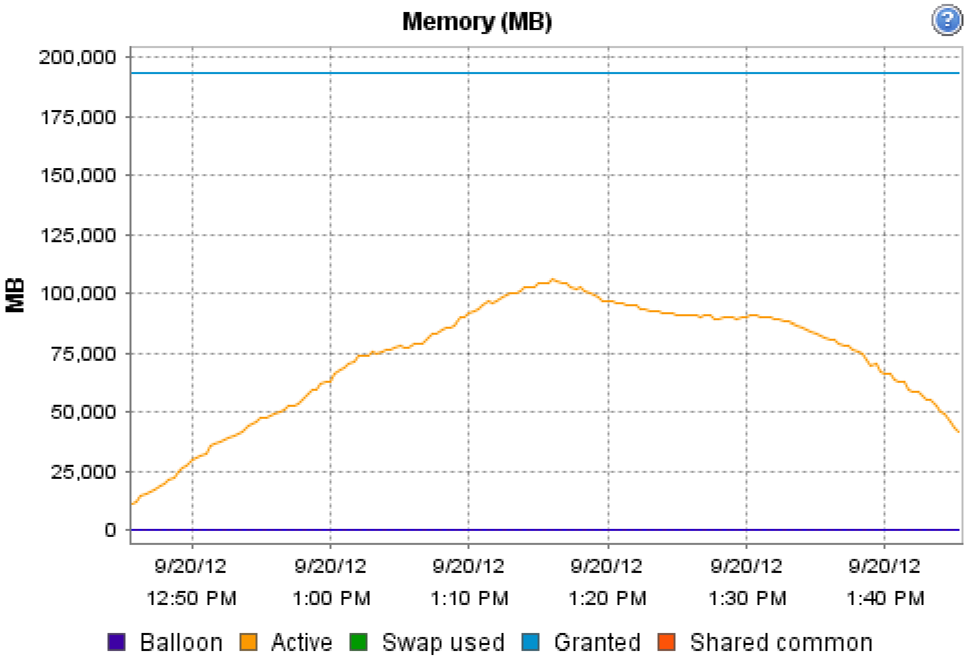

CPU (%)
Percent
100
90
80
70
60
50
40
30
20
10
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage

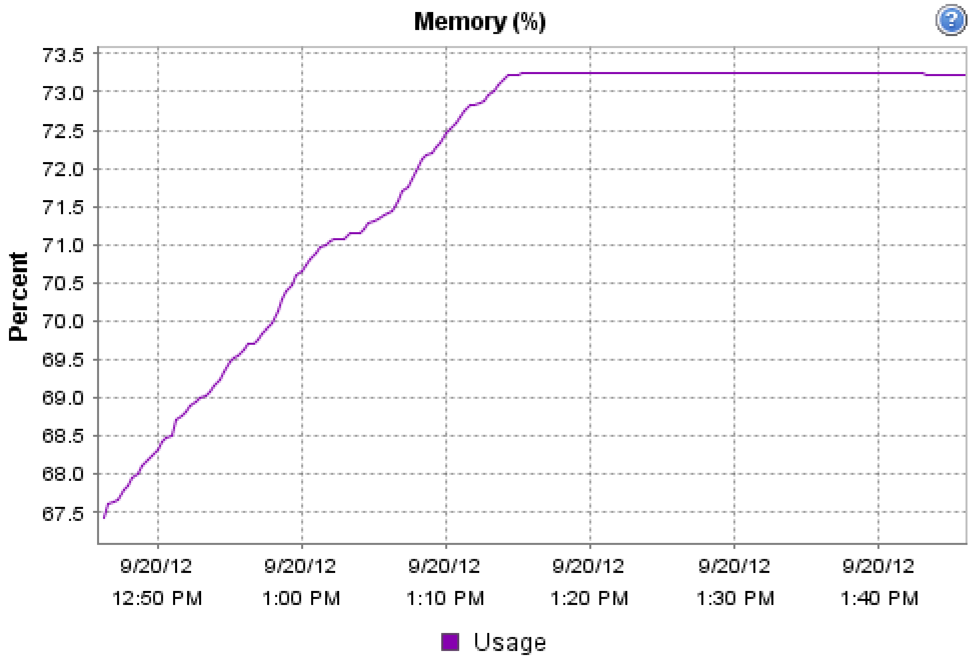

Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Balloon
Active
Swap used
Granted
Shared common

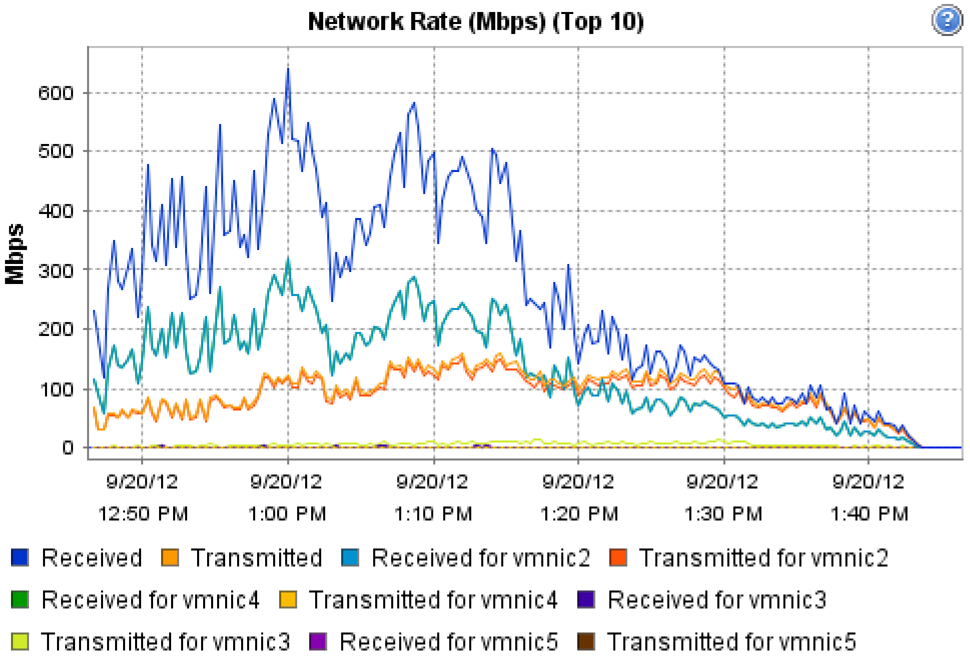

Memory (%)
Percent
73.5
73.0
72.5
72.0
71.5
71.0
70.5
70.0
69.5
69.0
68.5
68.0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage


Network Rate (Mbps) (Top 10)
Mbps
600
500
400
300
200
100
0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Received
Transmitted
Received for vmnic2
Transmitted for vmnic2
Received for vmnic4
Transmitted for vmnic4
Received for vmnic3
Transmitted for vmnic3
Received for vmnic5
Transmitted for vmnic5


CPU (%)
Percent
100
90
80
70
60
50
40
30
20
10
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Usage


Memory (MB)
MB
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
9/20/12 12:50 PM
9/20/12 1:00 PM
9/20/12 1:10 PM
9/20/12 1:20 PM
9/20/12 1:30 PM
9/20/12 1:40 PM
Balloon
Active
Swap used
Granted
Shared common





```
!Nexus 5548B NFS Variant VSPEX C500

!Command: show running-config
!Time: Wed Dec  9 23:12:09 2009

version 5.1(3)N1(1a)
```

```
hostname SJ2-B21-N5548-B

feature telnet
no feature http-server
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
feature fex

username admin password 5 $1$aWEymjJt$zqib1M7FZGO9ExVR6EHWg.  role
network-adminno password strength-check

banner motd #Nexus 5000 Switch
#

ip domain-lookup
ip domain-name cisco.com
ip name-server 171.70.168.183 171.68.226.120
system jumbomtu 9000
logging event link-status default
class-map type qos class-fcoe
class-map type qos match-any class-platinum
  match cos 5
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-platinum
  match qos-group 2
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
policy-map type qos jumbo
  class class-default
    set qos-group 0
policy-map type qos system_qos_policy
```

```
  class class-platinum
    set qos-group 2
  class class-default
    set qos-group 0
policy-map type queuing system_q_in_policy
  class type queuing class-platinum
    bandwidth percent 50
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 30
policy-map type queuing system_q_out_policy
  class type queuing class-platinum
    bandwidth percent 50
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 30
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-platinum
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos system_nq_policy
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos system_nq_policy
  class type network-qos class-platinum
    pause no-drop
    mtu 9000
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    mtu 9000
    multicast-optimize
```

```
system qos
  service-policy type qos input system_qos_policy
  service-policy type queuing input system_q_in_policy
  service-policy type queuing output system_q_out_policy
  service-policy type network-qos system_nq_policy
fex 130
  pinning max-links 1
  description "FEX0130"
snmp-server user admin network-admin auth md5
0x371b3192e7f154d1814e1748d100326c priv

0x371b3192e7f154d1814e1748d100326c localizedkey

vrf context management
  ip route 0.0.0.0/0 10.29.132.1
vlan 1
vlan 47
  name N1K-Mgmt
vlan 48
  name N1K-Ctrl
vlan 49
  name N1K-Pkt
vlan 50
  name Storage
vlan 51
  name vMotion
vlan 52
  name VDIAB
vlan 100
  name VDI
vlan 132
  name ESXi_Management
spanning-tree vlan 1,10-20,50-52,100,132 priority 20480
vpc domain 30
  role priority 4000
  peer-keepalive destination 10.29.132.7
```

```
interface Vlan1

interface Vlan50
  no shutdown
  ip address 10.10.50.2/24
  hsrp version 2
  hsrp 50

    preempt
    ip 10.10.50.1

interface Vlan51
  no shutdown
  ip address 10.10.51.2/24
  hsrp version 2
  hsrp 51
    preempt
    ip 10.10.51.1

interface Vlan52
  no shutdown
  ip address 10.10.52.2/24
  hsrp version 2
  hsrp 52
    preempt
    ip 10.10.52.1

interface Vlan100
  no shutdown
  ip address 10.10.1.2/22
  hsrp version 2
  hsrp 100
    preempt
    ip 10.10.1.1

interface port-channel2
  untagged cos 5
  switchport access vlan 50
  vpc 2

interface port-channel30
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  spanning-tree port type network
  vpc peer-link

interface Ethernet1/1
  switchport access vlan 132
  speed 1000

interface Ethernet1/2

interface Ethernet1/3
  description N1K-UplinkforInfraServers
  switchport access vlan 100

interface Ethernet1/4

interface Ethernet1/5
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/7
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/8
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/9
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/10
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26
interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29
  switchport mode fex-fabric
  fex associate 130

interface Ethernet1/30
  switchport mode fex-fabric
  fex associate 130

interface Ethernet1/31
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  channel-group 30 mode active

interface Ethernet1/32
  switchport mode trunk
  switchport trunk allowed vlan 47-52,100,132
  channel-group 30 mode active

interface Ethernet2/1
 description VNX-5300-10GB-UPLINK
  switchport access vlan 50
  channel-group 2 mode active

interface Ethernet2/2
  description VNX-5300-10GB-UPLINK
  switchport access vlan 50

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6
interface Ethernet2/7

interface Ethernet2/8

interface mgmt0
  ip address 10.29.132.6/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```