

Cisco Solution for EMC VSPEX End User Computing

For 2000 VMware Horizon View 5.2 Users

Last Updated: November 21, 2013



Building Architectures to Solve Business Problems

cisco.





About the Authors

About the Authors

Ramesh Guduru, Support Engineer, Cisco Systems

Ramesh Guduru is a Virtualization System Engineer at Cisco with SSVPG. Ramesh has over 7 years of experience with VMware view thin client administration, configuration and optimization of virtual desktop environment. Ramesh is skilled on core VMware applications in the virtual environment focusing in system design and implementation of virtualization components. Ramesh holds certification in virtualization, network and Microsoft.

Hardik Patel, Support Engineer, Cisco Systems

Hardik Patel is a Virtualization System Engineer at Cisco with SSVPG. Hardik has over 9 years of experience with server virtualization and core application in the virtual environment with area of focus in design and implementation of systems and virtualization, manage and administration, Cisco Unified Computing System, storage and network configurations. Hardik holds Masters degree in Computer Science with various career oriented certification in virtualization, network and Microsoft.

Acknowledgments

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

I

1

- Mike Brennan, Manager, Technical Marketing, Cisco Systems, Inc.
- Jason Ventresco, Solutions Engineer, Strategic Solutions Engineering, EMC
- Jack McMichael, EUC Technical Enablement, VMware

About Cisco Validated Design (CVD) Program

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

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

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

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

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

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

© 2013 Cisco Systems, Inc. All rights reserved

•1|1-1|1-CISCO

Cisco Solution for EMC VSPEX End User Computing

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 and reduce costs.

This Cisco Solution for EMC VSPEX End User Computing reports the results of a study evaluating the scalability of VMware Horizon View 5.2 environment on Cisco UCS B-Series B200 M3 Blade Servers running VMware ESXi 5.1 hypervisor software connected to an EMC VNX 5500 Storage Array. We utilize second and third generation Cisco Unified Computing System hardware and software. We provide best practice recommendations and sizing guidelines for large scale customer deployments of VMware Horizon View 5.2 on the Cisco Unified Computing System[™].

Audience

This document describes the architecture and deployment procedures of an infrastructure comprised of Cisco, EMC, and VMware hypervisor and desktop virtualization products. 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.

Solution Component 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

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

- Third generation Cisco UCS B-Series blade servers for infrastructure and virtual workload hosting
- Third generation 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
- Fabric Extender technology reduces the number of system components to purchase, configure and mainta
- 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
- Leverage Cisco UCS Management Packs for System Center 2012 for integrated management

Benefits of Nexus 5548UP

The Cisco Nexus 5548UP Switch 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:

- Cisco 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

Benefits of EMC VNX Family of Storage Controller

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

I

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

Benefits of VMware ESXi 5.1

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 VMware delivers on the core requirements for a business virtualization infrastructure solution:

- Built on a robust, reliable foundation
- Delivers a complete virtualization platform from desktop through the datacenter out to the public cloud
- · Provides the most comprehensive virtualization and cloud management
- Integrates with your overall IT infrastructure
- Proven with over 350,000 customers

And best of all, VMware provides:

• Low total-cost-of-ownership (TCO)

For detailed information about vSphere 5.1, go to:

http://www.vmware.com/files/pdf/products/vsphere/vmware-what-is-new-vsphere51.pdf

Benefits of VMware Horizon View 5.2

Deliver rich, personalized virtual desktops as a managed service from a virtualization platform built to deliver the entire desktop, including the operating system, applications and data. With Horizon View, desktop administrators virtualize the operating system, applications, and user data and deliver modern desktops to end-users. Get centralized automated management of these components for increased control and cost savings. Improve business agility while providing a flexible high performance desktop experience with VMware Horizon View, desktop administrators virtualize the operating system, applications, and user data and deliver modern desktops to end-users, across a variety of network conditions.

Deliver Business Agility

Bring the agility and availability of cloud computing to the desktop and applications with Horizon View. Built on VMware vSphere, Horizon View delivers desktops from a single integrated platform as part of your cloud services.

Dynamically allocate resources to enable highly responsive environment to end users. Scale up and down desktop services on demand to quickly meet changing business needs and proactively protect against planned and unplanned downtime. Run your desktops as business critical services for your workforce.

Easily Control and Manage Desktops

Increase control of desktops, applications and data by delivering and managing them as centralized services.

A single, powerful administrative console provides oversight of desktop services while enabling IT to simply execute previously cumbersome tasks like provisioning, updates and patches. Easily apply policies, quickly enable and disable users all from a centralized console for optimal business response. Free up time from maintenance for technology innovation.

Deliver a Better Desktop Experience

Unlike traditional PCs, View desktops are not tied to the physical computer. Instead, they reside in your cloud and end-users can access their View desktop when needed.

Horizon View with PCoIP delivers the richest, most flexible and adaptive experience for end-users around the world in a variety of network conditions. Business happens everywhere and whether online or offline, desktops or mobile devices, LAN or WAN, Horizon View delivers maximum workplace productivity.

Automate Desktop Operations Management

VMware vCenter Operations Manager for View allows administrators to gain insight into desktop and infrastructure performance, quickly pinpoint and troubleshoot issues. Administrators can optimize resource utilization, and proactively manage the desktop environment through the management dashboards. vCenter Operations Manager for View is an optional add-on for Horizon View customers. You can also leverage PCoIP Extension Services to collect Horizon View statistics into your existing WMI tool.

Built-in Security

Maintain control over data and intellectual property by keeping it secure in the datacenter. Encrypted protocol traffic provides secure end-users access virtual desktops inside or outside of the corporate network. Integration with vShield Endpoint enables offloaded and centralized anti-virus and anti-malware (AV) solutions. This integration helps to eliminate agent sprawl and AV storm issues while minimizing the risk of malware infection and simplifying AV administration. VMware View also supports integration with RSA SecureID for 2-factor authentication requirements.

Summary of Main Findings

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

- The combined power of the Cisco Unified Computing System, Nexus switching and EMC storage hardware with VMware ESXi 5.1, and VMware Horizon View 5.2 software produces a high density per blade and per chassis Virtual Desktop delivery system.
- Cisco UCS B200 M3 half-width blade with dual 8-core processors and 256GB of memory running at 1600 MHz supports 30% more virtual desktop workloads than the previously studied full width blade using a new medium workload with flash. In addition, density achieved with Horizon View 5.2 is equivalent to a prior study on the same platform with View 5.1 Update 2.

- The study design based on two Unified Computing System chassis, each with seven Cisco UCS B200 M3 blades, each with dual 8-core processors and 256GB of memory running at 1600 MHz and a Cisco VIC 1240 converged network adapter supports 2000 virtual desktop workloads running the new medium workload with flash providing outstanding End User Experience with average response times under 1.75 seconds at full load.
- Able to boot the full complement of 2000 virtual desktops (ready to login) in under 20 minutes.
- Able to ramp up (log in and start workloads) to steady state with all 2000 users running a knowledge worker workload with flash in 30 minutes without pegging the processor, exhausting memory or storage subsystems.
- Our design provides N+1 server fault tolerance for the 2000 virtual desktop system, making the design fully fault tolerant from end to end.
- Compared to previous studies with full width blades, the rack space required to support 2000 users was reduced from 30 Rack Units to 12 Rack Units.
- Pure Virtualization: We continue to present a validated design that is 100% virtualized on ESXi 5.1. All of the Windows 7 SP1 virtual desktops and supporting infrastructure components, including vCenter, Active Directory, Profile Servers, SQL Servers, and Horizon View 5.2 components were hosted as virtual servers.
- Maintained our industry leadership with our new Cisco UCS Manager 2.1(1b) 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 as we run more challenging workload testing, maintaining unsurpassed user response times.
- EMC's VNX5500 system provides storage consolidation and outstanding efficiency. Both block and file bases storage resources are available on a single system, utilizing EMC Fast Cache technology.
- VMware Horizon View 5.2 with the Sparse Virtual Disk feature used for floating assignment linked clones provided better disk performance and space efficiency.

Architecture

Deployed Hardware

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 Cisco UCS Domain) and out (adding additional Cisco UCS Domains and VNX Storage arrays).

The 2000 User Horizon View 5.2 solution includes Cisco networking, Cisco Unified Computing System and EMC storage, all of which fits in two data center racks (one for the EMC VNX and one for the Cisco networking and Cisco UCS gear.) In fact, there is adequate rack space in the Cisco rack to add blades and chassis to support an additional 4000 users

This document details the deployment of VMware Horizon View 5.2 floating assignment linked clones on VMware ESXi 5.1. Cisco Nexus 1000V distributed switch manages the two VMware Clusters hosting the virtual desktops, insuring end-to-end Quality of Service and ease of management by the network team.



Figure 1 VMware Horizon View 5.2 2000 User Hardware Components

The reference configuration includes:

- Two Cisco Nexus 5548UP switches with 16-universal port Expansion Modules (Optional)
- Two Cisco UCS 6248 Series Fabric Interconnects with Cisco UCS 6200 16-universal port Expansion Modules (Optional)
- Two Cisco UCS 5108 Blade Server Chassis with two 2204XP IO Modules per chassis
- Fourteen Cisco UCS B200 M3 Blade Servers with Intel E5-2690 processors, 256 GB RAM, and VIC 1240 mezzanine cards for Horizon View 5.2 virtual desktops (providing N+1 Server fault tolerance for the system)
- One EMC VNX5500 dual controller storage system for HA
- Two Cisco UCS B200 M3 Blade Servers with Intel E5-2650 processors, 96 GB RAM, and VIC 1240 mezzanine card for infrastructure (not shown in the drawing above)

The EMC VNX5500 disk shelf, disk and Fast Cache configurations are detailed in section "Storage Architecture Design" later in this document.

Software Revisions

Table 1

```
Software Used in this Deployment
```

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric	2.1 (1a)	Embedded Management
	Interconnect		
	Cisco UCS B200 M3		
		2.1 (1b)	Hardware BIOS
Network	Nexus 5500 Switch	5.2(1)N1(1)	Operating System Version
Storage	EMC VNX5500	05.32.000.6.203 Block	Operating System Version
		7.1.65-8 File	
Software	Cisco UCS Blade Hosts	VMware ESXi 5.1	Operating System Version
	Cisco Nexus 1000V	4.2(1)SV1(5.2)	Virtual Switch appliance
			version

Configuration Guidelines

The 2000 User Horizon View 5.2 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 VMware Horizon View 5.2 customer environment as stand-alone solution.

VLANs

For the 2000 User Horizon View 5.2 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
VDA	122	Virtual Desktops	No
MGMT	164	ESXi, N1KV	Yes
		Management	
INFRA	165	Infrastructure VMs	No
N1K-Control	167	N1KV Control	No
N1K-Packet	168	N1KV Packet	No
vMOTION	169	vMotion	No

VMware Clusters

Four VMware Clusters were used to support the solution and testing environment:

- Infrastructure Cluster (vCenter, Active Directory, DNS, DHCP, SQL Clusters, VMware View Connection Servers, View Composer, and Nexus 1000V Virtual Switch Manager appliances, etc.)
- VDA Clusters (2) (Windows 7 SP1 32-bit pooled virtual desktops; 1000 per cluster per VMware best practices recommended Horizon View 5.2 desktop cluster density.)
- Launcher Cluster (The Login Consultants Login VSI launcher infrastructure was hosted on the same Cisco UCS Domain sharing switching, but running on local storage).

Infrastructure Components

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

Cisco Unified Computing System

Cisco Unified Computing System (UCS) 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.

1

Cisco Unified Computing System Components

Cisco UCS components are shown in Figure 2.

Figure 2 Cisco Unified Computing System Components



Cisco Solution for EMC VSPEX End User Computing

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.

Fabric Interconnect

Cisco UCS Fabric Interconnects create a unified network fabric throughout the Cisco Unified Computing System. 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.

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 1Tbps 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+.

Cisco UCS 6248UP 48-Port Fabric Interconnects were used in this study.

Cisco UCS 2200 Series IO Module

The Cisco UCS 2100/2200 Series FEX multiplexes and forwards all traffic from blade servers in a chassis to a parent Cisco UCS Fabric Interconnect over from 10-Gbps unified fabric links. All traffic, even traffic between blades on the same chassis, or VMs on the same blade, is forwarded to the parent interconnect, where network profiles are managed efficiently and effectively by the Fabric Interconnect. At the core of the Cisco UCS Fabric Extender are ASIC processors developed by Cisco that multiplex all traffic.



Up to two fabric extenders can be placed in a blade chassis.

Cisco UCS 2104 has eight 10GBASE-KR connections to the blade chassis mid-plane, with one connection per fabric extender for each of the chassis' eight half slots. This gives each half-slot blade server access to each of two 10-Gbps unified fabric-based networks via SFP+ sockets for both throughput and redundancy. It has 4 ports connecting up the fabric interconnect.

Cisco UCS 2208 has thirty-two 10GBASE-KR connections to the blade chassis midplane, with one connection per fabric extender for each of the chassis' eight half slots. This gives each half-slot blade server access to each of two 4x10-Gbps unified fabric-based networks via SFP+ sockets for both throughput and redundancy. It has 8 ports connecting up the fabric interconnect.

Note

Cisco UCS 2208 fabric extenders were utilized in this study.

Cisco UCS Chassis

The Cisco UCS 5108 Series Blade Server Chassis is a 6 RU blade chassis that will accept up to eight half-width Cisco UCS B-Series Blade Servers or up to four full-width Cisco UCS B-Series Blade Servers, or a combination of the two. The Cisco UCS 5108 Series Blade Server Chassis can accept four redundant power supplies with automatic load-sharing and failover and two Cisco UCS (either 2100 or 2200 series) Fabric Extenders. The chassis is managed by Cisco UCS Chassis Management Controllers, which are mounted in the Cisco UCS Fabric Extenders and work in conjunction with the Cisco UCS Manager to control the chassis and its components.

A single Cisco UCS managed domain can theoretically scale to up to 40 individual chassis and 320 blade servers. At this time Cisco supports up to 20 individual chassis and 160 blade servers.

Basing the I/O infrastructure on a 10-Gbps unified network fabric allows the Cisco UCS to have a streamlined chassis with a simple yet comprehensive set of I/O options. The result is a chassis that has only five basic components:

- The physical chassis with passive midplane and active environmental monitoring circuitry
- Four power supply bays with power entry in the rear, and hot-swappable power supply units accessible from the front panel
- Eight hot-swappable fan trays, each with two fans
- Two fabric extender slots accessible from the back panel
- Eight blade server slots accessible from the front panel

Cisco UCS B200 M3 Blade Server

Cisco UCS B200 M3 is a third generation half-slot, two-socket Blade Server. The Cisco UCS B200 M3 harnesses the power of the latest Intel® Xeon® processor E5-2600 product family, with up to 384 GB of RAM (using 16-GB DIMMs), two optional SAS/SATA/SSD disk drives, and up to dual 4x 10 Gigabit Ethernet throughput, utilizing our VIC 1240 LAN on motherboard (LOM) design. The Cisco UCS B200 M3 further extends the capabilities of Cisco UCS by delivering new levels of manageability, performance, energy efficiency, reliability, security, and I/O bandwidth for enterprise-class virtualization and other mainstream data center workloads.

Cisco UCS VIC1240 Converged Network Adapter

A Cisco innovation, the Cisco UCS Virtual Interface Card (VIC) 1240 (Figure 1) is a 4-port 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed exclusively for the M3 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional Port Expander, the Cisco UCS VIC 1240 capabilities can be expanded to eight ports of 10 Gigabit Ethernet.

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

Figure 3 Cisco UCS VIC1240 Converged Network Adapter







The Cisco UCS VIC1240 virtual interface cards are deployed in the Cisco UCS B-Series B200 M3 blade servers.

VMware Horizon View

VMware Horizon View (formerly known as VMware View) simplifies desktop and application management while increasing security and control. Horizon View delivers a personalized high fidelity experience for end-users across sessions and devices. It enables higher availability and agility of desktop services unmatched by traditional PCs while reducing the total cost of desktop ownership up to 50 percent. End-users can enjoy new levels of productivity and the freedom to access desktops from more devices and locations while giving IT greater policy control.

Horizon View 5.2 Features

Horizon View delivers rich, personalized virtual desktops as a managed service from a virtualization platform built to deliver the entire desktop, including the operating system, applications and data. With VMware Horizon View, desktop administrators virtualize the operating system, applications, and user data and deliver modern desktops to end-users. Get centralized automated management of these components for increased control and cost savings. Improve business agility while providing a flexible high performance desktop experience for end-users, across a variety of network conditions.

Automated Desktop Provisioning

Horizon View Manager provides a single management tool for greater IT efficiency to provision new desktops or groups of desktops, and an easy interface for setting desktop policies. Using a template, you can customize virtual pools of desktops and easily set policies, such as how many virtual machines can be in a pool, or logoff parameters.

Streamlined Application Management

VMware ThinApp application virtualization separates applications from underlying operating systems and reduces conflict between the OS and other applications for increased compatibility and streamlined management. Applications packaged with ThinApp can be run centrally from the datacenter, deployed locally to physical or virtual desktops or on USB drives for deployment flexibility.

Advanced Virtual Desktop Image Management

Horizon View Composer enables the rapid creation of desktop images from a golden image. Updates are instant and guaranteed across any number of virtual desktops. When combined with ThinApp, IT administrators can reduce the number of total images, storage requirements and operational costs.

Automate Desktop Operations Management

VMware vCenter Operations Manager for View allows administrators to gain insight into desktop and infrastructure performance, quickly pinpoint and troubleshoot issues. Administrators can optimize resource utilization, and proactively manage the desktop environment through the management dashboards. vCenter Operations Manager for View is an optional add-on for Horizon View customers. You can also leverage PCoIP Extension Services to collect Horizon View statistics into your existing WMI tool.

Efficient Resource Utilization

Horizon View Storage Accelerator optimizes storage load by caching common image blocks when reading virtual desktop images. Space Efficient Disks continuously reduce the storage needed per desktop. Both these technologies improve storage capacity and utilization, thereby reducing costs of additional hardware.

Built-in Security

Maintain control over data and intellectual property by keeping it secure in the datacenter. Encrypted protocol traffic provides secure end-users access virtual desktops inside or outside of the corporate network. Integration with vShield Endpoint enables offloaded and centralized anti-virus and anti-malware (AV) solutions. To eliminate agent sprawl and AV storm issues, risk of malware infection, and simplify AV administration. Horizon View also supports integration with Radius 2-factor authentication requirements.

Enhancements in Horizon View 5.2

VMware Horizon View 5.2 continues to build upon the advancements released in Horizon View 5.2. TCO was further reduced by optimizing storage reads, improved desktop migration and large scale management, and further enhanced the user-experience with lower bandwidth and client diversity.

Lower Total Cost of Ownership

Space-efficient disks, native in vSphere, reduce storage costs and administrative overhead by efficiently using and reclaiming storage space to minimize Horizon View Composer image size. This lowers storage capacity requirements for persistent desktops and decreases the need to continuously recompose and restore images.

Simplified Management

Improved large-scale management allows customers with large Horizon View deployments to efficiently and logically manage their virtual desktop infrastructure. Overall desktop architecture is simplified with a single VMware vCenter ServerTM supporting up to 10,000 desktops in a pod. With support for 32 hosts per pool on VMFS along with NFS and pools spanning multiple VLANs, larger desktop pools can be created to decrease operational costs. Furthermore, View admin UI responsiveness increases and accelerates performance of operations such as provisioning, and rebalance improves the efficiency of the desktop administration team.

VMware vCenter Server virtual appliance support enables greater flexibility in Horizon View infrastructure deployment.

Seamless User Experience

Media services for rich 3D graphics add support for hardware accelerated 3D graphics for the most demanding 3D applications. By virtualizing the graphics processing unit (GPU), you can dedicate or share physical GPU resources across multiple users, providing a rich 3D experience from the data center. Using a combination of software and hardware-accelerated graphics, VMware Horizon View[™] provides the greatest flexibility for delivering 3D graphics for virtual desktops and workstation use cases. 3D graphics acceleration is built upon the VMware vSphere® platform. Only Horizon View is designed to fully leverage vSphere, expanding the value of combined solutions.

Horizon View media services already support unified communications for Cisco Unified Communications.

Horizon View HTML access enables users to access desktops based on Horizon View from HTML5-capable browsers to securely access their data and applications. Without requiring the installation of any software or plug-ins, end users conveniently can access their desktops on any device. With Horizon Workspace[™] integration, that same desktop convenience is expanded to provide end users access to their desktops, data and apps, all from a single location. Note: Horizon View HTML access is available in the Horizon View feature pack.

VMware Horizon View Clients for iOS and Android with Unity make it easier than ever to access Windows applications on your iPhone, iPad or Android device. Remove the frustration of working with Windows on mobile devices with a new mobile native user interface. With Unity users can easily browse, search, and open Windows applications and files, set applications and files as favorites, and easily switch between running applications.

Windows 8 support gives users ability to use the latest OS inside their virtual desktops. Horizon View Client has also been updated to run on the latest Windows 8 devices.

VMware Horizon View 5.2 Hosted Virtual Desktop Overview

Hosted Virtual Desktop (HVD) uses a hypervisor to host all the desktops in the data center.

Three types of HVD pools are available with Horizon View 5.2: Automated, Manual, and Terminal Services Pools. These pool types are discussed below.

- Automated HVD pools use Horizon View Composer to create some number of HVDs. HVD users can be assigned as floating or dedicated users. Floating users will be assigned randomly to HVDs as they log on. Once the user logs off, the HVD is available for any other user. Dedicated user assignments insure that a user is provided the same HVD each time he or she connects to the Horizon View Connection server. Automated pools can utilize the PCoIP protocol and View Persona Management.
- Automated HVD pools can create two types of HVDs: Full virtual machines created from a vCenter template or Horizon View Composer linked clones which share the same base image and use less storage.
- Manual HVD pools provide access to an existing set of HVDs. Any type of machine that can install the Horizon View Agent is supported. Examples could include vCenter virtual machines, physical machines, or blade PCs. Manual pools support the PCoIP protocol, View Persona Management, and Local Mode.
- Microsoft Terminal Services Pools provide Terminal Services sessions as desktops to Horizon View users. The Horizon View Connection Server manages these sessions in the same way it does for Automated or Manual HVD pools. Terminal Services Pools support View Persona Management.

For this study, we utilized Automated HVD pools with floating user assignments and Horizon View Composer linked clones over the PCoIP protocol.



View Persona Manager was not deployed.

The following figure shows the logical architecture for a Horizon View 5.2 deployment, including the optional related product; Thin App. Thin App provides application streaming capability and is not included in this study.



Figure 4 VMware Horizon View 5.2 Architecture

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 AtmosTM 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 (FAST VP is not part of the FAST Suite for VNX5100TM).
 - 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.
 - VNX Total Value Pack-Includes all three protection software suites and the Security and Compliance Suite (VNX5100 exclusively supports this package).

EMC VNX5500 Used in Testing

EMC VNX 5500 is a unified storage platform for multi-protocol file, block and object storage. It is powered by Intel quad-core Xeon 5500 series processors and delivers five 9's availability. It is designed to deliver maximum performance and scalability for enterprise and mid-tier companies, enabling them to dramatically grow, share, and cost-effectively manage multi-protocol file and block systems. It supports up to 250 drives and three X-Blades (also known as Data Movers) for file protocol support. This solution was validated Fibre Channel for hypervisor SAN boot, data storage of virtual desktops, SQL database, and infrastructure virtual machines such Horizon View Connection Servers, Horizon View Composer Servers, VMware vCenter Servers, and other supporting services. An NFS or iSCSI variant could be deployed on the VNX5500 using NFS or iSCSI for data storage of virtual desktops.

VMware ESXi 5.1

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

VMware on ESXi 5.1 Hypervisor

ESXi 5.1 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.

1

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.

Modular Virtual Desktop Infrastructure Technical Overview

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 5). 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.





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

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 6).

Figure 6 VMware Horizon View 5.2 on Cisco Unified Computing System



Simplified

Cisco Unified Computing System 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 Unified Computing System 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 Unified Computing System along with the reduced cabling and port count due to the unified fabric and unified ports of Cisco Unified Computing System and desktop virtualization data center infrastructure.

Simplification also leads to improved and more rapid success of a desktop virtualization implementation. Cisco and its partners -VMware and EMC - have developed integrated, validated architectures, including available pre-defined, validated infrastructure packages, known as Cisco Solutions for EMC VSPEX End User Computing.

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 Unified Computing System 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.

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 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.

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 resulting in fewer servers required, 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.

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 as follows:

• 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 (for example, 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 (for example, 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 (for example, 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 (for example, 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.

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.

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?

1

- 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 Thin App be used for streamed applications or will all applications be installed in the image?
- Will you use floating assignment or assigned user desktops?
- Will you use linked clone or full copy desktops?
- How will you manage user persona?
- 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?

Proof of Concept Pilot Program

To validate what you have learned during your analysis, create an isolated Proof of Concept environment to test the various workloads and validate your sizing calculations.

Then create a Pilot environment and get users from each user group who can exercise all of the organizations key applications. Use the pilot user feedback to further refine you design in preparation for production roll out.

Failure to follow these key steps will make a successful virtual desktop deployment project nearly impossible.

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

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

To meet the challenges of designing and implementing a modular desktop infrastructure, Cisco, 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

Cisco Networking Infrastructure

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

Cisco Nexus 5548 Switch

The Cisco Nexus 5548UP is a 1-RU 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 that accept modules and cables meeting the Small Form-Factor Pluggable Plus (SFP+) standard and one expansion slot. Expansion slot options include:

- Ethernet module that provides sixteen 1/10 Gigabit Ethernet and FCoE ports using the SFP+ interface.
- Fibre Channel plus Ethernet module that provides eight 1/10 Gigabit Ethernet and FCoE ports using the SFP+ interface, and eight ports of 8/4/2/1-Gbps native Fibre Channel connectivity using the SFP+/SFP interface.
- Unified port module that provides up to sixteen 1/10 Gigabit Ethernet and FCoE ports using the SFP+ interface or up to sixteen ports of 8/4/2/1-Gbps native Fibre Channel connectivity using the SFP+ and SFP interfaces; the use of 1/10 Gigabit Ethernet or 8/4/2/1-Gbps Fibre Channel on a port is mutually exclusive but can be selected for any of the 16 physical ports per module.
- Four port QSFP Ethernet module that provides 4 40 Gigabit Ethernet ports using QSFP interface.

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.

Cisco Nexus 5500 Series Feature Highlights

The switch family's rich feature set makes the series ideal for rack-level, access-layer applications. It protects investments in data center racks with standards-based Ethernet and FCoE features that allow IT departments to consolidate networks based on their own requirements and timing.

- The combination of high port density, wire-speed performance, and extremely low latency makes the switch an ideal product to meet the growing demand for 10 Gigabit Ethernet at the rack level. The switch family has sufficient port density to support single or multiple racks fully populated with blade and rack-mount servers.
- Built for today's data centers, the switches are designed just like the servers they support. Ports and power connections are at the rear, closer to server ports, helping keep cable lengths as short and efficient as possible. Hot-swappable power and cooling modules can be accessed from the front panel, where status lights offer an at-a-glance view of switch operation. Front-to-back cooling is

consistent with server designs, supporting efficient data center hot-aisle and cold-aisle designs. Serviceability is enhanced with all customer replaceable units accessible from the front panel. The use of SFP+ ports offers increased flexibility to use a range of interconnect solutions, including copper for short runs and fibre for long runs.

• FCoE and IEEE data center bridging features support I/O consolidation, ease management of multiple traffic flows, and optimize performance. Although implementing SAN consolidation requires only the lossless fabric provided by the Ethernet pause mechanism, the Cisco Nexus 5500 Series switches provide additional features that create an even more easily managed, high-performance, unified network fabric.

Features and Benefits

This sections details the specific features and benefits provided by the Cisco Nexus 5500 Series.

10GB Ethernet, FCoE, and Unified Fabric Features

The switch series, using cut-through architecture, supports line-rate 10 Gigabit Ethernet on all ports while maintaining consistently low latency independent of packet size and services enabled. It supports a set of network technologies known collectively as Data Center Bridging (DCB) that increases the reliability, efficiency, and scalability of Ethernet networks. These features allow the switches to support multiple traffic classes over a lossless Ethernet fabric, thus enabling consolidation of LAN, SAN, and cluster environments. Its ability to connect Fibre Channel over Ethernet (FCoE) to native Fibre Channel protects existing storage system investments while dramatically simplifying in-rack cabling.

Low Latency

The cut-through switching technology used in the Cisco Nexus 5500 Series ASICs enables the product to offer a low latency of 3.2 microseconds, which remains constant regardless of the size of the packet being switched. This latency was measured on fully configured interfaces, with access control lists (ACLs), QoS, and all other data path features turned on. The low latency on the Cisco Nexus 5500 Series enables application-to-application latency on the order of 10 microseconds (depending on the NIC). These numbers, together with the congestion management features described in the next section, make the Cisco Nexus 5500 Series a great choice for latency-sensitive environments.

Other Features

Other Nexus 5548UP features include: Nonblocking Line-Rate Performance, Single-Stage Fabric, Congestion Management, Virtual Output Queues, Lossless Ethernet (Priority Flow Control), Delayed Drop FC over Ethernet, Hardware-Level I/O Consolidation, and End-Port Virtualization.

Cisco Nexus 1000V Feature Highlight

Cisco Nexus 1000V Series Switches are virtual machine access switches that are an intelligent software switch implementation based on IEEE 802.1Q standard for VMware vSphere environments running the Cisco® NX-OS Software operating system. Operating inside the VMware ESX hypervisor, the Cisco Nexus 1000V Series supports Cisco VN-Link server virtualization technology to provide:

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

With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the virtual machine access layer to the core of the data center network infrastructure. Virtual servers can now use the same network configuration, security policy, diagnostic tools, and operational models as their physical server counterparts attached to dedicated physical network ports. Virtualization administrators can access pre-defined network policy that follows mobile virtual machines to help ensure proper connectivity, saving valuable time for virtual machine administration.

Developed in close collaboration with VMware, the Cisco Nexus 1000V Series is certified by VMware to be compatible with VMware vSphere, vCenter, ESX, and ESXi, and with many other vSphere features. You can use the Cisco Nexus 1000V Series to manage your virtual machine connectivity with confidence in the integrity of the server virtualization infrastructure.

The Cisco Nexus 1000V Release 2.1 software is being offered in two editions:

- Cisco Nexus 1000V Essential Edition: This is available at no cost and provides most of the comprehensive Layer 2 networking features of the Cisco Nexus 1000V Series, including VXLAN, Cisco vPath for service insertion and chaining, and VMware vCloud Director integration.
- Cisco Nexus 1000V Advanced Edition: This version offers value-added security features such as Domain Host Control Protocol (DHCP) snooping, IP source guard, Dynamic Address Resolution Protocol (ARP) Inspection, and Cisco TrustSec® Secure Group Access (SGA) support (a new feature in Release 2.1). The Cisco VSG zone-based virtual firewall is also included in the Advanced Edition.

Cisco Nexus 1000V Product Architecture

Cisco Nexus 1000V Series Switches have two major components: the Virtual Ethernet Module (VEM), which runs inside the hypervisor, and the external Virtual Supervisor Module (VSM), which manages the VEMs.

Virtual Ethernet Module (VEM)

The Cisco Nexus 1000V Series VEM runs as part of the VMware ESX or ESXi kernel and replaces the VMware virtual switch (vSwitch). This level of integration helps ensure that the Cisco Nexus 1000V Series is fully aware of all server virtualization events, such as VMware vMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the VSM and provides advanced networking functions: quality of service (QoS), security features, and monitoring features.

Virtual Supervisor Module (VSM)

The Cisco Nexus 1000V Series VSM controls multiple VEMs as one logical modular switch. Configuration is performed through the VSM and is automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on a host-by-host basis administrators can define configurations for immediate use on all VEMs being managed by the VSM from a single interface.

Cisco Nexus 1000V Features and Benefits

The Cisco Nexus 1000V Series provides a common management model for both physical and virtual network infrastructures through Cisco VN-Link technology, which includes policy-based virtual machine connectivity, mobility of virtual machine security and network properties, and a non-disruptive operational model.

Policy-Based Virtual Machine Connectivity

To facilitate easy creation and provisioning of virtual machines, the Cisco Nexus 1000V Series includes port profiles. Port profiles enable you to define virtual machine network policies for different types or classes of virtual machines and then apply the profiles through the VMware vCenter. Port profiles are a scalable mechanism for configuring networks with large numbers of virtual machines. When the Port Profiles include QoS and security policies, they formulate a complete service-level agreement (SLA) for the virtual machine's traffic.

Mobility of Virtual Machine Security and Network Properties

Network and security policies defined in the port profile follow the virtual machine throughout its lifecycle, whether it is being migrated from one server to another, suspended, hibernated, or restarted. In addition to migrating the policy, the Cisco Nexus 1000V Series VSM moves the virtual machine's network state. Virtual machines participating in traffic-monitoring activities can continue these activities uninterrupted by VMware vMotion operations. When a specific port profile is updated, the Cisco Nexus 1000V Series automatically provides live updates to all the virtual ports using that same port profile. The capability to migrate network and security policies through VMware vMotion makes regulatory compliance much easier to enforce with the Cisco Nexus 1000V Series because the security policy is defined in the same way as for physical servers and is constantly enforced by the switch.

Besides traditional switching capability, the Cisco Nexus 1000V Series offers the Cisco vPath architecture to support virtualized network services with:

- Intelligent Traffic Steering: This feature redirects packets in a network flow to a virtual service virtual machine called a Virtual Service Node (VSN), which can be on a different server. Thus, a VSN is not required on every server, providing flexible and consolidated deployment.
- Performance Acceleration: VEM caches the VSN's decision for a flow, implements the service in all subsequent packets of the flow, and accelerates virtualized network service in the hypervisor kernel.

Cisco Virtual Service Gateway (VSG) is the first VSN to leverage the Cisco vPath architecture and provides multi-tenant, scalable, security services for virtual machines on the Cisco Nexus 1000V Series Switches.

Non-disruptive Operational Model

Because of its close integration with VMware vCenter, the Cisco Nexus 1000V Series allows virtualization administrators to continue using VMware tools to provision virtual machines. At the same time, network administrators can provision and operate the virtual machine network the same way they do the physical network. While both teams work independently, the Cisco Nexus 1000V Series enforces consistent configuration and policy throughout the server virtualization environment. This level of integration lowers the cost of ownership while supporting organizational boundaries among server, network, security, and storage teams.

Inside VMware vCenter, virtual machines are configured as before. For network configuration, port profiles defined on the Cisco Nexus 1000V Series VSM are displayed by VMware vCenter as port groups. Virtualization administrators can take advantage of preconfigured port groups and focus on virtual machine management, and network administrators can use port profiles to apply policy for a large number of ports at the same time. Together, both teams can deploy server virtualization more efficiently and with lower operating costs.

Enhanced Deployment Scenarios

• Optimized server bandwidth for I/O-intensive applications: Today, network interfaces are often dedicated to a particular type of traffic, such as VMware Console or vMotion. With the Cisco Nexus 1000V Series, all network interface cards (NICs) can be treated as a single logical channel with QoS attached to each type of traffic. Consequently, the bandwidth to the server can be more efficiently utilized, with network-intensive applica-tions virtualized.

- Easier security audits with consistent security policy: Security audits on virtual machines are usually more difficult to perform because virtual machines are secured differently than physical servers. As the Cisco Nexus 1000V Series provides persistent security policy to mobile virtual machines, security audits are similar to those for physical servers.
- Virtual machine as basic building block of data center: With the Cisco Nexus 1000V Series, virtual machines are treated the same way as physical servers in security policy, monitoring and troubleshooting, and the operational model between network and server administrators, enabling virtual machines to be true basic building blocks of the data center. These operational efficiencies lead to greater scaling of server virtualization deployments with lower operating expenses.

VMware Product Compatibility

The Cisco Nexus 1000V Series is compatible with VMware vSphere as a VMware vNetwork Distributed Switch (vDS) with support for VMware ESX and ESXi hypervisors and integration with VMware vCenter Server. Cisco Nexus 1000V Series Switches are compatible with the various VMware vSphere features.

Architecture and Design of Horizon View 5.2 on Cisco Unified Computing System and EMC VNX Storage

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.

1

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 (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.

Hosted Virtual Desktop Design Fundamentals

This section details how the VMware Horizon View 5.2 can be used to deliver a variety of virtual desktop configurations.

Choosing a Display Protocol

A display protocol provides end users with a graphical interface to a View desktop that resides in the datacenter. You can use PCoIP (PC-over-IP), which VMware provides, or Microsoft RDP (Remote Desktop Protocol.)

You can set policies to control which protocol is used or to allow end users to choose the protocol when they login to a desktop.

Note

For this study, the PCoIP protocol was used.

VMware View with PCoIP

PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to make sure that end users can remain productive regardless of network conditions.

PCoIP is supported as the display protocol for View desktops with virtual machines and with physical machines that contain Teradici host cards.

PCoIP Features

Key features of PCoIP include the following:

- For users outside the corporate firewall, you can use this protocol with your company's virtual private network or with View security servers.
- Advanced Encryption Standard (AES) 128-bit encryption is supported and is turned on by default.
- Connections from all types of View clients. For more information, go to:

http://pubs.vmware.com/view-52/index.jsp?topic=/com.vmware.view.planning.doc/GUID-43E5EE F5-72D9-4CCA-8439-66D6FD6D1A1F.html

- USB redirection is supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN is supported.
- Optimization controls for reducing bandwidth usage on the LAN and WAN.
- Multiple monitors are supported. You can use up to four monitors and adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per display. Pivot display and autofit are also supported. When the 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920x1200.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Copy and paste of text and images between a local Windows client system and the desktop is supported, up to 1MB. Supported file formats include text, images, and RTF (Rich Text Format). You cannot copy and paste system objects such as folders and files between systems.

Video Quality

- 480p-formatted video You can play video at 480p or lower at native resolutions when the View desktop has a single virtual CPU. If the operating system is Windows 7 and you want to play the video in high-definition Flash or in full screen mode, the desktop requires a dual virtual CPU.
- 720p-formatted video You can play video at 720p at native resolutions if the View desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.
- 1080p-formatted video If the View desktop has a dual virtual CPU, you can play 1080p formatted video, although the media player might need to be adjusted to a smaller window size.
- 3D If you plan to use 3D applications such as Windows Aero themes or Google Earth, the Windows 7 View desktop must have virtual hardware version 8, available with vSphere 5 and later. You must also turn on the pool setting called Windows 7 3D Rendering. Up to 2 monitors are supported, and the maximum screen resolution is 1920 x 1200. This non-hardware accelerated graphics feature enables you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical graphics processing unit (GPU).

Recommended Guest Settings

Recommended guest operating system settings include the following settings:

- For Windows XP desktops: 768MB RAM or more and a single CPU
- For Windows 7 desktops: 1GB of RAM and a dual CPU

Microsoft RDP

Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

Microsoft RDP provides the following features:

- With RDP 6, you can use multiple monitors in span mode. RDP 7 has true multiple monitor support, for up to 16 monitors.
- You can copy and paste text and system objects such as folders and files between the local system and the View desktop.
- RDP supports 32-bit color.
- RDP supports 128-bit encryption.
- You can use this protocol for making secure, encrypted connections to a View security server in the corporate DMZ.
- The following are the RDP-related requirements and considerations for different Windows operating systems and features: For Windows XP and Windows XP Embedded systems, you should use Microsoft RDC 6.x.
- Windows Vista comes with RDC 6.x installed, though RDC 7 is recommended.
- Windows 7 comes with RDC 7 installed. Windows 7 SP1 comes with RDC 7.1 installed.
- You must have RDC 6.0 or later to use multiple monitors.
- For Windows XP desktop virtual machines, you must install the RDP patches listed in Microsoft Knowledge Base (KB) articles 323497 and 884020. If you do not install the RDP patches, a Windows Sockets failed error message might appear on the client.
- The View Agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.



You can download RDC versions from the Microsoft website.

Recommended Guest Settings

Client hardware requirements include the following:

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
- ARM processor with NEON (preferred) or WMMX2 extensions, with a 600MHz or higher processor speed.
- 128 MB RAM

Choose a User Profile Management System

There are a number of options for managing user profiles for HVDs. The two methods we considered for this study were Microsoft Roaming User Profiles and View Persona Manager. It is important to select and deploy a method so that user settings for software applications and user preferences are maintained, particularly for floating desktops. Both methods are discussed briefly below. (We used Microsoft Roaming User Profiles in the study.)

Microsoft Roaming User Profiles and Folder Redirection

This technology has been around for more than a dozen years. It was significantly enhanced with the introduction of Windows Vista and updated again with Windows 7. Version two (v2) roaming profiles were introduced, adding 8 additional folders that can be redirected. This greatly reduces the time it takes to load the user's profile during logon. Using Roaming User Profiles and Folder redirection require a network shares that all users have access to during the virtual desktop session. The user must have read and write access to their profile folder and folder redirection folder, which get created on first login after Roaming User Profiles is configured.

Utilizing Microsoft Active Directory Group Policy is the recommended method for providing Roaming User Profiles and Folder Redirection to your users. See the article titled Managing Roaming User Data Deployment Guide at the following url for details on how to configure both Roaming User Profiles and Folder Redirection:

http://technet.microsoft.com/en-us/library/cc766489%28WS.10%29.aspx



The significant changes to Roaming User Profiles and Folder redirection applies to Microsoft Windows 7 and Microsoft Windows Vista.

VMware Persona Management

You can use View Persona Management with View desktops on physical computers and virtual machines that are not managed by View. View Persona Management retains changes that users make to their profiles. User profiles comprise a variety of user-generated information.

- User-specific data and desktop settings, which allow the desktop appearance to be the same regard less of which desktop a user logs in to.
- Application data and settings. For example, these settings allow applications to remember toolbar positions and preferences.
- Windows registry entries configured by user applications.

To facilitate these abilities, View Persona Management requires storage on a CIFS share equal or greater than the size of the user's local profile.

Minimizing Logon and Logoff Times

View Persona Management minimizes the time it takes to log on to and off of desktops.

- View takes recent changes in the profile on the View desktop and copies them to the remote repository at regular intervals. The default is every 10 minutes. In contrast, Windows roaming profiles wait until logoff time and copy all changes to the server at logoff.
- During logon, View downloads only the files that Windows requires, such as user registry files. Other files are copied to the View desktop when the user or an application opens them from the profile folder in the View desktop.
- With View Persona Management, during logoff, only files that were updated since the last replication are copied to the remote repository.

With View Persona Management, you can avoid making any changes to Active Directory in order to have a managed profile. To configure Persona Management, you specify a central repository, without changing the user's properties in Active Directory. With this central repository, you can manage a user's profile in one environment without affecting the physical machines that users might also log on to.
With View Persona Management, if you provision desktops with VMware ThinApp applications, the ThinApp sandbox data can also be stored in the user profile. This data can roam with the user but does not significantly affect logon times. This strategy provides better protection against data loss or corruption.

Configuration Options

You can configure View personas at several levels: a single View desktop, a desktop pool, an OU, or all View desktops in your deployment. You can also use a standalone version of View Persona Management on physical computers and virtual machines that are not managed by View.

By setting group policies (GPOs), you have granular control of the files and folders to include in a persona:

- Specify whether to include the local settings folder. For Windows 7 or Windows Vista, this policy affects the AppData\Local folder. For Windows XP, this policy affects the Local Settings folder.
- Specify which files and folders to load at login time. For example: Application Data\Microsoft\Certificates. Within a folder, you can also specify files to exclude.
- Specify which files and folders to download in the background after a user logs in to the desktop. Within a folder, you can also specify files to exclude.
- Specify which files and folders within a user's persona to manage with Windows roaming profiles functionality instead of View Persona Management. Within a folder, you can also specify files to exclude.

As with Windows roaming profiles, you can configure folder redirection. You can redirect the same folders that support redirection with Windows Roaming User Profiles.

Accessing USB Devices Connected to the End Point

Administrators can configure the ability to use USB devices, such as thumb flash drives, VoIP (voice-over-IP) devices, and printers, from a View desktop. This feature is called USB redirection. (It was not used in this study.)

When you use this feature, most USB devices that are attached to the local client system become available from a menu in View Client. You use the menu to connect and disconnect the devices.

You can specify which types of USB devices end users are allowed to connect to. For composite devices that contain multiple types of devices, such as a video input device and a storage device, you can split the device so that one device (for example, the video input device) is allowed but the other device (for example, the storage device) is not.

USB devices that do not appear in the menu, but are available in a View desktop, include smart card readers and human interface devices such as keyboards and pointing devices. The View desktop and the local computer use these devices at the same time.

This feature has the following limitations:

- When you access a USB device from a menu in View Client and use the device in a View desktop, you cannot access the device on the local computer.
- USB redirection is not supported on Windows 2000 systems or for View desktops sourced from Microsoft Terminal Servers.

Printing from a View Desktop

The virtual printing feature allows end users with View Client on Windows systems to use local or network printers from a View desktop without requiring that additional print drivers be installed in the View desktop.

The location-based printing feature allows you to map View desktops to the printer that is closest to the endpoint client device.

With virtual printing, after a printer is added on a local Windows computer, View adds that printer to the list of available printers on the View desktop. No further configuration is required. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on. Users who have administrator privileges can still install printer drivers on the View desktop without creating a conflict with the virtual printing component. To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature.

The location-based printing feature is available for both Windows and non-Windows client systems. Location based printing allows IT organizations to map View desktops to the printer that is closest to the endpoint client device. Using this feature does require that the correct printer drivers be installed in the View desktop.

We did not use virtual printing in this study. Our workload generator, Login VSI, installs a pdf printer into the master image which is utilized for printing during the test.

Other Features to Consider

Horizon View 5.2 supports these additional features that were not deployed in this study:

- Streaming Multimedia with Wyse MMR. (Only used for Windows XP environments.)
- Single Sign-On for Logging In (Workload generator initiates multiple sessions from a single workstation.)
- Multiple Monitor Support (Workload generator supports single monitor.)

Designing a VMware Horizon View 5.2 Deployment

There are several elements that go into the design of a successful Horizon View 5.2 environment. This section covers those topics at a high level. Readers should consult the VMware View Architecture Planning guide for Horizon View 5.2 at the following URL for more details: https://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-architecture-planning.pdf

Determine Desktop Pools Required

Based on the analysis performed on user groups and the applications identified that will be supported by the Hosted Virtual Desktop (HVD) environment, a strategy for laying out your desktop pool structure should be create.

For this study, a single user group (knowledge workers) will be tested and the application workload that this group will run will be identified, which is based on the Login VSI 3.6 medium workload (with flash.) Virtual machines will be used as the desktop sourc.

If you use a vSphere virtual machine as a desktop source, you can automate the process of making as many identical virtual desktops as you need. You can set a minimum and maximum number of virtual desktops to be generated for the pool. Setting these parameters ensures that you always have enough View desktops available for immediate use but not so many that you overuse available resources.

Using pools to manage desktops allows you to apply settings or deploy applications to all virtual desktops in a pool. The following examples show some of the settings available:

- Specify which remote display protocol to use as the default for the View desktop and whether to let end users override the default.
- Configure the display quality and bandwidth throttling of Adobe Flash animations.
- If using a virtual machine, specify whether to power off the virtual machine when it is not in use and whether to delete it altogether.
- If using vSphere 4.1 or later, specify whether to use a Microsoft Sysprep customization specification or QuickPrep from VMware. Sysprep generates a unique SID and GUID for each virtual machine in the pool.
- Specify whether the View desktop can or must be downloaded and run on a local client system.

In addition, using desktop pools provides many conveniences.

- Dedicated-assignment pools: Each user is assigned a particular View desktop and returns to the same virtual desktop at each login. Users can personalize their desktops, install applications, and store data.
- Floating-assignment pools: The virtual desktop is optionally deleted and re-created after each use, offering a highly controlled environment. A floating-assignment desktop is like a computer lab or kiosk environment where each desktop is loaded with the necessary applications and all desktops have access to necessary data.

Using floating-assignment pools also allows you to create a pool of desktops that can be used by shifts of users. For example, a pool of 100 desktops could be used by 300 users if they worked in shifts of 100 users at a time.



Note

For this study, Automated Pools with Floating Assignments in conjunction with View Composer linked clones was used.

Managing Storage Requirements

VMware vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

With View 4.5 and later and vSphere 4.1 and later, you can now also use the following features:

- vStorage thin provisioning, which lets you start out with as little disk space as necessary and grow the disk to add space later
- Tiered storage, which allows you to distribute virtual disks in the View environment across high performance storage and lower-cost storage tiers, to maximize performance and cost savings
- Local storage on the ESX/ESXi host for the virtual machine swap files in the guest operating system.

With Horizon View 5.2 and later and vSphere 5.0 and later, you can now also use the following features:

• With the View storage accelerator feature, you can configure ESXi hosts to cache virtual machine disk data.

Using this content-based read cache (CBRC) can reduce IOPS and improve performance during boot storms, when many desktops start up and run anti-virus scans at the same time. Instead of reading the entire OS from the storage system over and over, a host can read common data blocks from cache.

• You can deploy a desktop pool on a cluster that contains up to 32 ESXi hosts, but you must store the replica disks on NFS datastores.

Although replica disks must be stored on NFS datastores, OS disks and persistent disks can be stored on NFS or VMFS datastores.

View Composer

Because View Composer creates desktop images that share virtual disks with a base image, you can reduce the required storage capacity by 50 to 90 percent.

View Composer uses a base image, or parent virtual machine, and creates a pool of up to 1,000 linked-clone virtual machines. Each linked clone acts like an independent desktop, with a unique host name and IP address, yet the linked clone requires significantly less storage.

When creating a linked-clone desktop pool, a full clone is first made from the parent virtual machine. The full clone, or replica, and the clones linked to it can be placed in a variety of locations. The options are:

- Replica and linked clones on same datastore
- Replica and lined clones on different datastores

As an example, you could place the replicas on low capacity read optimized drives with IOPS and place the linked clones on traditional spinning media

• Disposable Disks for Paging and Temp Files

Guest OS page files and temp files are placed here. When the HVD is powered off, this disk is deleted

• Persistent disks for dedicated desktops

End user's application data and profiles are stored here. The data survives refresh, recompose and rebalance operations.

· Local datastores for floating or stateless desktops

Host local drives store linked clone files, presenting some advantages and several disadvantages. Use this option with care after considering your requirements.



For this study, the technique was to have the replicas and linked clones on different datastores.

Hosted Virtual Desktop Infrastructure Design

To implement the automated pool floating desktop delivery model for this study, the VMware View Reference Architecture for virtual desktop delivery was followed.

Figure 7 View Desktop Infrastructure



Learn more about VMware Horizon View planning and design at the following location:

https://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-architecture-planning.pdf

Solution Validation

I

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

Configuration Topology for Scalable VMware View 5.2 Virtual Desktop Infrastructure on Cisco Unified Computing System and EMC Storage

Figure 8 illustrates the Cisco Unified Computing System VDI configuration.



Figure 8 illustrates the architectural topology for the purpose of this study. The architecture is divided into four distinct layers:

1

- 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

Figure 9 details the physical configuration of the 2000 seat View 5.2 environment.



Figure 9 Detailed Architecture Configuration

Cisco Unified Computing System Configuration

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-M GUI Configuration guide http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/gui/config/guide/2.1/b_UCS M_GUI_Configuration_Guide_2_1.html

Base Cisco Unified Computing 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. When 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&rele ase=2.0(4d)&relind=AVAILABLE&rellifecycle=&reltype=latest to download the most current Cisco UCS Infrastructure and Cisco UCS Manager software. Use the Cisco 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).

wit Summary	A G G I New - D Options ()	0 Arending Activitie	s 💽 Ext		
	3 >> iii Equipment				👬 Equipt
ipment Servers LAN SAN VM Admin	Main Topology View		Fabric Interconner mware Management		Policies Servers
Filter: Al 💌	Installed Firmware Download Tasks Packag	es Images Faults			
Equipment The Will Chassis	Name	Type	State Vend	lor Version	Deleted on Fabric
	⊕ @ ucs-k9-bundle-b-series.2.0.1s.8.bin	8 Series Bundle	Active	2.0(1s)8	*
- FEX	🕀 🗑 ucs-k9-bundle-b-series.2.0.3a.B.bin	8 Series Bundle	Active	2.0(3a)8	100
Servers	😥 🗑 ucs-k9-bundle-b-series.2.0.3c.8.bin	8 Series Bundle	Active	2.0(3c)8	
Fabric Interconnects	🛞 🗑 ucs-k9-bundle-b-series.2.0.4a.B.bin	B Series Bundle	Active	2.0(4a)8	
	🖲 🗑 ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active	2.0(1s)C	
	🕀 😵 ucs-k9-bundle-infra.2.0.1s.A.bin	Infrastructure Bundle	Active	2.0(1s)A	
	@ ucs-k9-bundle-infra.2.0.3a.A.bin	Infrastructure Bundle	Active	2.0(3a)A	
	🕀 🗑 ucs-k9-bundle-infra.2.0.3c.A.bin	Infrastructure Bundle	Active	2.0(3c)A	
	😥 😨 ucs-k9-bundle-infra.2.0.4a.A.bin	Infrastructure Bundle	Active	2.0(4a)A	

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



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.

Nil Summary	🚺 🕘 💷 New - ⊋ Options 😜 📵 🗥 Per	nding Activities 0 Duit	+
0 20 7 49	>> 🙀 Equipment * 🚥 Fabric Interconnects * 🚥 Fabric	interconnect A (primary) * 🚥 Fixed Module * 📲 Ethernet Ports * 📲 Port 1	- Port 1
upment Servers LAN SAN VM Admin	General Faults Events FSM Statistics		
Filter: Al 💌	Fault Summary Phys	sical Display	
8	🛛 🛛 🗸 🖉 🛆 🗖	CONTRACTORS AND ADDRESS OF	
B Tabric Interconnect A (primary)			
S S Fived Module		and an and a second s	
R - Ethernet Ports		ip 🧱 Admin Down 📕 Fail 🔄 Link Down	
- 🛛 Pore 1 🚽	Overal Status: 1 Up		
Port 2	PRODUCTS PTC.	perties	
Port 3	Admin State: Enabled	ID: 1 Sot ID: 1	
Port 4		r Label:	
	Actions	MAC: 54:7FEE45:2A:48	
Port 5	- Enable Port	Mode: Fabric	
Port 8	Por	t Type: Physical Role: Server	
Port 9	Cisable Port		
Port 10	- Reconfigure	ansceiver	
Port 11		Type: HIOGB CUSM	
Port 12	- Unconfigure	Model: 74752-9520	
	- Show Interface	endor: CISCO-MOLEX	
Port 14		Serial: MOC154205G0	
Port 16			
Port 10		nse Details	
Port 10	Uce		
		License State: License Ok	
	Lice	nse Grace Period: 0	
Port 21			

5. Configure and enable uplink Ethernet ports.

Fault Summ	ary 🔻	^		0	O D New -	🖌 Options 🛛 🔞	A Pending Activitie	s 👩 Dat			1
0	20	7	49	>>	Equipment * 🚥	Fabric Interconnects	• 💷 Fabric Interconnect A	A (primary) * 📖 Fixed	Module * Ethernet Ports	1	-C Ethernet Por
Equipment	ervers LAN SAN	VM Admin		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	hernet Ports			Martine Course Sectors 1994			
	Filter: Al			4		Print If Role:			PCoE Uplink 🖓 Unified Up		FCoE Storage
+ E					Slot	Port ID	MAC	1º Role	If Type	Overal Status	Administrative 🛱
				1		1	54:7F:EE:45:2A:48	Server	Physical	t Up	1 Enabled
	oric Interconnects	A destruction of a		1		2	54:7F:EE:45:2A:49	Server	Physical	1 Up	1 Enabled
	Fabric Interconnect	A (primary)		1		3	54:7F:EE:45:2A:4A	Server	Physical	1 Up	t Enabled
	B- Chernet Por			1		4	54:7FIEE:45:2A:4B	Server	Physical	t Up	1 Enabled
	- Port 1	1.1		1		5	54:7F:EE:45:2A:4C	Server	Physical	1 Up	t Enabled
	Port 2			1		6	54:7F:EE:45:2A:4D	Server	Physical	t Up	t Enabled
	Port 3			1		7	54:7F:EE:45:2A:4E	Server	Physical	1 Up	t Enabled
	- Port 4			1		8	54:7F:EE:45:2A:4F	Server	Physical	1 Up	t Enabled
	Port 5			1		9	54:7F:EE:45:2A:50	Server	Physical	1 Up	t Enabled
	Port 6			1		10	54:7F:EE:45:2A:51	Server	Physical	1 Up	1 Enabled
	Port 7			1		11	54:7F:EE:45:2A:52	Server	Physical	t Up	1 Enabled
	Port 8			1		12	54:7F:EE:45:2A:53	Server	Physical	1 10	1 Enabled
	Port 9			1		13	54:7F:EE:45:2A:54	Unconfigured	Physical	V Stp Not Present	Disabled
	Port 11			1		14	54:7F:EE:45:2A:55	Unconfigured	Physical	V Stp Not Present	Disabled
	Port 12					15	54:7F:EE:45:2A:56	Monitor	Physical	V Slp Not Present	1 Enabled
	Port 13			1		16	54:7F-EE:45:2A/57	Unconfigured	Physical	V Slp Not Present	Disabled
	Port 14					17	54-7F-EE-45-2A-58	Network	Physical	🛧 Lb	Enabled
	Port 15					10	54:7F-IE-45-2A-59	Network	Physical	1 Up	Trubled
	Port 16	-				19	54:7F (E) 45:2A:5A	Network	Physical	1 Llo	Enabled
	Port 17	-				20	54:7F.EE:45:2A:58	Network	Physical	1 10	Enabled
						21	54:7F:EE:45:2A:5C	Uncertinged	Physical	V Stp Not Present	Disabled
						22	54:7F:EE:45:2A:5D	Unconfigured	Physical	Sto Not Present	Disabled
	- Port 20			1		166	041/P31214512A/50	Unconngured	PTOSCA	V Srp not Present	 Everabled

6. Configure and enable FC uplink ports.



Use the Configure Unified Ports, Configure Expansion Module Ports to configure FC uplinks.



ſ

In this example, six FC ports are configured, two of which are in use.

7. From the LAN tab in the Navigator pane, configure the required Port Channels and Uplink Interfaces on both Fabric Interconnects.

Fault Summary	Δ	▲	🥥 🏐 🖪 New - ⊋ 😒	tions 🛛 😧 🌒 💧 🖾 Pending Activities	0 Dat
2 0	8	3	>> = LAN • CLAN Cloud •	E Fabric A	
Equipment Servers LAN SAN 1	M Admin		General VLANs Upink Interfa	ces Port Channels Events	
Filters M	Ince 225 (one 226 (one 227 (one 228 229 2110 7 (Fabric 8) (one 225 (one 226 (one 227 (one 229) 229		Actions Consta VLAbi Consta	laces 6	

8. Expand the Chassis node in the left pane; click each chassis in the left pane, then click Acknowledge Chassis in the right pane to bring the chassis online and enable blade discovery.



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.



- 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, a MAC address pool was created of sufficient size for the environment. In this project, a single pool with two address ranges for expandability was created.



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

I



13. For this project, a single VSAN was used, with the default VSAN with ID 1.



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



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

ault Summary	•		
	⊿	G Options 🕜	Pending Ac
1 21 9	57	>> 🥪 Servers 👌 🛞 Pools 👌 🗛 root 👌 🥪 S	ierver Pools
upment Servers LAN SAN VM Admin		Server Pools	
Filter: All		🛨 😑 🕰 Filter 👄 Export 🍪 Print	
	_	Name	
		🕑 🥪 Server Pool InfrastructurePool	12
🖃 🚿 Policies		E Server Pool VDI-Workloads	15
🖻 🙀 root		Server Pool default	0
Adapter Policies			
BIOS Defaults			
BIOS Policies			
Boot Policies			
Host Firmware Packages			
IPMI Access Profiles			
E-S Local Disk Config Policies			
Maintenance Policies			
Serial over LAN Policies			
Server Pool Policies			
Server Pool Policy Infra-Pool-Pol			
Server Pool Policy VDI-Pool-Pol			
Server Pool Policy Qualifications			
Sinfra-Qual			
WDI-Wrkld-Qual			
H-ST Threshold Policies			
- Si ISCSI Authentication Profiles			
- S vNIC/vHBA Placement Policies			
Sub-Organizations			
🖻 💮 Pools			
E & root			
E Server Pools			
 Server Pool InfrastructurePool 			
Server Pool VDI-Workloads			
Server Pool default			

ſ

16. Create two Server Pool Policy Qualifications to identify the blade server model for placement into the correct pool using the Service Profile Template. In this case we used Chassis ids to select the servers. (You can use slots or server models to make the selection.)



 The next step in automating the server selection process is to create corresponding Server Pool Policies for each Cisco UCS Blade Server model, utilizing the Server Pool and Server Pool Policy Qualifications created earlier.



18. Virtual Host Bus Adapter templates were created for FC SAN connectivity from the SAN tab under the Polices node, one template for each fabric.

Fault Summary		10
	 Q gations 	
	Policies * 🙏 root * 📷 vHEA Templates * 📷 vHEA Template VDA-HEA-A 🔤 vHEA T	emplate VDA-HBA
Equipment Servers LAN SAN VM Admin General v	terfaces Faults Events	
Filter: Al Action	Properties	
t c from	Name: YDA-HBA-A	
0 	Description: VCA Host Bus Adapter for Fabric A	
SAN Coud	Fabric ID: 🗭 A C 8	
🛞 🚥 Fabric B	VSAN: Of s.R.	
SAN Pin Groups	Target: Adapter	
	Template Type: C Initial Template 🧭 Updating Template	
 Storage Coud En Fabric A 	Max Data Field Size: 2048	
 ■ Fabric 8 ■ VSANs 	Policies	
© S Pokoes	WWN Pool: VDA-WWR14-Pool *	
SAN Coud Serveshold Policies	Qe5 Policy: PC	
S A root	Pin Group: <not set=""></not>	
S Fbre Channel Adapter Policies S Threshold Policies	Stats Threshold Policy: default	
HEA Template VCA-HEA-A		
TEW TENERAL YOUNG A		

- **19.** Create at least one HBA template for each Fabric Interconnect if block storage will be used. We used the WWPN pool created earlier and the QoS Policy.
- 20. From the LAN tab in the navigator pane, configure the VLANs for the environment.



Note	

I

- In this project we utilized six VLANs to accommodate our four ethernet system classes, a separate VLAN for infrastructure services, and two VLANs for Nexus 1000V packet and control functions. (N1KV management and VMware Management shared VLAN 164.) We did not use VLAN 166 in the FC variant we deployed in this study. However, if the NFS or iSCSI protocols were used, that VLAN is in place.
- **21.** From 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 eight virtual NICs per host, four pairs, with each pair connected to both Fabric Interconnects for resiliency.

2 0 8 3				
	>> 📰 LAN * 🚿 Pokcies * 🛕 root * 📷 vAIC Ter	iglates	Mac viac	C Template
upment Servers LAN SAN VM Admin	while Templates			
Filter: Al 👻	🚓 👝 🕰 Filter 👄 Export 🎲 Print			
	Name	VLAN	Native VLAN	10
8	S-M vNC Template Management-A			(D)
= LAN	Network ML-OC-VM-MQMT	ML-DC-VM-MQMT	c	
C LAN Cloud	- Network ML-NIKY_CTR	ML-NIKY_CTR	c	
8 🚥 Fabric A	- Network VLAN0901	VLAN0901	C	
R Car Fabric B	R- Template Management-8			
Qos System Class	Network ML-OC-VM-MQMT	ML-DC-VM-MQMT	c	
R-S Threshold Policies	Network ML-NIKY_CTR	ML-NIKY_CTR	c	
8 I VLANS	Network VLAN2901	VLAN0901	C	
Applances	IS-FEE vNDC Template NFS-A			
Internal LAN	Network ML-OC-STRG	ML-DC-STRG	c	
S Pokces	White Template NFS-8			
B Applances	Network ML-DC-STRG	ML-DC-STRG	c	
Gud LAN Cloud H Threshold Policies	IR - BE VADC Template VDA-A			
In- 30 Threshold Policies In- 0, root	- Network ML-OC-3MF	ML-DC-DVF	C	
- S Dunamic vADC Connection Policies	- Network ML-VDA	ML-VDA	C	
8-95 Plow Cantrol Policies	R-BE vN0C Template VDA-8			
9 5 Network Control Policies	Network ML-OC-DVF	MLOC OF	c	
B - S QoS Policies	- Network ML-VDA	ML-VDA	c	
8 1 Threshold Policies	Mole Template VMotion-A			
🕀 🜃 MDC Templates 🔫 🚃	Network ML-DC-VMMOTSON	ML-DC-VMMOTION	c	
11 vNIC Template Management-A	White Template VMotion-8			
VNUC Template Management-8 VNUC Template NFS-A	Network ML-DC-VMMOTION	ML-DC-VMMOTION	C	
- VNDC Template NFS-8	-			
- Tit vNIC Template VDA-A				
- Mill VAC Template VCA-8				
- And vh0C Template VMotion-A				

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



- **23.** Create a boot from SAN policy to use for both Cisco UCS B250 M2 and Cisco UCS B200 M3 blades, using the WWNs from the VNX5500 storage system as SAN targets.
- **24.** Create performance BIOS Policies for each blade type to insure optimal performance. The following screen captures show the settings for the Cisco UCS B200 M3 blades used in this study.

Fault Summary	🚱 🔘 🕮 New - 😥 gations 🛛 🕢 🙆 Pending Activities 🔄 🔯 Dat	¢
1 21 9 57	>> 🥪 Servers * 📓 Policies * 🔬 root * 📓 BIOS Policies * 📓 B200M3_PERF	S 8200M3_PERI
Equipment Servers LAN SAN VM Admin	Main Advanced Boot Options Server Management Events	
Filter: Al 💌	Actions Properties	
	Delete Name: E2004D_JFRF Show Policy Unique Rebot on BD05 Setting: Charge: S Policy Environment Caset Boot: State in analised in Platform Delnuit Policy Environment dashed if enabled if enabled if Platform Delnuit Resume A: On Power Loss: Instant of the instate if instate Platform Delnuit Proce Prever Loss: Instant of the enabled if enabled if Platform Delnuit Platform Delnuit	efa.k

The Advanced Tab Settings:

Elsco Unified Computing System Manager - UCS-G2-POD Fault Summary				
	3 💿 🗉 New - 😡 Qol	ions 🛛 😧 🚺 🖾 Pending Act	tivities 0 Exit	cere
1 21 9 57		🔥 root * 🚿 8005 Policies * 🚿 8		S B200M3_PERF
Equipment Servers LAN SAN VM Admin	Main Advanced Boot Options	Server Management Events		
Filter: Al 👻	Processor Intel Directed IO F	RAS Memory Serial Port USB PCI	Configuration	
± =	Turbo Boost:	C disabled C enabled C Platfo	orm Default	
Policies	Enhanced Intel Speedstep:	C disabled C enabled C Platfo	orm Default	
Good Defaults	Hyper Threading:	C disabled C enabled C Platfo	orm Default	
E - 5 8005 Policies	Core Multi Processing:	al 💌		
	Execute Disabled Bit:	C disabled C enabled @ Platfo	orm Default	
	Virtualization Technology (VT):	C disabled C enabled C Platfo	orm Default	
SRIOV	Direct Cache Access:	C disabled C enabled C Platfo	orm Default	
Soct Policies Soct Policies Soct Policies Soct Policies	Processor C State:	G disabled C enabled C Platfo	orm Default	
- DIMI Access Profiles Si Local Disk Config Policies	Processor C1E:	G disabled C enabled C Platfo	orm Default	
	Processor C3 Report:	G disabled C acpi-c2 C acpi-c	3 C Platform Default	
Srub Policies Srub Policies	Processor C6 Report:	C disabled C enabled C Platfo	orm Default	
- Serial over LAN Policies	Processor C7 Report:	C disabled C enabled C Platfo	orm Default	
Server Pool Policy Infra-Pool-Pol	CPU Performance:	C enterprise C high-throughput	t 📀 hpc 🔿 Platform Default	
Server Pool Policy Qualifications Server Pool Policy Qualifications Server Pool Policy Qualifications Server Pool Policy Qualifications	Max Variable MTRR Setting:	C auto-max C 8 @ Platform D	elak	

The remaining Advanced tab settings are at the platform default or not configured. Similarly, the Boot Options and Server Management tabs' settings are set at the defaults.

Note

Be sure to Save Changes at the bottom of the page to preserve this setting. Also, be sure to add this policy to your blade service profile template.

25. New in Cisco UCS Manager 2.1(1a) is a way Host Firmware Package polices can be set by package version across the Cisco UCS domain rather than by server model .



I

You can still create specific packages for different models or for specific purposes.



sult Summary	10.0							
	🕼 🔘 🗆 Nev	v * 😧 Qptions 🛛 🔞	• • A Pending	Activities 0 Ext				
		S Policies * 🙏 root *	S Host Firmware Pa	schages 🕴 🛒 2.1.1a			W	2.1
upment Servers LAN SAN VM Admin	General Events							
Filter: Al	Actions		Properties					
	T Delete		Name: 2.1.	.1a				
S Policies	Show Pol	ky Licane	Description:				_	
B-00 root	A use debut		Owner: Loc	al				
	and the second se		Blade Package:					
 BIOS Defaults 	Modify Pr	ackage Versions	Rack Package:					
	and the second							
- 55 8200M2-Per/BIOS - 55 8200M3 - 55 8200M3_PERF - 55 8230M2-Per/BIOS - 55 8250M2-Per/BIOS	🕰 Filter 👄 Expo				Controller			
- 55 820042-Per/BIOS - 55 820045 - 55 820045 / PEP/ - 55 823042-Per/BIOS - 55 825042-Per/BIOS - 55 825042-Per/BIOS - 55 825042-Per/BIOS	Filter Select	rt 😸 Print Vendor	Model	PID	Presence	Version	0	
- SE ECONCY-Perf8105 - SE ECON43_PERF - SE ECON43_PERF - SE ECON43_PERF - SE ECON43_PERF - SE ECON43_PERF - SE SECON 0: SE ECON Paloises	🕰 Filter 👄 Expo	et 😸 Print Vendor Cisco Systems Inc	Model Cisco UCS 8230 M2	PID 8230-BASE-M2	Presence N/A	<not set=""></not>	10	
- SE BOOMS Perfitions - SE BOOMS - SE BOOMS - SE BOOMS - SE BOOMS - SE BOOMS - PERFIT - SE BOOMS - PERFIT - SE BOOMS - PERFIT - SE SERVE AnnuBerf - SE SERVE AnnuBerf - SE BOOK PRAGES - SE MOKE Finnisse Padages	Filter Select	ver G Prink Vendor Cisco Systems Inc Cisco Systems Inc	Model Cisco UCS 8230 M2 Cisco UCS 8440 M2	PID 6230-8A5E-M2 8440-8A5E-M2	Presence N/A N/A	<not set=""> <not set=""></not></not>		
	Filter Select	et Cosco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Osco UCS 8230 M2 Osco UCS 8440 M2 Osco UCS 8440 M1	PID 8230-845E-M2 8440-845E-M2 N20-86620-1	N/A N/A N/A	<not set=""> <not set=""> <not set=""></not></not></not>	00 	
- 5 20045-9-481005 - 5 20045 - 5 20045 - 5 20045,964 - 5 20045,964 - 5 20045,964 - 5 5 20045 - 5 5 1005 - 5 5 1005 - 5 5 1005 - 5 5 20.36 - 5 20.36 - 5 20.48	Filter Select	et Coo Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Cisco UCS 8230 M2 Cisco UCS 8440 M2 Cisco UCS 8440 M2 Cisco UCS 8200 M1 Cisco UCS 8250 M1	PID 8230-8432-442 8440-8432-442 N20-86620-1 N20-86620-2	N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not>	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
	Select	et Coo Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Cisco UCS 8230 M2 Cisco UCS 8240 M2 Cisco UCS 8200 M1 Cisco UCS 8250 M1 Cisco UCS 8250 M2	PID 8230-845E-M2 8440-845E-M2 N20-86620-1 N20-86620-2 N20-86620-2 N20-86625-1	Presence N/A N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not>		
- 55 20042-9-481005 - 55 20043 - 55 20043 - 55 20043 - 55 20043-968 - 55 20043-968 - 55 2004 - 55 2.0.36 - 55 2.0.14 - 55 2.0.	Filter Select	et Coo Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Gaco UCS 8230 M2 Gaco UCS 8440 M2 Gaco UCS 82400 M1 Gaco UCS 8250 M1 Gaco UCS 8250 M2 Gaco UCS 8250 M2 Cinco UCS 8250 M2	PID 8230-845E-M2 8440-845E-M2 N20-86620-1 N20-86620-2 N20-86620-2 N20-86625-1	Presence N/A N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not>	• •	
- 55 800x6-9-efficios - 55 800x6-9-efficios - 55 800x6-9-efficios - 55 800x6-9-efficios - 55 800x6-9-efficios - 55 800x7-9-efficios - 55 800x7-9-efficios - 55 2.0.35 - 55 2.0.45 - 55 2.0.45	Select	et Coo Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Cisco UCS 8230 M2 Cisco UCS 8240 M2 Cisco UCS 8200 M1 Cisco UCS 8250 M1 Cisco UCS 8250 M2	PID 8230-845E-M2 8440-845E-M2 N20-86620-1 N20-86620-2 N20-86620-2 N20-86625-1	Presence N/A N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not>	••••	
- Si BOOKS-PHILOS - Si BOOKS-PER - Si BOOKS-PER - Si BOOKS-PER - Si BOOKS-PER - Si BOOKS-PHILOS - Si BOOK PHILOS - Si BOOKS-PHILOS - SI BOOKS-	Select	et Cisco Systems Inc Cisco Systems Inc Cisco Systems Inc Cisco Systems Inc Cisco Systems Inc Cisco Systems Inc Cisco Systems Inc	Model Gaco UCS 8230 M2 Gaco UCS 8440 M2 Gaco UCS 82400 M1 Gaco UCS 8250 M1 Gaco UCS 8250 M2 Gaco UCS 8250 M2 Cinco UCS 8250 M2	PID 8230-8A5E-M2 8440-8A5E-M2 N20-86620-1 N20-86620-1 N20-86620-2 N20-86625-1 2 N20-86625-2	Presence N/A N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> 2.1(1a)</not></not></not></not></not></not>	•••	
	Select	et Sprink Vendor Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Osco UCS 8230 M2 Osco UCS 8230 M2 Osco UCS 8200 M1 Osco UCS 8200 M1 Osco UCS 8200 M2 Cisco UCS 8230 M Osco UCS 8230 M1	PID 8230-8458-M2 8440-8458-M2 N20-86620-1 N20-86620-2 N20-86625-1 2N20-86625-2 N20-86625-2 N20-86730-1 N20-86730-1	Presence N/A N/A N/A N/A N/A N/A N/A N/A	<not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> 2.1(1a) <not set=""></not></not></not></not></not></not></not>		
- 55 80045-9-441605 - 55 80049 - 55 80049 (FF) - 55 80049 (FF) - 55 80049 (FF) - 55 8004 - 55 8004 - 55 800 - 55 800	Fiter Cope	et Sprink Vendor Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc Osco Systems Inc	Model Osco UCS 8230 M2 Osco UCS 8230 M2 Osco UCS 8230 M1 Osco UCS 8240 M1	PID 8230-8458-M2 8440-8458-M2 N20-86620-1 N20-86620-2 N20-86625-1 2N20-86625-2 N20-86625-2 N20-86730-1 N20-86730-1	Presence N/A N/A N/A N/A N/A N/A N/A N/A	<pre><not set=""> <not set=""> </not> <td>•</td><td></td></pre>	•	



The process was continued across the remaining tabs choosing the appropriate model and versions.

- **26.** Management Firmware Packages are no longer supported. Host Firmware packages replaced this functionality in Cisco UCS Manager 2.1.
- 27. Create a service profile template using the pools, templates, and policies configured above.





In this project, we created two templates, one for each of the Cisco UCS Blade Server models used.

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



On the Operational Policies screen, select the appropriate performance BIOS policy you created earlier to help ensure the maximum LV DIMM performance.



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

28. From the Create Service Profile Template wizard, enter a unique name, select the type as updating, and select the VDA-UUID-Suffix_Pool created earlier, then click Next.

Unified Computing System Manager to serve hole register • Vestige to the serve • Vestige to the serve profile Template • Vestige to the serve profile template and specify the template type. You can also specify how a UUD will be server to the serve to the serve of the serve of the serve of the serve of the template to the serve of the s	Service Broffe Template	Service André Template Subscription Subscriptin Subscriptin Subscription Subscription Subscripti	eate Service Profile Templat	
Videntify Service Vou must enter a name for the service profile tamplate and specify the template type. You can also specify how a UUD will be assigned to this template and enter a description. Vou must enter a name for the service profile tamplate and specify the template type. You can also specify how a UUD will be assigned to this template and enter a description. Vou must be unque within the organization. Where: organol Vou must be unque within the organization. Vou be undue to the server associated with the service generated by the template. Vou be undue to the server associated with the service generated by the template. Vou be undue to the server associated with the ser	Volumental ends of the service profile template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to this template and specify the template type. You can also specify how a UUD will be assigned to the template and specify the template type. You can also specify how a UUD will be assigned to the template and specify the template type. You can also specify how a UUD will be assigned to the template and specify the template type. You can also specify how a UUD will be assigned to the template and specify the template type. You can also specify how a UUD will be assigned to the template and specify the template type. You can also specify how a UUD will be assigned to the server associated with the organization.	Volumental of the complete constraints will be created in the following organization. Its name must be unique within the organization. Volument Assonment Constitutional Pholes Constit	Unified (Computing System Manager
Construction of the service of the service of the service generated by this template. Construction of Policies Construc	Construction of the construction of the second problem of the	Construction of the construction of the second problem of the	Service Profile Template I	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: property Jourd Sav Template and be created in the following organization. Its name must be unque within this organization.
	The available/total UUEDs are displayed after the pool name.	The available/total UUEs are displayed after the pool name.	6. Contemport Condex 7. Maintenance Policy 8. Server Assignment	The template will be created in the following organization. Its name must be unique within this organization. Type:: Initial Template © Updating Template Specify Nom the ULID will be assigned to the server associated with the service generated by this template. UUID Template: Specify Nom the ULID will be assigned to the server associated with the service generated by this template. UUID Specify Nom the ULID will be associated with the service generated by this template.

29. From the Storage page, select the Expert mode and select the WWNN Pool created earlier from the drop-down list and then click Add.

omputing System Manager
Storage Optionally specify disk policies and SAN configuration information.
Select a local dak 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 sentice profile. Create Local Disk Configuration Policy
How would you like to configure SAX connectivity
Name W45%
Diviter 🖬 Add 📷 Modify



I

We used the default Local Storage configuration in this project. Local drives on the blades were not used.

30. From the Create HBA page, enter a name (FCO) and check Use SAN Connectivity Template, which will change the display as follows.



- **31.** Select the vHBA template for Fabric Interconnect A and the VMware Adapter Policy from the drop-downs, then click OK.
- **32.** Repeat this process for FC1, choosing VDA-HBA-B for Fabric Interconnect B. The result is shown in the Storage page that appears as follows:

I

1

33. Click Next.

a Service Profile Template 1. √ <u>Identify Service Profile</u>	Storage Optionally specify disk policies and SAN configuration	n information.		
Innolate 2. 4 Storage, 3. Networking 4. UvdC/vrBit Placement, 5. Server Boot Order, 6. Utdirtenance Policy, 7. Server Assignment, 8. Operational Policies		othing is selected, the default Local St icy will be assigned to this service profile		
	How would you like to configure	e SAN connectivity? 🔿 Simple 📀	Expert 🔿 No vHBAs	
	profile.			
	World Wide Node Name Widtly Assignment: Y2M-WMMM Pro(1377200) The WMMM will be assigned from the selected pool. The available/botal WMMM are displayed after the pool name.			
	World Wide Node Name WWNRV Assignment: VDA-WWNRV Pool(137/200) The WWNRV will be assigned from the selected pool.		www	
	World Wide Node Name WMNR Assgment: VCA-WMNR4Pool(137/200)	Derived	www.see	
	World Wide Node Name WinR4 Assignment: VCA-WinR4-Pool(137/200) The WinR4 Assignment: VCA-WinR4-Pool(137/200) The winR44 Assignment: VCA-WinR44 are displayed after the pool name. Name		WWPN	
	World Wide Node Name WWHR Assignment: VCA-WWHR Pool(137/200) The WWHR Assignment: VCA-WWHR Pool(137/200) The walable/total WWHR are displayed after the pool name. Name Name Name Name Name Name Name Nam	Derived	WWFN	
	World Wide Node Name WMNR Assignment: VCA-WMNR4Pool(137/200) The WMNR4-ell be assigned from the selected pool. The analabilitytical WMNRs are displayed after the pool name. Name Name Name Name Name Name Name Nam	Derived	WWW	
	World Wide Node Name WWNRV Assignment: VCA-WWNRV-Pool(137/200) The WWNRV-assignment: VCA-WWNRV-Pool(137/200) The washabe/total WWNRV are dissigned after the pool name. Name Name Image: State of the selected pool. Name	Derived	WWRW	

- 34. Click Next.
- **35.** Select the Expert configuration option and click Add.

Template		onfiguration information.			
2. √ <u>Storage</u> 3. √ <u>Networking</u> 4. □ <u>vhIC/vHBA Placement</u> 5. □ <u>Server Boot Order</u>	Dynamic vNBC Connection Policy:	Select a Policy to use (no Dynamic vNI	IC Policy by defa 💌 🎇 Create	Dynamic vHIC Connection Policy	
Gerver Assignment Gerver Assignment Gervational Policies		would you like to configure LAN	connectivity? 🗇 Simple 🕞 Expert nect to the LAN.	C No vHICs	
	Name	MAC Address	Fabric ID	Native VLAN	1
					-
			1		
			V		-

36. From the Create vNIC window, enter a unique Name, check the Use LAN Connectivity Template checkbox, select the vNIC Template from the drop-down, and repeat this process for the Adapter Policy.



ſ

37. Repeat the process for the remaining seven vNICs, which will result in the following: (Eth5, 6, and 7 not shown).

Optionally specify LAN	configuration information.				
<u>writ</u>	Select a Policy to use (no Dyna	anic vNIC Policy by defa	Create D	ynamic vNBC Connection Policy	
Click Add to specify one or more	ow would you like to configur		Smple 🤆 Expert (No vNBCs	
Name	MAC Add	tress	Fabric ID	Native VLAN	(11)
-G vNIC Eth0	Derived	derived			
	Derived	derived			
	Derived	derived			
	Derived	derived			_
-S vNIC Rh4	Derived	derived			-
		Delete 🛄 Add 🎼 M	odify		_
ISCST VNICS					0
		_			~

1

- **38.** Click Next.
- **39**. Accept the default placement and click Next.

ce Profile Template Identify Service Profile	vNIC/vHBA Placem Specify how vNICs and vf		cal network adapters		0
mplate	ABC/H4BA Placement: specifies how v n a server hardware configuration ind Select Placement: Let System Per System will perform automatic pl	form Placem 💌 🔲 Cre	ate Placement Policy	ezzanime)	
	Name	Address	Order	-	
		Derived	1	-	
		Derived	2	_	
	-1 vNIC Etho	Derived	3		
	- 1 vNIC Eth1	Derived	4		
	- VNIC Eth2	Derived	5		
		Derived	6		
		Derived	7		
		Derived	8		
		Derived	9		
		Derived	10		
				2	
	🛦 Move Up 🔹	r Move Down 👚 Delete	🕅 Reorder 🛛 👪 Modify		

40. Select the Boot from SAN policy created in Section 5.4.5 from the drop-down.

iervice Profile Template ↓ √ Identify Service Profile	Server Boot Order Optionally specify the boot polis	cy for this s	ervice profile template.				
Instant Jerner Prove Instant Jerner Prove Versonen Versonen Versonen Versonen Server Bost Order Server Assistment Operational Policies	Select a boot policy. Boot Policy: Boot Prom-SAN Name: Boot -P Reboot on Boot Order Charge: no Epfroro.vMC(2)r4RA/SCS Name: yes WARNING:	from-SAN 00 BFS Polic;					
	The type (primary/secondary) does not it The effective order of boot devices within if Enforce vHIC/VHIBA/ISCSI Name is if it is not selected, the VHICs/VHBAs/ISC Boot Order	n the same de s selected and ISI are selecte	vice class (LAN/Storage/ISCS the vNIC/vHBA/ISCSI does	not exist, a cor	ning error will b	be reported.	used.
	The effective order of boot devices with If Enforce while/vHBA/ISCSI Name is If it is not selected, the vHICs/vHBA/ISC Boot Order (b) (c) (d) Fitter (c) Export (c) Print	n the same de s selected and ISI are selecte	vice class (LAN/Storage/IGC) the vNIC/VHBA/IGCSI does d if they exist, otherwise th	not exist, a cor e vNIIC/VHBA/C	nfig error will t SCSI with the	be reported. lowest PCIe bus scan order is	
	The effective order of boot devices with if forfance which with a second of the second if it is not selected, the vitil cs/vHBAs(SC Eccol Order	n the same de s selected and ISI are selecte	vice class (LAN/Storage/ISCS the vNIC/vHBA/ISCSI does	not exist, a cor	ning error will b	be reported.	used.
	The effective order of boot devices within If Inforce wVIE/vVIEI/ASSIST Name is If it is not selected, the vVIECs/vVIEAs/ISC Boot Conder	n the same de s selected and ISI are selecte	vice class (LAN/Storage/IGC) the vNIC/VHBA/IGCSI does d if they exist, otherwise th	not exist, a cor e vNIIC/VHBA/C	nfig error will t SCSI with the	be reported. lowest PCIe bus scan order is	9
	The effective order of boot devices with all for forder or which (with IN/SST SI mane is in a selected, the with Cs/HERA/SC Boot Order	n the same de s selected and ISI are selecte	vice class (LAN/Storage/IGC) the vNIC/VHBA/IGCSI does d if they exist, otherwise th	not exist, a cor e vNIIC/VHBA/C	nfig error will t SCSI with the	be reported. lowest PCIe bus scan order is	9
	The effective order of boot devices with a Effective VertRA/ISCS Name is If it is not selected, the VBICs/VERAdSC Doct Crider ↓ □ d, Ren → Export @ Prot Name Prot CP RCH ≥ Strappe ≥ Strappe ≥ Stay primary	n the same de s selected and ISI are selecte	vice class (LAN2RorappIOC) the vNIC/VHBA/ISCSI closs i d if they exist, otherwise th vNIC/VHBA/ISCSI vNIC	not exist, a cor e vNDC/VHBA(t Type	nfig error will t SCSI with the	be reported. lowest PCIe bus scan order is	9
	The effective order of boot devices with If enforce which yether (ASSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (ArtHild) (SSI have is If a not selected, the vhill (SSI have	n the same de s selected and ISI are selecte	vice class (LAN2RorappIOC) the vNIC/VHBA/ISCSI closs i d if they exist, otherwise th vNIC/VHBA/ISCSI vNIC	not exist, a cor e vNDC/VHBA/t Type Primary	fig error will 1 SCSI with the	be reported. kwest PCIe bus scan order is WWM	9
	The effective order of boot devices wells If Enforce VHLC /VHLB //KSL Name is If it is not selected, the VHICs/VHBAGSC DOC Order	n the same de s selected and ISI are selecte	vice diss (LAN)Storagy/ICC the villc/HeBA(ISCS) does not d if they exist, otherwise th villc/wBA(ISCS) villc FCD	not exist, a cor e vNIIC(VHBA/C Type Primary Primary Secondary	ofig error will the SCSI with the Lun ID	e reported. lowest PCIe bus scan order is WWM 50:06:01:60:46:E0:5E:0A	9
	The effective coder of boot devices wells If Enforce which yetles, Vieta, Vie	n the same de s selected and ISI are selecte	vice class (LAN2RorappIOC) the vNIC(VHBA/ISCSI closs i d if they exist, otherwise th vNIC(VHBA/ISCSI vNIC	not exist, a cor e vNIC[/vHBA](t Type Primary Primary Secondary Secondary	ofig error will i SCSI with the Lun ID	50:06:01:60:46:20:5E:0A 50:06:01:60:46:20:5E:0A	9
	The effective coder of boot devices with a If Enforce WHL (VHBL/IGSL Name is If it is not selected, the vHBC()/vHBL/IGS	n the same de s selected and ISI are selecte	vice diss (LAN)Storagy/ICC the villc/HeBA(ISCS) does not d if they exist, otherwise th villc/wBA(ISCS) villc FCD	not exist, a cor e vNIC(VHBA)C Type Primary Primary Secondary Primary Primary	ofig error will i SCSI with the Lun ID 0 0	e reported. Iowest PCIe bus scan order is WWW 50:06:01:60:46:E0:5E:0A 50:06:01:69:46:E0:5E:0A 50:06:01:61:46:E0:5E:0A	9
	The effective coder of boot devices wells If Enforce WHL (VHBL/(KSL) Name is If a not selected, the vBlC()+HBL/(SC RotC()+HBL/(SC)) Ro	n the same de selected and SI are selected t Crder 1 2	vice diss (LAN)Storagy/ICC the villc/HeBA(ISCS) does not d if they exist, otherwise th villc/wBA(ISCS) villc FCD	not exist, a cor e vNIC[/vHBA](t Type Primary Primary Secondary Secondary	ofig error will i SCSI with the Lun ID	50:06:01:60:46:20:5E:0A 50:06:01:60:46:20:5E:0A	9
	The effective coder of boot devices wells If Enforce VMEL/VELX/SEX Name is If it is not selected, the vMEC(sh+Biblig)C to Circler Concord Concord Concord Concord	n the same de s selected and ISI are selecte	vice diss (JAN)Storagy(ICS) dist the vice/vielAp(ICS) does in d if they exist, otherwise the vielC/wHBA(ISCS) vielC PC0 PC1	Primary Primary Secondary Secondary	ofig error will i SCSI with the Lun ID 0 0	e reported. Iowest PCIe bus scan order is WWW 50:06:01:60:46:E0:5E:0A 50:06:01:69:46:E0:5E:0A 50:06:01:61:46:E0:5E:0A	9
	The effective coder of boot devices wells 2 Enforce which yells //KSK1 haves is 2 Enforce which yells //KSK1 haves is 2 Enforce which yells //KSK1 haves is 2 Enforce which yells // KSK1 haves is 2 Statistical	n the same de selected and SI are selected t Crder 1 2	ince clais (LANPOR expected) which (HANPOR expected) d if they exist, otherwise the watch-HEAJOCSE watc FC0 FC1 Eb0	not exist, a cor e vNIC(VHBA)C Type Primary Primary Secondary Primary Primary	ofig error will i SCSI with the Lun ID 0 0	e reported. Iowest PCIe bus scan order is WWW 50:06:01:60:46:E0:5E:0A 50:06:01:69:46:E0:5E:0A 50:06:01:61:46:E0:5E:0A	9

41. A Maintenance Policy for the project was not created, so click Next.



ſ

42. Make the following selections from the drop-downs as shown below, then click Next.



43. From the Operational Policies page, expand the BIOS Configuration section and select the BIOS Policy for the Cisco B200 M3 created earlier, then click Finish to complete the Service Profile Template.

1

vice Profile Template	Operational Policies Optionally specify information that affects how the system operates.		(
V Identify Service Profile Template V Storage Vetworking Vetworking Vetwork Pool Orden Vetwork Pool Orden Vetwork Pool Orden Vetwork Assignment	BIDS Configuration If you want to overside the default BIDS settings, select a BIDS policy that will be associated with the BIDS Policy: BIDS	© s service profile	
Operational Policies	External IPMI Management Configuration	0	
	Management IP Address Monitoring Configuration (Thresholds)	0	
	Power Control Policy Configuration	0	
			1
			2

<u>Note</u>

The result is a Service Profile Template for the Cisco UCS Blade Server B200 M3. We repeated the procedure to create a Service Profile Template for the Cisco UCS Blade Server B200 M3 used in the study.



44. Use the newly created Service Profile Templates for each Cisco UCS Blade Server model for this project and create the appropriate number of Service Profiles. From the Servers tab in the navigation page, from the Service Profile Templates node, expand the root and select Service Template B200 M3, then click Create Service Profiles from Template in the right pane, Actions area.

Tailt Sammary	🥥 🕕 🗈 New - 📿 Optors 🛛 O	Arendrig Activities	1
2 0 8 3		🙏 root + 🎆 Service Template 8200PD-8P5-Template	Service Template 8200HD-0PS-Temple
Coupment Servers LAN SAN VM Admin	General Storage Network GCSLvNdCs Boot	Inder Pokies Events FSM	
Part A and A	Contract Sources Andrées Annue Marielles Private Contract & Clove Contract & Clove	Properties Income 2003-2015 Computer Uncer 2003-2015 Computer Description Uncer 2003-2015 Computer Uncer 2004-2014 Computer Annuel Computer Provide Annuel Computer Description Descriptio	file if it migrates between servers.

45. Provide the naming prefix and the number of Service Profiles to create and click OK.

📥 Create Service Profiles From Template	×
Create Service Profiles Fr	om Template 👘 🤨
Naming Prefix: B200M3-VDI-E5Xi51-Srv	
Number: 14	
	· .
	OK Cancel

I

46. Cisco UCS Manager creates the requisite number of profiles and because of the Associated Server Pool and Server Pool Qualification policy, the Cisco UCS B200 M3 blades in the test environment automatically associate with the proper Service Profile.



This process was repeated for the Cisco UCS B250M2-INFRA-SAN template and the same result was achieved.



47. Verify that each server has a profile and that it receives the correct profile. The image below is a Cisco UCS B200 M3 Sample:



The Cisco UCS Blade Servers are ready for the hypervisor installation.

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.

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 9217.
- Through Cisco Unified Computing System you 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).

(Weight of the given priority * 100)

% b/w shared of given Class = ____

Sum of weights of all priority

Cisco UCS Class Configuration

- Platinum
- Gold
- Silver
- Bronze

Table 3 Name Table Map Between Cisco UCS 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

Steps to Enable QOS on 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	166 (Storage – Not used in FC variant)
Gold	eth4, eth5	122 (VDA)
Silver	eth0, eth1	164 (Management)
Bronze	eth6, eth7	169 (vMotion)

Configure Platinum, Gold, Silver and Bronze policies by checking the enabled box. The Platinum Policy, used for NFS storage, was configured for Jumbo Frames in the MTU column. Notice the option to set no packet drop policy during this configuration.

Figure 10 Cisco UCS QoS System Class Configuration

🚊 Cisco Unified Co	mputing System M	lanager - FT-6248A)											_0
Fault Summary	V	Δ		0	D New	• 😧 🕬	tions	0 0 🖾 Per	ding Activities	🙆 Evit				¢.
2	0	8	3	>>		AN Cloud *	🙀 Qo5 :	System Class						🙀 QoS System Clar
Equipment Servers	LAN SAN VH A	dmin		60	neral Events /	5M								
	Filter: Al				Priority	Enabled	Co5	Packet Drop	Weight		Weight (%)	MTU		Multicast Optimized
d (1)					Platinum	P	5	R	10		22	9000		
B LAN B C LAN Cloud					Gold		4	R	9		20	normal		T
B C Fabric					Silver	P	2	R	8		18	normal		
8 m Fabric	8 iysten Class 🚽				Bronze	P	1	P	7		15	nomal	*	F
LANP	in Groups				Best Effort	F	Any	R	5		11	normal	-	F
8-5 Thres	hold Policies				Fibre Channel	F	3		5		14	fc		N/A
Applance Applance Diternal L	s AN													

Next, from 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 11 Cisco UCS QoS Policy Configuration

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 12 Utilize QoS Policy in vNIC Template



This is a unique value proposition for Cisco Unified Computing System with respect to end-to-end QOS. For example, there is a VLAN for the EMC storage; configure the Platinum policy with Jumbo frames and receive an end-to-end QOS and performance guarantees from the Blade Servers to the Nexus 1000V virtual distributed switches running in vCenter through the Nexus 5548UP access layer switches.

LAN Configuration

I

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.

Cisco UCS Connectivity

Four 10 Gigabit Ethernet uplink ports are configured on each of the Cisco UCS 6248 fabric interconnects, and they are connected to the Cisco Nexus 5548 pair in a bow tie manner as shown below in a port channel.

The 6248 Fabric Interconnect is in End host mode, as we are doing both Fiber Channel as well as Ethernet (NAS) data access as per the recommended best practice of the Cisco Unified Computing System. We built this out for scale and have provisioned more than 40 G per Fabric interconnect (Figure 13).



The upstream configuration is beyond the scope of this document; there are some good reference document [4] that talks 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 13 Ethernet Network Configuration with Upstream Cisco Nexus 5500 Series from the Cisco Unified Computing System 6200 Series Fabric Interconnects



EMC VNX5500 LAN Connectivity

The Cisco Nexus 5548UP is used to connect to the EMC VNX5500 storage system for Fiber Channel and file-based access.

The VNX5500 is equipped with dual-port 8GB FC modules on each controller. These are connected to the pair of Nexus 5548 unified ports to provide block storage access to the environment. (See section SAN Configuration)

The VNX5500 supports two dual-port 10G Data Movers which are connected to the pair of N5Ks downstream. One of the Data Movers is set to Active, with the second providing failover capability. This allows end-to-end 10G access for file-based storage traffic. We have implemented jumbo frames on the ports and have priority flow control on, with Platinum CoS and QoS assigned to the vNICs carrying the storage data access on the Fabric Interconnects. (Note: This configuration was not used in this study, but is shown as a supported option.)

The EMC ethernet connectivity diagram is shown below. There is a total of 40 Gbps bandwidth available for the servers.



Figure 14 EMC VNX Ethernet Connectivity





ſ

For information on configuring ethernet connectivity on a EMC VNX5500 Storage System, refer to the EMC website: www.emc.com.

Nexus 1000V Configuration in L3 Mode

- Download the Nexus1000 V 4.2(1) SV1 (5.2): http://www.cisco.com/cisco/software/release.html?mdfid=282646785&flowid=3090&softwareid= 282088129&release=4.2(1)SV1(5.2)&relind=AVAILABLE&rellifecycle=&reltype=latest
- 2. Extract the downloaded N1000V .zip file on the Windows host.
- **3.** To start the N1000V installation, run the command below from the command prompt. (Make sure the Windows host has the latest Java version installed)



4. After running the installation command, you will see the "Nexus 1000V Installation Management Center."

I

🛃 Nexus 1000V Installation Manageme		_
Steps	Enter vCenter Credentials	
Enter vCenter Credentials Select the VSM's host Select OVA File to create VSM Configure Networking Configure Networking Configure VSM Centrol ConfigureItion	vCenter IP 10.29.165.41 Port (https only) 443 vCenter User ID administrator vCenter Password *******	
7. Configure Migration 8. DVS Migration		
CISCO. Nexus 1000V		

5. Enter the vCenter IP and the logon credentials.

Steps	Select the VSM's host
L. Exter vCerter Credentials Select UK 1 Hot oracle VSH L. configure Hetworking C. configure Hetworking L. externer Configuration L. DrSH Migration L. DrSH Migration Migration	WCenter Inventory W VD1 W Hotski Folders/Clusters W VB1 W VB1 <

I

Γ

- 6. Select the ESX host on which to install N1KV Virtual Switch Manager.
- 7. Select the OVA file from the extracted N1KV location to create the VSM.

Steps	Select OVA File to create VSM	
Etter vCerter Credenbals .Select UM Hits to create VSM .confayer Networking .confayer Networking .onfayer Networking .enview Confayer also .DrS Migration .DrS Migration	OVA Image System Rodundancy Vital Machine Name Vital Machine Name PatraStore Centre Record Look II: PatraStore PatraSt	Browse OVA
Nexus 1000V	My, Coursents	

8. Select the System Redundancy type as "HA" and enter the virtual machine name for the N1KV VSM and choose the Datastore for the VSM.



- 9. To configure L3 mode of installation, select the "L3 : Configure port groups for L3"
 - a. Create Port-group as Control and specify the VLAN ID and select the corresponding vSwitch.

- **b.** Select the existing port group "VM Network" for N1K Mgmt and choose mgmt0 with the VLAN ID for the SVS connection between vCenter and VSM.
- **c.** In the option for L3 mgmt0 interface port-profile enter the vlan that was pre-defined for ESXi mgmt and accordingly it will create a port-group which will have L3 capability. In this case it is n1kv-L3 port-group as shown in the screenshot below.

```
UDI-M1KU-DUS# sh run port-profile n1kv-L3

!Command: show running-config port-profile n1kv-L3

!Time: Fri Oct 26 16:53:34 2012

version 4.2(1)SU1(5.2)

port-profile type vethernet n1kv-L3

capability 13control

vmmare port-group

switchport mode access

switchport access vlan 164

no shutdown

system vlan 164

state enabled
```

Steps	Configure Networking		
1. Enter vCenter Credentials 2. select White the VSM's host 3. Select VAN File to create VSM 4. Configure Networking 5. Configure VS 6. Benier Configuration 7. Configure Hypothon 8. DVS Migration	Please choose a configuration option: T L2: Configure port groups for L2. T L3: Configure port groups for L3. Control Port Group: C Choose Existing C Create Port Group: Conterr Management, MARE 0 P Valedat Vehich D (PECC): Venico	e New Port Group Name: VLAN ID: vSwitch:	Control 167 vSwtch0, PMICs: vmrk0
CISCO Nexus 1000V	Management Port Group: (* Choose Existing (*) Port Group: (MMMethonh, VLME: 165 v Voletch: voletch0, PMBCs: vmex0 Choose an interface for L3 Connectivity: (* proutid Exister L3 mgmb0 Interface Port Profile VLMI) (*)	Create New Port Group Name: VLAN ID: vSwitch: C control0	(South), PAICs: venico

10. To Configure VSM, Type the Switch Name and enter the admin password for the VSM. Type the IP address, subnet mask, Gateway, Domain ID (Note: If there are multiple instance of N1KV VSM need to be install, make sure that each are configured with different Domain ID) and select the SVS datacenter Name and Type the vSwitch0 Native vlan ID. (Make sure the Native VLAN ID specified should match the Native VLAN ID of Cisco UCS and the Nexus 5k)

Steps	Configure VSM	
	Configure V9-1 Switch Name Admin User Name Dither Admin Sessord Corfm. Admin Password Corfm. Admin Password Mogil: Ph. Address Subnet Mask. Gateway: Ph. Address Domain ID PVS Dutacenter Name viswitch Native VLAN ID IF Enable SSH (USA 2049 bits)	VOL-NIKV Madian Terrererererererererererererererererere
		<prev [<="" td=""></prev>

I

11. Review the configuration and click Next to proceed with the installation.

	Review Configuration	
reps	Review Configuration	
Enter vCenter Credentials Select the VSM's host	Primary Host IP Address	10.29.164.120
Select OVA File to create VSM	Secondary Host IP Addres	s 10.29.164.120
Configure Networking	Primary VSM VM Name	VDI-NIKV-1
Configure VSM Review Configuration	Secondary VSM VM Name	VDI-NIKV-2
Configure Migration	Datastore	InfraStore
DVS Migration	Control Port Group	Control, VLAN: 167 on vSwitch0, PNBCs: vmnic0
	Management Port Group	VM Network, VLAN: 165
	L3 Interface	mgmt0
	L3 Mgmt0 Host Vian	165
	VSM Switch Name	VDI-NIKV
	Management IP Address	10.29.165.47
	Subnet Mask IP Address	255.255.255.0
CISCO.	Gateway IP Address	10.29.165.1
Nexus 1000V		ha
1102003 10001	Domain ID	165
	Datacenter (SVS)	NOI
	Enable SSH	Yes
	Enable Teinet	Yes
	vSwitch0 Native VLAN ID	164

1

12. Wait for the Completion of Nexus 1000V VSM installation.

Sexus 1000V Installation Manageme	nt Center 📃 🖾 🗙
Steps	Review Configuration
Lotter Vorder Orderstelle Schert ber Vorder Forderstelle Schert ber Vorder for sorease VSM Schert ber VSM Configure Monten Configure Manadom Config	Inst allotion Progress: Configuring Responses: Configuring Responses: Configuring Responses: Configuring Properties: Configuring Property Specification Configuring Distribution Response On VBM Control (Station Property Specification Control (Station Property Specification Configuring Distribution Response On VBM Control (Station Properties) Deleting Temporary Files Validating Install Installation Completed
Powering On VSN	
	< Prev Next > Finish Cancel

13. Click Finish to complete the VSM installation.


14. Log into (ssh or telnet) to the N1KV VSM with the IP address and configure VLAN for ESX Mgmt, Control, N1K Mgmt and also for Storage and vMotion purposes as mentioned below (VLAN ID differs based on your Network). No need to create VLANs for N1KV packet and control with version 4.2(1)SV2(1.1) of N1KV installer.

VDI-N1KV# conf t

15. Enter the following configuration commands, one per line, an d end with CNTL/Z:

```
VDI-N1KV(config) # vlan 122
VDI-N1KV(config-vlan) # name
                             VDA
VDI-N1KV(config-vlan) # no sh
VDI-N1KV(config) # vlan 164
VDI-N1KV(config-vlan) # name ESXi-Mgmt
VDI-N1KV(config-vlan) # no sh
VDI-N1KV(config) # vlan 165
VDI-N1KV(config-vlan) # name Infra-Mgmt
VDI-N1KV(config-vlan) # no sh
VDI-N1KV(config) # vlan 166
VDI-N1KV(config-vlan) # name Storage
VDI-N1KV(config-vlan) # no sh
VDI-N1KV(config) # vlan 167VDI-N1KV(config-vlan) # name N1K-Control
VDI-N1KV(config-vlan) # no sh
VDI-N1KV(config) # vlan 169
VDI-N1KV(config-vlan) # name vMotion
VDI-N1KV(config-vlan) # no sh
VDI-N1KV (config) #<CNTRL/Z>
```

```
vlan 122
name VDI-desktops
vlan 164
name ESX_Mgmt
vlan 165
name Infra_Mgmt
vlan 166
name Storage
vlan 167
name Control
vlan 169
name vMotion
```

I

16. Run the following configuration command to configure jumbo mtu and qos polices: VDI-N1KV# conf t

```
VDI-N1KV(config)# policy-map type qos jumbo-mtu
VDI-N1KV(config-pmap-qos)# policy-map type qos platinum_Cos_5
VDI-N1KV(config-pmap-qos)# class class-default
VDI-N1KV(config-pmap-c-qos)# set cos 5
VDI-N1KV(config-pmap-c-qos)# end
VDI-N1KV# copy running-config startup-config
policy-map type qos jumbo-mtu
```

policy-map type qos platinum_Cos_5

class class-default set cos 5

17. To migrate and manage all the ESXi you will need to network using Nexus 1000V VSM, Configure Port Profiles and port groups as shown below.

```
port-profile type ethernet Unused_Or_Quarantine_Uplink
vmware port-group
shutdown
description Port-group created for Nexus1000V internal usage.
Do not use.
state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
vmware port-group
shutdown
description Port-group created for Nexus1000V internal usage.
Do not use.
state enabled
```

```
<u>Note</u>
```

Do not make any changes to the port profiles; they are created by default.

18. Create the DC System Uplink for ESXi and Nexus 1000V Management:

```
VDI-N1KV(config)# port-profile type ethernet Mgmt-uplink
VDI-N1KV(config)# vmware port-group
VDI-N1KV(config-port-prof)# switchport mode trunk
VDI-N1KV(config-port-prof)# switchport trunk allowed vlan 164-165,167
VDI-N1KV(config-port-prof)# channel-group auto mode on mac-pinning
VDI-N1KV(config-port-prof)# no shutdown
VDI-N1KV(config-port-prof)# system vlan 164,167
VDI-N1KV(config-port-prof)# system vlan 164,167
```

19. Create the DC Storage Uplink port profile for NFS traffic:

```
VDI-N1KV(config)# port-profile type ethernet storage-uplink
VDI-N1KV(config)# vmware port-group
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 166
VDI-N1KV(config-port-prof)# mtu 9000
VDI-N1KV(config-port-prof)# channel-group auto mode on mac-pinning
VDI-N1KV(config-port-prof)# no shutdown
VDI-N1KV(config-port-prof)# system vlan 166
VDI-N1KV(config-port-prof)# system vlan 166
```

```
port-profile type ethernet storage-uplink
wmware port-group
mtu 9000
switchport mode access
switchport access vlan 166
channel-group auto mode on mac-pinning
no shutdown
system vlan 166
state enabled
```

20. Create the Storage virtual ethernet communications port profile:

```
VDI-N1KV(config)# port-profile type vethernet storage
VDI-N1KV(config-port-prof)# vmware port-group
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 166
VDI-N1KV(config-port-prof)# service -policy type qos input platinum_Cos_5
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV(config-port-prof)# system vlan 166
VDI-N1KV(config-port-prof)# state enabled
```

port-profile type vethernet storage
vmware port-group
switchport mode access
switchport access vlan 166
service-policy type gos input platinum Cos 5
no shutdown
system vlan 166
state enabled

21. Create the DC vMotion Uplink port profile:

```
VDI-N1KV(config)# port-profile type ethernet vmotion-uplink
VDI-N1KV(config-port-prof)# vmware port-group
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 169
VDI-N1KV(config-port-prof)# channel-group auto mode on mac-pinning
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV(config-port-prof)# system vlan 169
VDI-N1KV(config-port-prof)# system vlan 169
```

```
port-profile type ethernet vmotion-uplink
vmware port-group
switchport mode access
switchport access vlan 169
channel-group auto mode on mac-pinning
no shutdown
system vlan 169
state enabled
```

22. Create the virtual ethernet port profile for vMotion:

```
VDI-N1KV(config)# port-profile type vethernet vmotion
VDI-N1KV(config-port-prof)# vmware port-group
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 169
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV(config-port-prof)# system vlan 169
VDI-N1KV(config-port-prof)# system vlan 169
```



23. Create the DC VDA Uplink port profile:

```
VDI-N1KV(config)# port-profile type ethernet vdi-uplink
VDI-N1KV(config-port-prof)# vmware port-group
VDI-N1KV(config-port-prof)#switchport mode access
VDI-N1KV(config-port-prof)#switchport access vlan 122,164-165
VDI-N1KV(config-port-prof)#channel-group auto mode on mac-pinning
VDI-N1KV(config-port-prof)#no shutdown
VDI-N1KV(config-port-prof)# system vlan 122,165
VDI-N1KV(config-port-prof)# system vlan 122,165
```

port-profile type ethernet vdi-uplink
vmware port-group
switchport mode trunk
switchport trunk allowed vlan 122,164-165
channel-group auto mode on mac-pinning
no shutdown
system vlan 122,165
state enabled

24. Create the virtual ethernet port profile for VDA traffic:

```
VDI-N1KV(config)# port-profile type vethernet vdi-pool1
VDI-N1KV(config)# vmware port-group
VDI-N1KV(config-port-prof)# port-binding static auto expand
VDI-N1KV(config-port-prof)# max-ports 1024
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 122
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV(config-port-prof)# system vlan 122
VDI-N1KV(config-port-prof)# system vlan 122
```



25. Create the virtual ethernet port profile for VDA1 traffic:

```
VDI-N1KV(config)# port-profile type vethernet vdi-pool2
VDI-N1KV (config-port-prof)# vmware port-group
VDI-N1KV(config-port-prof)# port-binding static auto expandVDI-N1KV
(config-port-prof)# max-ports 1024
VDI-N1KV(config-port-prof)# switchport mode access
VDI-N1KV(config-port-prof)# switchport access vlan 122
VDI-N1KV(config-port-prof)# no sh
VDI-N1KV (config-port-prof)# system vlan 122
VDI-N1KV(config-port-prof)# system vlan 122
VDI-N1KV(config-port-prof)# state enable
```

```
port-profile type vethernet vdi-pool2
vmware port-group
switchport mode access
switchport access vlan 122
no shutdown
system vlan 122
max-ports 1024
state enabled
```

26. After creating port profiles, make sure vCenter shows all the port profiles and port groups under the respective N1KV VSM. Then, Add the ESXi host to the VSM.

I

27. Go to Inventory> networking > select DVS for N1KV> click Hosts.

Storage-Uplink										Name or State cor	ntains: *	Cie
System_Upirk	Name	2.sto	V05 9J	Rus	2.0	15	% OPU	% Memory	Memory Size	CPU Count	NDC Count Uptime	_
sug_r0_t	10.29.164.91	Connected	0 4	p		Normal	0	4	262086-00 MB	2	8 7 days	
pink m-Upink	10.29.164.92	Connected	0 4	p.		Normal	0	2	262086-00 MB	2	8 7 days	
*	10.29.164.90	Connected	0 4	p	•	Normal	0	1	262006-00 MB	2	8 7 days	
y_Qur	☐ 10.29.164.98	Connected	o u		•	Normal	•	: (252066.00 MB	2	8 7 days	

28. Right-click and select Add host to vSphere Distributed Switch.

Storage-Uplink								Name or State	contains: •
	Name	State	VDS Status	244	% CPU	% Memory	Memory Size	CPU Count	NOC Count Upt
Unused_Or_Que	10.29.164.91	Connected	🗢 Up	Normal	0	4	262086.00 MB	2	8 7 di
VC6-Uplink.	10.29.164.92	Connected	🔿 Up	Normal	0	2	262086.00 MB	2	8 7 di
vMotion-Uplink n1ko-0	10.29.164.90	Connected	🗢 Up	Normal	0	1	262086.00 MB	2	8 7 di
Storage	10.29.164.94	Connected	🙂 Up	Normal	0	1	262086.00 MB	2	8 7 di
VDE-5 vMotion antrol aduet			Manage Hos Refresh		arrichten.				
er Managemenit 1 twork			View Colum Export List		•				



ſ

This brings up the ESXi hosts which are not part of the existing configuration.

29. Select ESXi hosts to add in N1KV.

Select Hosts and Physical Adapter Select hosts and physical adapters	rs : to add to this vSphere distributed s	witch.			
elect Host and Physical Adapters	ī			Settings View Incompati	ble Hos
letwork Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group	
rtual Machine Networking	🔲 🥽 vmnic3		View Details	Select an uplink port gr	
eady to Complete	vmnic4		View Details	Select an uplink port gr	
	E 10.29.164.126		View Details		
	Select physical adapters				
	🔲 📰 vmnic0	vSwitch0	View Details	Select an uplink port gr	
	🔲 🦏 vmnic2		View Details	Select an uplink port gr	
	🔲 📷 vmnic3		View Details	Select an uplink port gr	
	🔲 i vinnic4		View Details	Select an uplink port gr	
	Image: Book of the second s		View Details		
	Select physical adapters				
	🔲 🖏 vmnic0	vSwitch0	View Details	Select an uplink port gr	
	vmnic1		View Details	Select an uplink port gr	
	🔲 💵 vmnic2		View Details	Select an uplink port gr	
	🔲 📷 vmnic4		View Details	Select an uplink port gr	
	E 🗹 📋 10.29.164.95		View Details		
	Select physical adapters				
	🔲 📰 vmnic0		View Details	Select an uplink port gr	
	🔲 🔛 vmnici	vSwitch0	View Details	Select an uplink port gr	
	🔲 🛤 vmnic2		Vew Details	Select an uplink port gr	
	🔲 🜇 vmnic3		View Details	Select an uplink port gr	
	🗖 🛤 vmnic4		Vew Details	Select an uplink port gr	
	🔲 🜇 vmnic5		View Details	Select an uplink port gr	
	🔲 🐖 vmnic6		View Details	Select an uplink port gr	
	🗖 📪 vmnic7		View Details	Select an uplink port gr	

30. Click Select an uplink port-group and from the drop-down menu select appropriate Uplink that is allowed for corresponding vmnic as per the configuration on Cisco UCS Manager vNICS.

For example, consider vmnic0 and vmnic1 for use as the System-Uplink. As per the best practices here we have 8 vmnics (4 pairs) and each pair of vmnics will be associated with one uplink; system/mgmt uplink, storage uplink, VM/VDI traffic uplink, vMotion Uplink.

Image: Select physical adapters

View Details...

View Details...

1

Seleccpr	iysical adapters			
🗹 छ	vmnic0		View Details	Select an uplink port gro 💌
🗹 💷	vmnic1	vSwitch0	View Details	Select an uplink port group
🗹 🚥	vmnic2		View Details	Storage-Uplink
- - -	vmnic3		View Details	System_Uplink Unused_Or_Quarantine_Upli
🗹 🚥	vmnic4		View Details	VDI-Uplink
- - -	vmnic5		View Details	vMotion-Uplink
🗹 💷	vmnic6		View Details	Select an uplink port gr
v 💀	vmnic7		View Details	Select an uplink port gr

□ □ □ 10.29.164.95 Select physical adapters

Select pl	nysical adapters			
V 💀	vmnic0		View Details	Select an uplink port gr
🗹 💷	vmnic1	vSwitch0	View Details	Select an uplink port gr
🗹 📭	vmnic2		View Details	Select an uplink port gro 💌
🗹 💷	vmnic3		View Details	Select an uplink port group
🗹 💷	vmnic4		View Details	Storage-Uplink System Uplink
🗹 💷	vmnic5		View Details	Unused_Or_Quarantine_Upli
🗹 💷	vmnic6		View Details	VDI-Uplink
🗹 💷	vmnic7		View Details	Motion-Uplink

	View Details	System_Uplink
vSwitch0	View Details	System_Uplink
	View Details	Storage-Uplink
	View Details	Storage-Uplink
	View Details	Select an uplink port gro 💌
	View Details	Select an uplink port group
	View Details	Storage-Uplink System Uplink
-	View Details	System_Opink Unused_Or_Quarantine_Upli VDI-Uplink
		vMotion-Uplink
	-	View Details View Details View Details View Details View Details

- ! 1	0.29.164.95		View Details	
Select pl	nysical adapters			
I	vmnic0		View Details	System_Uplink
I 💀	vmnic1	vSwitch0	View Details	System_Uplink
I	vmnic2		View Details	Storage-Uplink
I	vmnic3		View Details	Storage-Uplink
🗹 💷	vmnic4		View Details	VDI-Uplink
I 💀	vmnic5		View Details	VDI-Uplink
I 💀	vmnic6		View Details	Select an uplink port gro 💌
2 💀	vmnic7		View Details	Select an uplink port group Storage-Uplink System Uplink
				System_opiink Unused_Or_Quarantine_Upli VDI-Uplink vMotion-Uplink

31. After selecting appropriate uplinks click Next.

🗹 瞑 vmnic0		View Details	System_Uplink	
vmnic1	vSwitch0	View Details	System_Uplink	
🗹 瞑 vmnic2		View Details	Storage-Uplink	
🗹 🛄 vmnic3		View Details	Storage-Uplink	
🗹 瞑 vmnic4		View Details	VDI-Uplink	
Vmnic5	-	View Details	VDI-Uplink	
🗹 🔢 vmnicé	-	View Details	vMotion-Uplink	
🗸 📷 🛛 vmnic7		View Details	vMotion-Uplink	

32. From the Network Connectivity tab, select Destination port group for vmk0.

Network Connectivity Select port group to provide net	work connectivity for the adapters	s on the vSphere distrib	uted switch.	
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking		the warning sign might		ti-select. ess they are migrated to the vSphere distributed swi
Ready to Complete	Host/Virtual adapter	Switch	Source port group	Destination port group
	-			
	In 10.29.164.95			

33. From the drop-down menu select a port group that was configured for L3 capability and for ESXi host management communication. In this case it is n1kv-13 and click Next.

Network Connectivity Select port group to provide net	work connectivity for the adapters	on the vSphere distrib	uted switch.		
Select Host and Physical Adapters Network Connectivity			lose network connectivity unli	ti-select. ess they are migrated to the vSphere dis	ributed switch.
Virtual Machine Networking	select a descriation port				
Virtual Machine Networking Ready to Complete	Host/Virtual adapter	Switch	Source port group	Destination port group	
				Destination port group	

34. On the tab for virtual machine networking, select VMs and assign them to a destination port-group if there are any. Otherwise click Next.

Virtual Machine Networking Select virtual machines or netwo	ik adapters to migrate to the vSphere distribute	rd switch.		
elect Host and Physical Adapters Jetwork Connectivity	 Migrate virtual machine networking Assign VMs or network adapters to a d 	lestination port group to migrate	them. Ctrl+click to multi-select.	
Virtual Machine Networking Ready to Complete	Host/Virtual machine/Network adapter	NIC count Source port grou		
	Network adapter details			Assign port gro

I

35. Verify the Settings and click Finish to add the ESXi host part of N1KV DVS.





This will invoke VMware update manger (VUM) to automatically push the VEM installation for the selected ESXi hosts. After successful staging, install and remediation process, now the ESXi host will be added to N1KV VSM. From the vCenter task manager, quickly check the process of VEM installation.

In the absence of Update manager:

- 1. Upload vib file cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.1.vib for VEM installation to local or remote datastore which can be obtained by browsing to the management IP address for N1KV VSM.
- 2. Login to ESXi host using ESXi shell or SSH session.
- **3**. Run the following command:

esxcli software vib install -v /vmfs/volumes/ datastore/ cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.1.vib

4. Verify the successful installation of ESXi VEM and the status of ESXi host.

VCENTER.vdilab-v.local - vSphere 0	lient						The second s		0	•
File Edit View Inventory Admini	istration Plug-ins H	elp								
🖸 🔯 🔥 Home 🕽 🚮 Stre	entory 🕨 💇 Networ	king						Search 1	Inventory	
4 10 2 4										
© VCENTER.vdiab-v.local B ↓ v04-2000 B ♥ V04-0xxv B ▲ V04-0xxv B ▲ V04-0xxv	VDI-NIKV Getting Started Su	nnay (Networ	ia Para Conf	iguration 🛛 Wrbuel Mad	Viel Hoto Ta	ks & Events Alama	Permissione	Name or State	contains: •	_
Storage-Uplink System_Uplink	Nate	2.44	105 Status	Salus	% OPU	% Memory	Memory Size	CPU Count	MC Court Uptime	-
B. Unued, Or., Out B. Vickapink B. Wetzon-Lipink B. Water, United B. Strange Wetzon Control NIX-Control NIX-Control NIX-Control NIX-Control	10.29.164.9 10.29.164.9 10.29.164.9 10.29.164.9 10.29.164.95	Connected Connected Connected Connected Connected		 Nornal Nornal Nornal Nornal Nornal 	0 0 0 0		262066.00 MB 262066.00 MB 262066.00 MB 262066.00 MB 262066.00 MB	2 2 2 2 2	8 7 days 8 7 days 8 7 days 8 7 days 8 7 days 8 45 minutes	

5. Verify putty into N1KV VSM. Run sh module command which will show all the ESXi hosts attached to that VSM.

VDI-N1KV(config) # sh module

VDI-	N1KV (co	nfig)# sh mod	ule				
Mod	Ports	Module-Type				Model	Status
		Virtual Supe	rvisor 1	Modul	2	Nexus1000V	active *
		Virtual Supe	rvisor 1	Modul	2	Nexus1000V	ha-standby
16	248	Virtual Ethe	rnet Mo	dule		NA	ok
17	248	Virtual Ethe	rnet No	dule		NA	ok
18	248	Virtual Ethe	rnet Mo	dule		NA	ok
19	248	Virtual Ethe	rnet No	dule		NA	ok
20	248	Virtual Ethe	rnet Mo	dule		NA	ok
Mod	Sw		Hw				
1 2	4.2(1)	SV1(5.2)	0.0				
	4.2(1)	SV1(5.2)	0.0				
16	4.2(1)	SV1(5.2)	VMware	ESXi	5.1.0	Releasebuild-799733	(3.1)
17	4.2(1)	SV1(5.2)	VMware	ESXi	5.1.0	Releasebuild-799733	(3.1)
18	4.2(1)	SV1(5.2)	VMware	ESXi	5.1.0	Releasebuild-799733	(3.1)
19	4.2(1)	SV1(5.2)	VMware	ESXi	5.1.0	Releasebuild-799733	(3.1)
20	4.2(1)	SV1(5.2)	VMware	ESXi	5.1.0	Releasebuild-799733	(3.1)

Nod	Server-IP	Server-UUID	Server-Name
1	10.29.165.47	NA	NA
2	10.29.165.47	NA	NA
16	10.29.164.93	9476f312-1321-e111-0000-1b00000006e	10.29.164.93
17	10.29.164.91	9476f312-1321-e111-0000-1b000000005f	10.29.164.91
18	10.29.164.94	9476f312-1321-e111-0000-1b000000007e	10.29.164.94
19	10.29.164.92	9476f312-1321-e111-0000-1b000000001f	10.29.164.92
20	10.29.164.95	9476f312-1321-e111-0000-1b000000004e	ESX15-BFS-Srv5

6. Repeat the procedure to configure additional VSM pairs for each ESX cluster.

SAN Configuration

The same pair of Nexus 5548UP switches were used in the configuration to connect between the FC ports on the EMC VNX5500 and the FC ports of the UCS 6248 Fabric Interconnects.

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 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 of the 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.

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.

SAN Configuration on Nexus 5548UP

The FCoE and NPIV feature has to be turned on in the Nexus 5500 series switch. Make sure you have 8 GB SFP+ modules connected to the Nexus 5548UP ports. The port mode is set to AUTO as well as the speed is set to AUTO. Rate mode is "dedicated" and when everything is configured correctly you should see something like the output below on a Nexus 5500 series switch for a given port (for example, Fc1/17).



A Nexus 5500 series switch supports multiple VSAN configurations. A single VSAN was deployed in this study.

Cisco Fabric Manager can also be used to get a overall picture of the SAN configuration and zoning information. As discussed earlier, the SAN zoning is done upfront for all the pwwns of the initiators with the EMC VNX5500 target pwwns.

```
VDI-N5548-A# show feature | grep npiv
npiv 1 enabled
VDI-N5548-A# show interface brief
```

Interface	Vsan	Admin	Admin	Status	S	SFP	Oper	Oper	Port		
			Mode	e Trunk						Mode	Speed
Channel											
				Mo	ode						
(Gbps)											
fc1/17	1	auto	on	up		swl	F	8			
fc1/18	1	auto	on	up		swl	F	8			
7.0					~						

The FC connection was used for configuring boot from SAN for all of server blades. In addition, a general purpose 1TB infrastructure LUN for infrastructure virtual machine storage and 14 write-cache LUNs for each VDI host were provisioned.

Single vSAN zoning was set up on the Nexus 5548's to make those VNX5500 LUNs visible to the infrastructure and test servers.

An example SAN zone configuration is shown below on the Fabric A side:

```
VDI-N5548-A# sh zone name B200M3-CH1-SERVER1-FC0 vsan 1
zone name B200M3-CH1-SERVER1-FC0 vsan 1
   member pwwn 20:00:00:25:b5:c1:00:af
                [B200M3-CH1-SERVER1-fc0]
L
   member pwwn 50:06:01:60:46:e0:5e:0a
!
                [VNX5500-A0]
    member pwwn 50:06:01:69:46:e0:5e:0a
1
                [VNX5500-B1]
VDI-N5548-A# sh zone name B200M3-CH1-SERVER2-FC0 vsan 1
zone name B200M3-CH1-SERVER2-FC0 vsan 1
   member pwwn 20:00:00:25:b5:c1:00:9f
               [B200M3-CH1-SERVER2-fc0]
1
   member pwwn 50:06:01:60:46:e0:5e:0a
                [VNX5500-A0]
!
   member pwwn 50:06:01:69:46:e0:5e:0a
I.
                [VNX5500-B1]
```

Where 20:00:00:25:b5:c1:00:af /20:00:00:25:b5:c1:00:9f are blade servers pwwn's of their respective Converged Network Adapters (CNAs) that are part of the Fabric A side.

The EMC FC target ports are 50:06:01:60:46:e0:5e:0a /50:06:01:69:46:e0:5e:0a and belong to one port on the FC modules on SP-A and SP-B.

Similar zoning is done on the second Nexus 5548 in the pair to take care of the Fabric B side as shown below:

```
VDI-N5548-B# sh zone name B200M3-CH1-SERVER1-FC1 vsan 1
                                                           zone name
B200M3-CH1-SERVER1-FC1 vsan 1
   member pwwn 20:00:00:25:b5:c1:00:bf
              [B200M3-CH1-SERVER1-fc1]
   member pwwn 50:06:01:61:46:e0:5e:0a
              [VNX5500-A1]
   member pwwn 50:06:01:68:46:e0:5e:0a
              [VNX5500-B0]
VDI-N5548-B# sh zone name B200M3-CH1-SERVER2-FC1 vsan 1
zone name B200M3-CH1-SERVER2-FC1 vsan 1
   member pwwn 20:00:00:25:b5:c1:00:8f
                [B200M3-CH1-SERVER2-fc1]
   member pwwn 50:06:01:61:46:e0:5e:0a
              [VNX5500-A1]
   member pwwn 50:06:01:68:46:e0:5e:0a
               [VNX5500-B0]
```

Where 20:00:00:25:b5:c1:00:bf /20:00:00:25:b5:c1:00:8f are blade servers pwwn's of their respective Converged Network Adapters (CNAs) that are part of the Fabric B side.

The EMC FC target ports are 50:06:01:61:46:e0:5e:0a /50:06:01:68:46:e0:5e:0a and belong to the other port on the FC modules on SP-A and SP-B. They were spread across the two controllers for redundancy as shown in Figure 16.



Figure 16 VNX5500 FC Target Ports

For detailed Nexus 5500 series switch configuration, refer to Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide. (See the Reference Section of this document for the link.)

Configuring Boot from SAN on EMC VNX

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

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

	meters						
Storage Pool Type:		O RAID G					
		eduled Auto	o-Tiering				
Storage Pool ID:	6						~
Storage Pool Name:	VDI-SAN	Boot					
- Extreme Perform							
RAID Configuration		mber of Fla	ab Dieles				
RAID Conngeration RAIDS (4+1)		nber of Fia					
Performance							
RAID Configuration RAID5 (4+1)		mber of SA Recommer					
Distribution Performance : 268							
Distribution Performance : 268 Disks	4.038 GB	(100.00%)				
Distribution Performance : 268 Disks • Automatic Use	4.038 GB	(100.00%)		Total Raw	Capacity:	2684.0.
Distribution Performance : 268 Disks • Automatic Use	4.038 GB	(100.00%) le Disks	Model	Total Raw	Capacity:	2684.0.
Distribution Performance : 268 Disks • Automatic Use Manual Disk * Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10	(100.00%) Select Drive Type SAS	Model STE600	State	Capacity:	2684.0.
Distribution Performance : 268 Oisks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9	(100.00%) Select Drive Type SAS SAS	Model STE600 STE600	State Unb	Capacity:	2684.0.
Distribution Performance : 268 • Aytomatic Use • Manual Disk • Bus 0 Enclosure 3 • Bus 0 Enclosure 3 • Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8	(100.00%) Select Drive Type SAS SAS SAS	Model STE600 STE600 STE600	State Unb Unb	Capacity:	2684.0.
Distribution Performance : 268 Disks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8 3 Disk 7	(100.00%) Select SAS SAS SAS SAS SAS SAS	Model STE600 STE600 STE600 STE600	State Unb	Capacity:	2684.0.
Distribution Performance : 268 Oisks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8 3 Disk 7	(100.00%) Select SAS SAS SAS SAS SAS SAS	Model STE600 STE600 STE600 STE600	State Unb Unb Unb	Capacity:	2684.0.
Distribution Performance : 268 Oisks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8 3 Disk 7	(100.00%) Select SAS SAS SAS SAS SAS SAS	Model STE600 STE600 STE600 STE600	State Unb Unb Unb	Capacity:	2684.0.
Distribution Performance : 268 Oisks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8 3 Disk 7	(100.00%) Select SAS SAS SAS SAS SAS SAS	Model STE600 STE600 STE600 STE600	State Unb Unb Unb	Capacity:	2684.0.
Distribution Performance : 268 Oisks Automatic Use Manual Disk Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3 Bus 0 Enclosure 3	4.038 GB Power Sa 3 Disk 10 3 Disk 9 3 Disk 8 3 Disk 7	(100.00%) Select SAS SAS SAS SAS SAS SAS	Model STE600 STE600 STE600 STE600	State Unb Unb Unb	Capacity:	2684.0.

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

VNX5500 - Create	LUN						_ 0
General Advance	ed						
┌ Storage Pool	Properties						
Storage Pool Ty	pe:	<u>е</u>	ool 🔘 <u>R</u> AID Grou	P			
RAID Type:		RAI	D5: Distributed Pa	rity (Hi	igh Throug	ghput)	~
Storage Pool for	new LUN:	VDI,	/Infra-SANBoot		~	New	v
Available Capa		00 GE	B Consumed	Capaci	ity: 387.7	56 GB	
LUN Propertie	5						
User Capacity:	10			-	GB		~
LUN ID:	37	~	Number of LUNs	to cre	ate: 1		~
LUN Name —							
🔘 Name							
Automaticall	y assign LUN	I IDs	as LUN Names				
			A	oply	<u>C</u> ancel		<u>H</u> elp

Γ

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



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.

Initiator Type: CLARiiON/VNX Salover Mode: //e-Active mode(ALUA)-failover Host Agent Information	
New Host October	
	d Host
Host Name: B200-CH3-BL-01 Browse Host	
IP Address: 192.168.1.63	

5. Assign each registered host to a separate storage group



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.

I

Show LUNs: N		age Groups			
Name A	ID	Capac	city	Drive Type	
🖅 – 🦋 Consister	ncy Gro		,		^
🕂 💭 MetaLUN					
🛨 – 🌃 Snapshot 🛨 – 🎬 Snapviev					**
- SP A	v Shaps				
🖃 – 👰 SP B					
🗄 – 🔛 Thin LUN	s				~
					A <u>d</u> d
Selected LUN	5				
Name	ID	Capacity	Drive Type	Host LUN	ID
ESXI5_BootLUN	0	15.000 GB	SAS	0	
					<u>R</u> emove

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.

SAN Configuration on Cisco UCS Manager

ſ

To enable Boot from SAN on the Cisco UCS Manager 2.1 (UCS-M) series, do the following:

1. Add SAN Boot for primary to the new policy. The vHBA name is optional, it can be left blank and it is unnecessary to enforce the vHBA name. Click OK.

reate Boot Policy			
		Add SAN Boot	
Name: VNX55	00BFS rom SAN Policy for VNX5500	Add SAN Boot	0
teoropoli addresses teorot on Boot Charl Charge 2 force vtillC/vtBA/SCSI Name 2 ARNINGS: te effective order of boot devices with the strategy of the strategy of the strategy the not selected, the vtICs/vtBA/SCSI Name 2 the not selected, the vtICs/vtBA/SCSI Name 2 the strategy of the strategy o	ndicate a boot order presence. In the same device class (LAN/Sto selected and the VMIC/VHBA/GC	SI does not rwise the o	
Add LCC-II Disk Add CD-RCM Add Floppy VNICs	Name	Order Primary	OK Cancel
Add SAN Boot Add SAN Boot Add SAN Boot Target		👞 Nove Do 🤝 Nove Down 🏦 Delete	

2. Add SAN Boot for primary to the new policy. The vHBA name is optional, it can be left blank and it is unnecessary to enforce the vHBA name. Click OK.

AN Boot 🥹
Pemary Secondary CK Cancel
ove Up

3. Add SAN boot for SAN Secondary, click OK. Leave the optional vHBA name blank.

1

Create Boot Policy	Add SAN Boot
Name: VNXSS008FS	Add SAN Boot
Description Goot From SAN Policy for VXX5500 Rebot on Boot Order Change & Enforce VMC/VHEA/SCS1 Name & WARNINGS The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (promary/secondary) does not indicate a boot order presence. The type (p	
Add Local Dick Add CD-ROM Add FRopy VNICS Stormer SAN secondary	Craer visic/vresposal visic 1/per con 20 wrVin (Cancel) Craer visic/vresposal visic 1/per con 20 wrVin (Cancel) Primary Secondary
VHBAN Add SAN Boot Add SAN Boot Carget ISCSI VNICS	▲ More Up マ More Down (@Dekte

4. Add the Boot target WWPN to the SAN Primary; make sure this matches the EMC VNX pwwn. To avoid any mistakes, copy and paste from the Nexus 5500 Series command, for each switch, as shown below:

VDI-N5548-A	# sh	ow fcns database vsan 1		
0xe300ef	Ν	50:06:01:60:46:e0:5e:0a	(Clariion)	scsi-fcp:both
0xe301ef	Ν	50:06:01:69:46:e0:5e:0a	(Clariion)	scsi-fcp:both
VDI-N5548-B	#	show fcns database vsan 1		
0x470400	Ν	50:06:01:61:46:e0:5e:0a	(Clariion)	scsi-fcp
0x470500	Ν	50:06:01:68:46:e0:5e:0a	(Clariion)	scsi-fcp

reate Boot Policy	Add SAN Boot Target	-×
Name: VNX5S00BFS	Add SAN Boot Target	0
Rebot on Boot Order Change Inforce vH2(VHBA)(SCS) Name: ARXINGS: In Sign (Smmary) sicondary) does not indicate a boot order presence is effective vH2(VHBA)(SCS) Name sicolated and by vH2(VHBA) its not selected, the vH2(VHBA)(SCS) are selected af the vH2(VHBA) its not selected, the vH2(VHBA)(SCS) are selected of they exit, and the ScS are selected of the VH2(VHBA) and the ScS are selected of the ScS are se	Storage(SCSI) Type: • Primary Seconds USCSI does not otherwise the vi	
Add Ekcopy Add Ekcopy VNICs Sorage Storage		\$0:06:01:61:3E:A0:30:99
veillas C	▲ More Do マ More Down (音Debte	

- 5. Repeat step 4 for SAN Primary's—SAN Target Secondary.
- 6. Repeat step 4 for SAN Secondary's—SAN Target Primary.
- 7. Repeat step 4 for SAN Secondary's—SAN Target Secondary.

At the end your Boot from SAN policy will look like the following:

Add Local Disk		Name	Order	WIC/WHEAISCSI WIC	Type	Lun ID	WWW	0
Add Floppy		CD-ROM	1			-		1
	8	Storage	2					
		E SAN primary		FC0	Primary			٦
dts (3	SAN Target primary			Primary	0	50:06:01:60:46:E0:5E:0A	
		SAN Target secondary			Secondary	0	50:06:01:69:46:E0:5E:0A	
Add LAN Boot		E E SAN secondary		FC1	Secondary			1
		SAN Target primary			Primary	0	50:06:01:61:46:E0:5E:0A	
IBAs (3	SAN Target secondary			Secondary	0	50:01:06:68:46:E0:5E:0A	
NORT C	ė	LAN	3					
Add SAN Boot		LAN Eth0		Eth0	Primary			
Add SAN Boot Target								
CSI VNICs	3							
CSI WILLS								
Add ISCSI Boot								

8. Make the association of the service profile template to the Boot from SAN policy during the service profile template configuration which was described earlier in this document.

EMC VNX5500 Storage Configuration

ſ

Figure 17 illustrates the layout of the disks that are required to store 2,000 desktop virtual machines. This layout does not include space for user profile data. Refer to "VNX shared file systems" on page 23 section for more information.

Figure 17 Core Storage Layout



Core Storage Layout Overview

The following core configuration is used in the reference architecture:

- Four SAS disks (0_0_0 to 0_0_3) are used for the VNX OE
- Disks 0_0_6, 0_0_7, and 1_0_2 are hot spares. These disks are marked as hot spare in the storage
- layout diagram.
- Thirty SAS disks (0_0_10 to 0_0_14, 1_0_5 to 1_0_14, and 0_1_0 to 0_1_14) in the RAID 5 storage
- pool 0 are used to store virtual desktops. FAST Cache is enabled for the entire pool.
- For NAS, thirty LUNs of 200 GB each are carved out of the pool to provide the storage required to create fourteen 410 GB NFS file systems and two 50 GB file systems. The file systems are presented to the vSphere servers as NFS datastores.
- For FC, sixteen LUNs of 375 GB each and two LUNs of 50 GB each are carved out of the pool to present to the vSphere servers as eighteen VMFS datastores.
- Four Flash drives (0_0_4 to 0_0_5 and 1_0_0 to 1_0_1) are used for EMC VNX FAST Cache. There are no user-configurable LUNs on these drives.
- Disks 0_0_8 to 0_0_9 and 1_0_3 to 1_0_4 were not used for testing this solution

In solution validation testing, storage space for user data and infrastructure was allocated on the VNX array as shown in the following figure. This storage is in addition to the core storage shown above. If storage for user data exists elsewhere in the production environment, this storage is not required.

EMC Storage Configuration for VMware View

EMC Storage Configuration for VMware ESXi 5.1 Infrastructure Clusters

The steps required to configure LUNs for the VDI Datastores are as follows:

 Create a storage pool using EMC Unisphere; select Storage > Storage Configuration > Storage Pools and click Create.

Hosts 🛛 🖗 Data Protec
2 🖓 🔧 🍺 🤉
Consu Subscrib %Subscr
•Cr

Create a storage pool from LUNs from the pool created in step 1. RAID type, drive number and type are specified in the dialog box. Select 30 x 600GB SAS drives from manual Selection to create RAID 5 Storage pool: Uncheck Schedule Auto-Tiering to disable automatic tiering.

Two LUNs of 2.08TB are carved out of the RAID 5 storage pool configured with 10 SAS drives. The LUNs are used to store infrastructure virtual machines such as VMware Horizon View 5.2 Connection Servers, View Composer servers, and VMware vCenter server.

Example EMC Boot LUN Configuration

Each ESXi server requires a boot LUN from SAN for the hypervisor OS. A total of 43 LUNs are carved out of the 5-disk RAID 5 pool. Each LUN is 5GB in size.

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.

Cisco UCS Manager Configuration for VMware ESXi 5.1

This section addresses creation of the service profiles and VLANs to support the project.

Service Profile Templates

Two types of service profiles were required to support two different blade server types (Table 7).

Table 7 Role/Server/OS Deployment

Role	Blade Server Used	Operating System Deployed
Infrastructure	UCS B250 M2	ESXI 5 1
VDI Hosts	UCS 8 200 M 3	ESXI 5 1

To support those different hardware platforms, service profile templates were created, utilizing various policies created earlier.

The service profile templates were then used to quickly deploy service profiles for each blade server in the Cisco UCS system. When each blade server booted for the first time, the service profile was deployed automatically, providing the perfect configuration for the VMware ESXi 5.1 installation.

VLAN Configuration

In addition, to control network traffic in the infrastructure and assure priority to high value traffic, virtual LANs (VLANs) were created on the Nexus 5548s, on the Cisco UCS Manager (Fabric Interconnects,) and on the Nexus 1000V Virtual Switch Modules in each vCenter Cluster. The virtual machines in the environment used the VLANs depending on their role in the system.

A total of seven Virtual LANs, VLANs, were utilized for the project. Table 8 identifies them and describes their use.

Table 8VLAN Naming and Use

VLANName	VLAN ID Use	
VDA	122	VDI Virtual Machine Traffic
MGMT	164	VM wa re ESXi Management
infra-Mernt	165	Infrastructure Management Traffic (vCenter, SQL, AD, 1000 Vetc)
STRG	166	VNX5500 NFS Traffic (Optional)
N1 K-Control	167	Nexus 1 000V Control Traffic
VMOTION	169	VM ware v Motion Traffic

VLANs are configured using Cisco UCS Manager from the LAN tab; LAN\VLANs node in the left pane of Cisco UCS Manager. They were set up earlier in section 7.2.1 Base Cisco UCS System Configuration.

Installing and Configuring ESXi 5.1

In this study, we used Fibre Channel storage to boot the hosts from LUNs on the VNX5500 storage system. Prior to installing the operating system, storage groups are created, assigning specific boot LUNs to individual hosts. (See section Configuring Boot from SAN on EMC VNX for details.)

VMware ESXi 5.1 can be installed in boot-from-SAN mode using standard hypervisor deployment techniques including:

- Mounting a Cisco Customized ESXi 5.1 ISO image from the KVM of the blade
- Using automated deployment tools from third party sources (Optional)

Install VMware ESXi 5.1

ESXi was installed using the UCS Manager KVM console with the Cisco Customized ESXi 5.1 ISO image mounted. The Cisco UCS Manager boot policy deployed to each blade was set to boot from CD then SAN to accommodate hypervisor installs or updates.

The IP address, hostname, and NTP server were configured using Direct Console ESXi Interface accessed from Cisco UCS Manager KVM console;

http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.install.doc_50%2FGUI D-26F3BC88-DAD8-43E7-9EA0-160054954507.html

http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-command-line-interface-getting-started-guide.pdf.

Install and Configure vCenter

To manage hypervisors and virtual machines a dedicated vCenter server instance was installed on Windows 2008R2 SP1 based virtual machine.

Vmware vCenter	Vmware vCenter Server		
		Service	
OS:	Windows 2008 R2	Pack:	
CPU:	4vCPUs	RAM:	16GB
Disk:	80GB	Network:	1x10Gbps

To support vCenter instance a Microsoft SQL Server 2008 R2 server was created to host vCenter database. Refer to the Microsoft documentation about configuring SQL Server and SQL Server clusters: http://msdn.microsoft.com/en-us/library/ms189134(v=sql.105).aspx and http://msdn.microsoft.com/en-us/library/ms189134(v=sql.105).aspx)

Install and Configure vCenter

- 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: Make sure to use FQDN's for everything.
- Create Active Directory user account and call it vcenter. (This user account will be used to connect to vCenter, you will have to follow a VMware specific procedure and assign specific permissions on vCenter for View components to connect to vCenter. (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&exter nalId=2034833).
- 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&exter nalId=1021514).

Install VMware Licenses

- 1. Connect to vCenter using vSphere client.
- 2. Go to Home > Administration > Licensing.
- 3. Click Manage vSphere Licenses.

Edit	View Inventory Adm	ninistration Plug-ins Help		
	🟫 Home 🕨 🖗 Ad	Iministration 🕨 ஜ Licensing		
Manag	ge vSphere Licenses			
ensing				
-	C Product C License key	C Accet		
icense l			Assigned	Capa
	3-XE09N-28C43 vCer		1 instances	1 insta
		iter berver b btandard		A misco
1 C 2	VCENTER.vdilab		1 instances	
		are vSphere 5 Enterprise Plus	1 instances 12 CPUs	40 (
EOOA				
E004 Ssign L	A7-48K1H-M8J41 VMw icense: VCENTER.vdilab a an existing license key to	-v.local		40 0
Assign L	A7-48K1H-M8J41 VMw icense: VCENTER.vdilab a an existing license key to	-v.local o this vCenter Server		
Assign Prod	27-48K1H-M8341 VMw iccense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key)	-v.local o this vCenter Server Available		
Assign Prod	77-48K1H-M8341 VMw icense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key) Center Server 5 Standa	v.local o this vCenter Server Available 0 instanc		
Assign Prod	27-48K1H-M8341 VMw iccense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key)	v.local o this vCenter Server Available 0 instanc		
Assign Prod	77-48K1H-M8341 VMw icense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key) Center Server 5 Standa	v.local o this vCenter Server Available 0 instanc		
Assign Prod	77-48K1H-M8341 VMw icense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key) Center Server 5 Standa	v.local o this vCenter Server Available 0 instanc		
Assign Prod	77-48K1H-M8341 VMw icense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key) Center Server 5 Standa	v.local o this vCenter Server Available 0 instanc		
Assign Prod	77-48K1H-M8341 VMw icense: VCENTER.vdilab- a an existing license key to uct valuation Mode O (No License Key) Center Server 5 Standa	v.local o this vCenter Server Available 0 instanc		

ESXi 5.1 Cluster Configuration

To accommodate maximum recommendations for View 5.2 on ESXi 5.1 we created four ESXi 5.1 clusters described below. For each of the two VDI clusters using seven Cisco UCS B200 M3 Blade Servers and 1000 virtual machines being hosted.

1

The 14 Cisco UCS B200 M3s and six Cisco UCS B250 M2 ESX hosts were configured into four Clusters:

- Infra-Cluster
- Launcher-CL
- VDI-Desktops-Pool1
- VDI-Desktops-Pool2



Infra-Cluster Infrastructure Cluster

The Infra-Cluster cluster was used to host all of the virtualized servers within the VDA Infrastructure, including two pairs of Nexus 1000V Virtual Switch Manager (VSM) appliances, one for each virtual desktop cluster.

Two physical Cisco UCS B250-M2 hosts were used in this cluster.

One standard switch to manage VMware Management, VDA, vMotion, and Storage traffic were configured on DC-INF cluster hosts. Three pairs of fault tolerant VSMs introduced the N1KV Management, Control and Packet VLANs to the environment.

5tan	dard Switch: vSwitch0		Remove Properties
	Virtual Machine Port Group	Т	Physical Adapters
÷	2 virtual machine(s) VLAN ID: 167 Virtual Machine Port Group vCenter Management		Le 🔛 vmnic3 10000 Full 🖓
+	3 virtual machine(s)		
þ	Virtual Machine Port Group		
+	8 virtual machine(s) VLAN ID: 165		
P	VMkernel Port		
	vmk1 : 10.29.164.42		
P	VMkernel Port Management Network		
	vmk0 : 10.29.164.120		

Virtual Desktop Clusters

The following clusters were used to host 2000 desktops:

VDI-CL1-N1KVVDI-CL2-N1KV

Each of these desktop clusters were configured identically with a Nexus 1000V high availability distributed virtual switch providing the required network connectivity.

The Nexus 1000V switches were configured to manage networking for all three ESX Clusters hosting virtual desktops, working in concert with the Cisco UCS Fabric Interconnects and Nexus 5548UP access layer switches to provide end to end Quality of Service for network communications, insuring the highest quality virtual desktop end user experience.

The Nexus 1000V configuration is described in detail in section Nexus 1000V Configuration in L3 Mode.



Login VSI Launcher Cluster

The separate Launcher-CL cluster was used to host Login Consultants' LoginVSI launcher VMs and a LoginVSI console VM. It was hosted on the same Cisco UCS Domain with dedicated storage.

The Laucher-CL cluster utilized the Standard vSwitch configured as shown below:

Net	working	
Stan	dard Switch: vSwitch0	Remove Properties
Þ	Virtual Machine Port Group	-Physical Adapters
+	25 virtual machine(s) VLAN ID: 165	-
_	VMkernel Port	
P	Management Network	PT
	vmk0 : 10.29.164.121	

Installing and configuring VMware View 5.2

Building out a VMware View 5.2 environment requires the installation of the following components:

- View Connection Server
- View Replica Server
- View Administrator
- View Composer
- View Transfer Server

This section outlines the tasks required to build the View 5.2 environment used in this study. Refer to the VMware View Installation guide for View 5.2 for more details:

I

https://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-installation.pdf.

Pre-requisites

The following is a list of pre-requisites that are required with installing View 5.2 components. They are as follows:

- One of the following operating systems:
 - Windows Server 2008 R2, Standard or Enterprise Edition
 - Windows Server 2008 R2, Standard or Enterprise Edition SP1



You can mix operating systems within a site.

- vCenter 5.0 Update 1 or later
- A supported Microsoft SQL or Oracle database for vCenter and View Composer databases
- A supported vSphere hypervisor host operating system
- Physical or virtual hardware meeting the following recommended requirements
 - For View Connection Server: Pentium IV 2.0 Ghz or higher, 4 CPUs/vCPUs; 10GB+ RAM; 1GB NIC
 - For View Administrator: IE 8 or 9; Firefox 6 or 7; Adobe Flash 10 or later
 - For View Composer: 2.0 GHz or faster, 4 CPUs/vCPUs; 8GB+RAM; 1GB NIC; 60GB+ Disk Space
 - For View Transfer Server: Can co-exist on the same VM with any other View Manager component

Create SQL Databases for View 5.2

View Manager Installer needs a separate database for View Composer Server and View Server events.

Create Database for View Composer Server

- 1. Create a Database for View Composer server and create a user with server authentication.
- 2. On the VM where View Composer will be installed, go to Start' Administrative Tools ' ODBC.
- 3. Create a system DSN using DB server and user with SA authentication.

Create Event Database for View Administrator.

Create a Database for View Administrator Events and user with SA authentication.

Install View Manager and components

Download View Manager software from the link given below.

https://my.vmware.com/web/vmware/details?downloadGroup=VIEW-520-PREMIER&productId=320 &rPId=3908

Install View Connection server

Log into View Connection server with Domain Administrator credentials.

- 1. Open installer file VMware-viewconnectionserver-x86_64-5.2.0-987719.exe with "Run as administrator."
- 2. Click Next.



3. Read the VMware End User License Agreement and click Next.



4. Select the location for the installer to install all the components and click Next.

VMware	View Connection Server				
estination Folder Click Next to install to this folder, or click Change to install to a different folder.					
_	Install VMware View Connecti	on Server to:			
	C:\Program Files\VMware\VM	ware View\Server	۸.	Change	
		< Back	Next >	Cancel	

5. Select Standard server installation.

I

ſ



6. Enter a password and click Next.

🛃 ¥Mware ¥iew Connection Server	×				
Data Recovery Enter data recovery password details.					
This password protects data backups of yo require entry of this password.	our View Connection Server, Recovering a backup will				
Enter data recovery password:	•••••				
Re-enter password:	•••••				
Enter password reminder (optional):	default				
	< Back Next > Cancel				

7. Select the radio button Configure Windows Firewall automatically. Click Next.

VMware View Connection Server	
Firewall Configuration Automatically configure the Windows F connections.	irewall to allow incoming TCP protocol
must be allowed through the local Win the Standard Server are 8009 (AJP13	
C Do not configure Windows	
	< Back Next > Cancel

8. Select the radio button Authorize a specific domain user or domain group. Click Next.

1

VMware View Connection Server
Initial View Administrators Specify the domain user or group for initial View administration.
To login to View Administrator, you will need to be authorized. Select the local Administrators group option or enter the name of a domain user or group that will be initially allowed to login and will be granted full admistrative rights.
The list of authorized administrator users and groups can be changed later in View Administrator.
 Authorize the local Administrators group Authorize a specific domain user or domain group
VDI-VSPEX\administrator
(domainname\username, domainname\groupname or UPN format)
< Back Next > Cancel

- 9. Uncheck the box Participate anonymously in the user experience improvement program. Click Next.
- **10.** Click Install.

User Experience Improvement Prog	am		
Basic Customer Demographics			
VMware is constantly trying to improve the help us in this effort by agreeing to send pu completely anonymous, and is restricted to about it visit the VMware user experience in button.	roduct usage : product usag	statistics. This data is e metrics. For more de	etails
Participate anonymously in the user	experience im	provement program	
Select your organization industry type:			7
Select location of your organization's head	quarter:		

11. Double-click the View Administrator icon on the desktop; ignore the security warning on IE.



You need to install Flash player plugin v10.3 or higher to use Web Browser for Login to View Administrator.

12. Log into View Administrator GUI by entering username, password and Domain name.

vm ware [.]		
User name:	viewadmin	VMware Horizon View Administrator
Password:	******	
Domain:	VDILAB-V	
	🗹 Remember user name	
	Login	

Install View Replica Server

ſ

- 1. Log into the replica server with domain administrator credentials
- 2. Open the installer file VMware-viewconnectionserver-x86_64-5.2.0-987719.exe with "Run as administrator."
- 3. Click Next.



4. Read the VMware End User License Agreement and click Next.



5. Select a destination for installation. Click Next.



6. Select Replica server installation. Click Next.

Installation Options		
-	tion Server instance you want to install.	
Select the type of View Connec	tion Server instance you want to install.	
View Standard Server View Replica Server View Security Server View Transfer Server	Perform a replica instance install joining an instance. This is used to install a second or server in a group of servers that all autom same directory configuration.	subsequent
		_
	< Back Next >	Cancel

7. Select IP Address/Host name for view connection server primary instance to connect with replica server. (FQDN is recommended)

🖥 ¥Mware '	View Connection Server
Source Se Select ar	erver n existing View Connection Server instance from which to replicate.
	View Connection Server instances that share the same configuration data is called a action Server group. Setup will replicate configuration data from an existing server
Enter the s of that gro	erver name of an existing View Connection Server instance to make this server part up.
Example se	erver: view.internal.vmware.com.
<u>S</u> erver:	view-cs01.vdi-vspex.com (hostname or IP address)
	< Back Next > Cancel

8. Click Next.

I

Γ

9. Click Next.

🛃 VMware View Connection Server		×
Ready to Install the Program The wizard is ready to begin installation		6
VMware View Connection Server will be C:\Program Files\VMware\VMware View	v\Server\	
Click Install to begin the installation or C	Cancel to exit the wizard.	
	< Back Install	Cancel

Install View Composer Server

View Composer server can be install on a separate stand alone server or on the same server that was used for vCenter server installer. For our test, we installed View Composer server on the same server we used for vCenter server.

1

- 1. Open View composer installer VMware-viewcomposer- 5.2.0-983460.
- **2.** Create a database and ODBC connection for view composer installation. See section 7.8.2.1 for how to create database for view composer server.
- 3. Click Next.



4. Read the VMware End User License and click Next.



5. Select a location for the View Composer installation. Click Next.



I

6. Enter the newly created Database and SA user Information for the View Composer installation.Click Next.



7. Accept the default port settings and click Next.



8. Click Install.

🖶 ¥Mware ¥iew Composer			×
Ready to Install the Program The wizard is ready to begin installation			6
VMware View Composer will be installed	in:		
C:\Program Files (x86)\VMware\VMwar	e View Compose	n	
If you want to review or change any of begin the installation or Cancel to exit th	your installation he wizard.	settings, click Back.	Click Install to
InstallShield	< Back	Install	Cancel

View Administrator Configuration

ſ

To configure the View 5.2 system, follow these steps:

- 1. Log into Vmware View Administrator using web browser.
- 2. Select View configuration.
- 3. From the drop-down menu select Product Licensing and Usage.
- 4. Click Edit settings and enter a valid License key for View Manager.

Updated 8/2/2013 11:56 AM 🥭	Licensing and Usage			
Remote Sessions 0				
Local Sessions 0	Licensing			
Problem Desktops 0				
Events 0 A 0 System Health	Edit License			
77 0 0 0				
// 0 0 0	License expiration: Sa	aturday, January 18, 2014 12:0	0:00 AM PST	
Inventory	View Composer license: Er	nabled		
S Dashboard	Local Mode license: Er	nabled		
S Users and Groups	Edit License			
V Inventory				
Pools	License serial number: •			
Desktops				
Persistent Disks			Cancel	
P ThinApps			Cancer	2
▶ Monitoring	Session Mode	Current		Web - at
► Policies				Highest
▼ View Configuration	Total Remote	0	0	
Servers	Active - full virtual machines	0	0	
Product Licensing and Usage	Active - linked clone	0	0	
Global Settings	Active - other desktop source:	s 0	0	
Registered Desktop Sources	Local	0	0	
Administrators				
ThinApp Configuration				

5. In View Configuration Click on servers. Select vCenter Servers tab. Click Add.

pdated 12/7/2012 3:42 PM 🖉	Servers	
Remote Sessions 0 Local Sessions 0	vCenter Servers Security Servers Connection Servers Transfer Servers	
Problem Desktops 0 Events	Add Edt Remove Disable Provisioning Enable Provisioning	8.4
System Health	vCenter Server	Provisioning
Deshboard Supers and Groups Inventory Monitoring Policies View Configuration Servers		
Servers Product Licensing and Usage Global Settings Registered Desktop Sources Administrators ThinApp Configuration Event Configuration Event Configuration		

6. Enter FQDN for vCenter server and username/password. Make the necessary changes for Advanced settings. Click Next.

For this test case we used the following parameters.

Max concurrent vCenter Provisioning operations: 20

Max concurrent Power operations: 10

Max concurrent View Composer maintenance operations: 50

Max concurrent View Composer provisioning operations: 50



7. Click View Certificate and accept certificate warning.


8. Select View Composer settings. Select the radio button for View Composer Server; either coinstalled with Vcenter or Standalone View Composer Server.



I

For the study, the View Composer Server was installed as a Standalone.



9. Click View Certificate and accept the certificate.



10. Click Add to add view composer domain.

Full domain name:	vdi-vspex.com
User name:	administrator
Password:	ander samer samer samer samer samer

1

11. Click Next.



12. Select the check box to enable host caching. Set Default host cache siz. Click Next.



For this test case we used 2048MB cache size.

Servers	
vCenter Servers Security Serve	ers Connection Servers Transfer S
Add Edit Remove Dis	able Provisioning
vcenter.vdilab-v.local(administrator	-)
Edit vCenter Server	
vCenter Server Storage	
Storage Settings	
Reclaim VM disk space	
Enable View Storage Accelerator	
Default host cache size: 2048	MB
Cache must be between 100 MB a	and 2048 MB
Hosts	
Show all hosts	
Edit cache size	
Host	Cache Size
/VDI-2000/host/Infra-Cluster/10.29	: Default
/VDI-2000/host/Infra-Cluster/10.29	: Default #
/VDI-2000/host/Launcher-CL/10.29.	1 Default
/VDI-2000/host/Launcher-CL/10.29.	1 Default
/VDI-2000/host/Launcher-CL/10.29.	1 Default
, vor-2000, nosc, cautioner-cc, ro.29.	1 Defeut
/VDI-2000/host/Launcher-CL/10.29.	1 Default

- **13.** Create a new database for View Event Database in SQL server.
- 14. Click Event Database configuration.

ſ

15. Enter Database server information, database name, username/password. For the table prefix add VE_

VMware Horizon View A	Administrator	
Updated 0/2/2013 11/56 AM Remote Sessions Local Sessions Problem Desktops Events System Health 77 0 0 0	Event Configuration Event Database Clear Edit Database server typ Database server:	pe: Microsoft SQL Server mssql-db
Inventory	Port:	1433
← Dashboard	Database name: User name: Table prefix:	ViewEventDB5.2 sa VE_
B Desktops		
Persistent Disks ThinApps	Edit Event Database	
► Monitoring	Database server:	mssql-db
► Policies ▼ View Configuration	Database type:	Microsoft SQL Server -
Servers Product Licensing and Usage	Port:	1433
Global Settings	Database name:	ViewEventDB5.2
Registered Desktop Sources Administrators	User name:	sa
ThinApp Configuration Event Configuration	Password:	
	Confirm password:	Sec les sec les sec les
	Table prefix:	VE_
		OK Cancel

16. After completion of the View configuration go to Dashboard for View Administrator and check System Health and verify all components are shown as green.

Updated 8/2/2013 12:16 PM	Dashboard	
Remote Sessions 0 Local Sessions 0 Problem Desktops 0		
Events 0 0 A 0	System Health	Desktop Status
System Health 77 0 0 0	▼ View components	Desktops
// 0 0 0	Connection Servers	▶ 🔛 Preparing
Inventory	Event database	Problem Desktops
A Dashboard	▶ View Composer Servers	
Users and Groups	▼ vSphere components	Prepared for use
/ Inventory	▶ Datastores	
Pools	ESX hosts	
Desktops	▶ ■ vCenter Servers	
Persistent Disks	Tother components	
📌 ThinApps	> Domains	
 Monitoring 		
▶ Policies		
View Configuration		

Install SSL Certificate for View Connection and Replica Server

1. Log into AD server and Add role for Active Directory Certifiacate services if does not exist.

1

2. Go to start Menu > Run > mmc.



3. Click File and select Add/Remove Snap-in.

Console1 - [Console Root]			_ 🗆 🤉
File Action View Favorites		þ	
Dpen	Ctrl+N Ctrl+O		
Save	Ctrl+S		Actions
Save As		There are no items to show in this view.	Console Root
Add/Remove Snap-in Options	Ctrl+M		More Actions
1 C:\Windows\system32\dsa			
2 C:\Windows\\ServerManager 3 C:\Windows\system32\dhcpmg			
	nic		
Exit			
	J		J
hanges the options for the user and/or	the snap-in cor	sole.	

4. Select Certificates and click Add.

Remove
Remove
Move Up
Move Down
Advanced

5. Select the radio button for Computer account.

I

Γ

Certificates snap-in			×
This snap-in will always manage certificates for:			
My user account			
C Service account			
C Computer account			
	< Back	Finish	Cancel

6. Select the radio button for Local Computer. Click Finish.

Local computer: (the computer this console is running on) Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	elect the computer you wan This snap-in will always mar	
Allow the selected computer to be changed when launching from the command line. This	Local computer: (the c	omputer this console is running on)
	C Another computer:	Browse
		< Back Finish Can

7. Add Certificate Templates and Certification Authority. Click OK.

		_	Selected snap-ins:	
ap-in	Vendor	1	Console Root	Edit Extensions
	Microsoft Cor		Certificates (Local Computer)	Remove
			Certification Authority (Local)	nemove
Active Directory Use			Certificate Templates	
	Microsoft Cor			Move Up
	Microsoft Cor			Have David
, and a second	Microsoft Cor	Add >		Move Down
	Microsoft Cor	- MOU >		
	Microsoft Cor			
a a constant of the standard	Microsoft Cor			
DHCP	Microsoft Cor	-1		Advanced
Disk Management	Microsoft and	<u> </u>		Havancoann

8. Click Certificate Template and from the list of template displayed on the right side select Web Server.

1

9. Right -click Web Server; select properties.

File Action View Favorites					_10
Certificate Templates (AD-ONS)	Template Display Name * Template Agent Agent Template Agent Agent Template Agent Agent Template Agent Agent Template Agent Template Agent Template Display Name Agent Template Agent Te	Minimum Supported CAs Windows 2000 Windows 5000 Windows 2000 Windows 2000 <th>4.1 110.0 6.1 4.1 5.1 7.1 8.1 7.1 100.0 105.0 105.0 101.0 5.1 3.1 3.1 4.1 4.1</th> <th>Intended Purpor Clerk Authentic Clerk Authentic Key Recovery A OCSP Signing Clerk Authentic</th> <th>Actions Certificate Templates (AD More Actions Web Server More Actions</th>	4.1 110.0 6.1 4.1 5.1 7.1 8.1 7.1 100.0 105.0 105.0 101.0 5.1 3.1 3.1 4.1 4.1	Intended Purpor Clerk Authentic Clerk Authentic Key Recovery A OCSP Signing Clerk Authentic	Actions Certificate Templates (AD More Actions Web Server More Actions

10. Select for the Security tab and add the computer name to assign for connection server, replica server. Allow full control to both servers.

eb Server Properties		?
General Request Handling Subject	Name Extensions	Security
Group or user names:		
Authenticated Users		
VIEW-CS01 (VDI-VSPEX/VIEW-		
VIEW-CS02 (VDI-VSPEX/VIEW- & Domain Admins (VDI-VSPEX/Do		
& Enterprise Admins (VDI-VSPEX\	,	
	Add	Remove
		·
Permissions for VIEW-CS02	Allow	Deny
Full Control		
Read	\checkmark	
Write	\checkmark	
Enroll	\checkmark	
		I
For special permissions or advanced s	ettinas, click	Advanced
Advanced.	_	Advanced
Learn about access control and permi	iesione	
	10010110	
OK Cano	el Apply	Help

- **11**. Select Certificates on the Console Root > Personal > Right-click Certificates.
- **12**. Select Request New Certificate on All Tasks.

I

🕨 🔿 📩 📅 📋 🙆 😼 📘	Issued To A	Issued By	Expiration Date	Intended	Actions	
Certificates (Local Computer) Personal	Wew-CS01.vdi-vspex.com	n View-CS01.vdi-vspex.com	12/5/2022	Server A	Certificates	
	Import	Operations			More Actions	,
Contrusted C New Taskpace Third-Party F	d View					
Trusted Peor Refresh Export List						
Smart Card * Help Trusted Development						

1

13. Click Next.

🜏 Cert	iificate Enrollment
📮 Cer	tificate Enrollment
E	Before You Begin
	The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
E	Before requesting a certificate, verify the following:
	Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate
L	Learn more about <u>digital certificates</u>
	Next Cancel

- 14. Check the box for Web Server. Click Details.
- **15.** Click Properties.

equest Certificates		
ou can request the following t	ypes of certificates. Select the certificates you want to request	, and then click Enroll
Active Directory Line	Junient Folicy	
Computer	(1) STATUS: Available	Details 🛞
Web Server	💓 STATUS: Available	Details ®
🔥 More information i	s required to enroll for this certificate. Click here to configure se	ttings.
Key usage:	cribe the uses and validity period that apply to this type of certi Digital signature Key encipherment Server Authentication	ficate:
Validity period (days)		
		Properties
Validicy period (days)	730	Properties

- **16.** On the left side from the drop menu for Subject Type select Common Name, Organization, Country, Locale and add them with their appropriate value as shown in the screenshot below.
- **17.** Alternative name: from the drop menu for type select DNS and add DNS name for view connection server. Do the same for view Replica server.
- **18.** Click Apply.

rtificate Properties	
Subject General Extensions Private K	ey Certification Authority
The subject of a certificate is the user or compo enter information about the types of subject n in a certificate. Subject of certificate The user or computer that is receiving the certi	ame and alternative name values that can be used
Subject name:	CN=viewcs2.foita.com
Type:	CN-public.url.com
	dd > C=CZ L=Prague
Value:	O=fojta.com
Iternative name:	
Type:	viewcs2.fotta.com
DNS V	public.url.com
Value:	
A	dd >
< F	emove
5 C	
earn more about subject name	
	OK Cancel Apply

19. Click Apply > Click OK.

Γ



20. Export certificate created for view connection server and Replica server. Copy them to their corresponding server.

1

- **21**. Go to View connection server/Replica server. Start Menu > Run > mmc.
- 22. Click File and Select Add/remove Snap-in.

🙀 Console1 - [Console Root]		
File Action View Favorites	Ctrl+N	<u>_8×</u>
Open Save Save As	Ctrl+O Ctrl+S There are no items to show in this view.	Actions Console Root
Add/Remove Snap-in Options 1 C:\Windows\system32\dsa 2 C:\Windows\\ServerManager	Cbi+M	More Actions
3 C:\Windows\system32\dhcpmgm Exit		
Changes the options for the user and/or t	te snap-in console.	1

23. Select Certificate from the Available snap-ins on the left side and click Add.

ilable snap-ins: iap-in	Vendor			Selected snap-ins:		Edit Extensions
Active Directory Site		-		Certificates (Lo	cal Computer)	Edit Extensions
ActiveX Control	Microsoft Cor				car compacery	Remove
ADSI Edit	Microsoft Cor					
Authorization Manager						Maria Un
Certificates	Microsoft Cor					Move Up
Component Services	Microsoft Cor					Move Down
Computer Managem			Add >			
Device Manager	Microsoft Cor					
Disk Management	Microsoft and					
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
	Microsoft Cor					
IP Security Policy Ma		-				Advanced
cription:						

24. Select the radio button for Computer account.

I

Γ

Certificates snap-in			X
This snap-in will always manage certificates for:			
My user account			
Service account			
Computer account			
	< Back	Next >	Cancel

25. Select the radio button for Local computer. Click Finish.

The second in 1990 all second as	ant this snap-in to manage.
his snap-in will always m	-
 Local computer: [the 	e computer this console is running on)
C Another computer:	Browse

26. Select Certificates on the Console Root; Select Personal > Certificates > All Tasks > Import.

1

	Issued To	A	Issued By	Expiration Date	Intended	Actions	
Certificates (Loc	sl Computer)	01.vdi-vspex.com	View-C501.vdi-vspex.com	12/5/2022	Server A	Certificates	
Personal Certifica						More Actions	
Trusted Roo		Request New Certificat	e			Plate Hours	
Enterprise T		Import					
🚞 Intermediate	New Window from Here	Advanced Operations					
🗉 📄 Trusted Pub							
Contrusted C Definition Third-Party	New Taskpad View						
Third-Party I Trusted Peo	Refresh						
E Remote Des							
🗉 🧮 Smart Card	Help						
🗉 🧮 Trusted Dev	1000						

- **27.** Browse and select copied certificate for view connection server and follow the same for view Replica server.
- **28.** Select the previous installed certificate and change the friendly name. Replace the newly created certificate with vdm as the friendly name.

🚪 Console1 - [Console Root\Certificates (Local C	omputer)/Personal (Certificates]							_0	IX
🚡 File Action Vew Favorites Window Help								_16	5 X
🏟 🖄 🖬 🖬 🖉 🖬 👘									
📔 Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
🖂 🕎 Certificates (Local Computer)	vilab-v-40-001-CA	vdilab-v-AD-DC1-CA	10/9/2017	ab	dime>			Certificates	
🖂 🛄 Personal	Wew-Sn/01.vdlab-v.local	vdiab-v-AD-DC1-CA	1/16/2015	Server Authentication	vdn		Web		-
Certificates	Wew-Sn01.vdlab-v.local	View-Sn/01.vdilab-v.local	1/14/2023	Server Authentication	vdm-old			More Actions	•
Inusted Root Certification Authorities	1.								
🕑 🦳 Enterprise Trust									

For more information about VMare's best practices to obtain the self-signed certificate, go to: http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-obtaining-certificat es.pdf

Install View Client on End Points

1. Download the installer file from the link given below:

https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_horizon_view/5 _2?rct=j&q=cmware%20view%205.2%20horizon%20download&source=web&cd=1&ved=0CEIQFjA A&url=http://www.vmware.com/go/downloadview

2. Open the installer file for 32-bit or 64-bit OS and click Next.



3. Read the VMWare EndUser Lincednse Agreement and click Next.

母 VMware View Client	×
License Agreement Please read the following license agreement carefully.	P
VMWARE END USER LICENSE AGREEMENT	•
IMPORTANT-READ CAREFULLY: BY DOWNLOADING,	
INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDU. OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF	
END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT	ins
AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT	
DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MU	
DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDO	
I accept the terms in the license agreement	
I do not accept the terms in the license agreement	
< Back Next > C	ancel
< Back Next > C	ancel

4. Click Next.

ſ

Custom Setup Select the program features you want installed.	R
lick on an icon in the list below to change how a fe	
View Client USB Redirection Log in as current user	Feature Description VMware View Client
	This feature requires 38MB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 13MB on your hard drive.

1

5. Enter FQDN for View Connection server ad click Next.

VMware View Client				×
Default Server Configures the server View Client co	onnects to by defa	oult.		6
Specify a default server for this View	/ Client. This setti	ing is optiona	ıl.	
Default View Connection Server:	l			
	< Bac	ck	Next >	Cancel

6. Accept the default or add the fqdn of your View Connection Server and click Next.

nhanced Single Sign On		
Sign on as currently logged on user.		
Set default behavior for the "Log in as o	current user" checkbox:	
Show in connection dialog		
Set default option to login as curr	ent user	

7. Click Next.

L

Γ

Configure Shortcuts		
Creates program shortcuts.		2
Create shortcuts for VMware View	V Client in the following places:	
✓ Desktop		
🔽 Start Menu Programs folde	er	
	< Back Next >	Cancel

8. Click Install.

eady to Install the Program		
The wizard is ready to begin installation.		7
VMware View Client will be installed in:		
C:\Program Files\VMware\VMware Vi	ew\Client\	
Click Install to begin the installation or C	ancel to exit the wizard.	

9. Reboot is required after completing the installation.

Configure the View 5.2 Hosts and Storage

Configure Content Based Read Cache (CBRC) on View 5.2 Hosts

CBRC was introduced as a feature of vSphere 5. It is a read cache that is particularly useful during boot storms. It becomes an essential configuration for floating assignment View 5.2 Linked Clones.

The CBRC feature provides a per-host RAM-based solution for View desktops. This considerably reduces the read I/O requests that are issued to the storage layer, and also addresses boot storm snags.

CBRC is configured in vCenter by highlighting the host; access the Configuration Tab, Software, and Advanced Settings.

Each ESXi host used for View Desktops we enabled CBRC and increased the CBRC.DCacheMemReserved to 2048.

 Annotations BufferCache CBRC Config 	CBRC.DCacheMemReserved Memory consumed by CBRC Data Cache (in MB)	204
- Vpx	Min 100 Ma 2048	
- COW - Cpu	CBRC.DCacheSize	204
 DataMover DCUI Digest DirentryCache 	Size of CBRC Data Cache in MB. This cannot be changed if CBRC.Enablement Min 2048 Ma 2048	ble is set to 1.
– Disk – FSS	CBRC.DigestJournalBootInterval	1
– FT – HBR – Irq	Interval (in minutes) for which Digest Journal is temporarily disabled Min 0 Ma 10000	to avoid interfering with the boot pro
– LPage – LSOM – Mem – Migrate	CBRC.Enable Enable Content Based Read Cache	V

These CBRC settings are used in conjunction with the View 5.2 Administrator, View Configuration, Servers, vCenter Server Properties, Host Cashing tab.

In our test environment, we enabled 2GB of CBRD and correspondingly, 2GB of Host Cache in View Administrator. This combination enables the View Storage Accelerator feature.

I

Storage Configuration for View 5.2 Hosts

On VNX 5500 30 SAS disks with 300 GB capacity were used to create 16 LUNs, each with a capacity of 370 GB. 2 LUNs with capacities of 50 GB each were created to store replica disks.

Each ESXi host in each cluster was assigned 8 LUNs as VMFS5 datastores for linked clones and one 50Gb VMFS5 datastore to hold the Replica disk.

(R) Infra-Cluster (R) Launcher-CL	Hardware	View: Datastores De	evices					
WDI-Desktops-Pool1	Processors	Datastores						
10.29.164.91 10.29.164.92	Memory	Identification /	Status	Device	Drive Type	Capacity	Free	Туре
10.29.164.93 10.29.164.94 10.29.164.95 10.29.164.95 10.29.164.95 10.29.164.97 Characteristics 10.29.164.97 Characteristics 10.29.164.97 Characteristics 10.29.164.97 Characteristics 10.29.164.93 10.29.164.93 10.29.164.93 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.94 10.29.164.95 10.2	Storage	datastore1 (3)	 Normal 	DGC Fibre Ch	Non-SSD	10.00 G	7.78 GB	VMFS
	Networking	InfraStore	Normal	DGC Fibre Ch	Non-SSD	2.00 TB	1.25 TB	VMFS
	Storage Adapters	VDI-LC-LUN1	 Normal 	DGC Fibre Ch	Non-SSD	349.75 G	247.88 G	VMPS
	Network Adapters	VDI-LC-LUN2	Normal	DGC Fibre Ch	Non-SSD	349.75 G	258.41 G	VMPS
	Advanced Settings	VDI-LC-LUN3	 Normal 	DGC Fibre Ch	Non-SSD	349.75 G	260.97 G	VMFS
	Power Management	VDI-LC-LUN4	 Normal 	DGC Fibre Ch	Non-SSD	349.75 G	261.66 G	VMP
VDI-CL1-100	Torrer Hundgement	VDI-LC-LUN5	Normal	DGC Fibre Ch	Non-SSD	349.75 G	261.85 G	VMFS
VDI-CL1-1000 VDI-CL1-1001	Software	VDI-LC-LUN6	 Normal 	DGC Fibre Ch	Non-SSD	349.75 G	259.61 G	VMPS
VDI-CL1-1001 VDI-CL1-101 VDI-CL1-101 VDI-CL1-103 VDI-CL1-103 VDI-CL1-104 VDI-CL1-105 VDI-CL1-106	Licensed Features	VDI-LC-LUN7	Normal	DGC Fibre Ch	Non-SSD	349.75 G	261.31 G	VMFS
	Time Configuration	VDI-LC-LUN8	 Normal 	DGC Fibre Ch			260.78 G	
	DNS and Routing	VDI-Replica-CL1	 Normal 	DGC Fibre Ch	Non-SSD	49.75 G	28.46 G	VMPS
	Authentication Services							

Note

The same configuration was done for second Cluster.

Infra-Cluster Launcher-CL Hardware	View: Datastores De	evices					
DI-Desktops-Pool1 Processors DI-Desktops-Pool2	Datastores						
164.100 Memory	Identification	Status	Device	Drive Type	Capacity	Free	Туре
101 · Storage	datastore1 (17)	Normal	DGC Fibre Ch	Non-SSD	10.00 G	7.93 GB	VMFSS
1.102 Networking	InfraStore	Normal	DGC Fibre Ch	Non-SSD	2.00 TB	1.25 TB	VMFSS
4.103 4.104 Storage Adapters	VDI-LC-LUN10	Normal	DGC Fibre Ch	Non-SSD	349.75 G	266.60 G	VMFSS
98 Network Adapters	VDI-LC-LUN11	Normal	DGC Fibre Ch	Non-SSD	349.75 G	261.87 G	VMPS5
4.99	VDI-LC-LUN12	Normal	DGC Fibre Ch	Non-SSD	349.75 G	262.83 G	VMFS5
2785185-833 Advanced Settings 1 Power Management	VDI-LC-LUN13	Normal	DGC Fibre Ch	Non-SSD	349.75 G	263.67 G	VMFS5
10 Power Hanagement	VDI-LC-LUN14	Normal	DGC Fibre Ch	Non-SSD	349.75 G	263.40 G	VMFS5
00 Software	VDI-LC-LUN15	Normal	DGC Fibre Ch	Non-SSD	349.75 G	263.57 G	VMFS5
1000 Licensed Features	VDI-LC-LUN16	Normal	DGC Fibre Ch	Non-SSD	349.75 G	262.03 G	VMFS5
2-102 Time Configuration	VDI-LC-LUN9	Normal	DGC Fibre Ch	Non-SSD	349.75 G	250.26 G	VMFSS
12-103	VDI-Replica-Pool2	Normal	DGC Fibre Ch	Non-SSD	49.75 G	38.63 G	VMFSS

Desktop Delivery Base Image Creation and Desktop Deployment

Microsoft Windows 7 Golden Image Creation

Create base Windows SP1 Virtual Machine

1. Select ESXi host in Infrastructure cluster and create a virtual machine to use as Golden Image with windows 7 OS. MS Windows 7 32 bit OS was used for testing.

For the virtual machine following parameters were used:

Memory: 1536Mb

Processor: 1vCPU

Hard Disk: 18Gb

Network Adapter: 1 attached to VDI port-group on Nexus 1000v

2. Right-click Windows 7 Golden Image properties and select Hardware TAB to attach the Windows -7 SP 1 ISO.

	DI - Virtual Machine Properties	;
Hardware Options Resources	Add Remove	Virtual Machine Version: 8
Hardware	Summary	Connect at power on
Meronavie Memory OUs Vdeo card VdCI device SSCI controller 0 Hard disk 1 CD/DVD drive 1 (edi Network adapter 1 (Junnary 1536 MB 1 Video card Restricted LST Logic SAS Virtual Dak Virtual Dak Virtual Vak Virtual Vak Virtual Vak	Device Type Crome Theore Note: To connect this device, you must power on the visual machine and then dick the Connect CD/DVD button in the Hord Device T Detactive ISO: File Browse
Browse Datastores		X
W7sp1-GI-v500 Win-7-Golden-1 SQLFULL_ENU. (2) en_windows_7	d9-2ead-4132-9516-6db0e69d4d1) Image5 Iso _professional_with_sp1_x86_dvd_c	
 en_windows_se view5.1.iso adobeflash.iso 	erver_2008_r2_standard_enterprise	_datacenter3 GB 9/13/; 792 MB 7/19/; 2 MB 7/19/; ↓
.		
File type:	ISO Image (*.iso)	Салсе!

- 3. Click OK.
- 4. Right-click Windows 7 Golden Image Properties and click Edit Setting. Click the Options tab
 - **a**. Go to the Options tab.
 - b. Select Boot Options and check box for Force BIOS Setup
 - c. Click OK and complete installation.
- 5. After the installation, log in to Windows 7 Golden Image virtual machine and configure IP Address, join the domain and Restart the Virtual Machine.
- 6. Install Windows Upates, then disable the Windows Update service on the Golden Image machine.

This complete the process of creating the Golden Image virtual machine.

Optimization of Base Windows 7 SP1 Virtual Machine

1. Click the link below for instructions about how to optimize MS Windows 7 SP1 32 bit virtual machine.

www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

Install View 5.2 Virtual Desktop Agent Software

1. Download software from the following link:

https://my.vmware.com/web/vmware/details?downloadGroup=VIEW-520-PREMIER&productId= 320&rPId=4175

I

- Open the installer VMware-viewagent-5.2.0-987719.exe for 32bit OS or VMware-viewagent-x86_64-5.2.0-987719.exe 64bit OS.
- 3. Click Next.



4. Read the VMware End User License Agreement, click I accept and click Next.

License Agreement Please read the following license agree	ement carefully.		
VMWARE END US	ER LICENSE	AGREEMENT	r =
IMPORTANT-READ CAREF			VG,
INSTALLING, OR USING THE			
INDIVIDUAL OR LEGAL ENT			
TERMS OF THIS END USER L			
YOU DO NOT AGREE TO TH			
NOT DOWNLOAD, INSTALL,			
MUST DELETE OR RETURN		SOFTWARE I	UTHE _
I accept the terms in the license agree	ement		
C I do not accept the terms in the licens	e agreement		

5. Click Next to accept the default setup.

Γ

select the program	features you want i	ostalled		
	list below to change		installed	
	Agent USB Redirection View Composer Ag Virtual Printing PCoIP Server X PCoIP Sma PCoIP Sma View Persona Man	rtcard This udio The	ature Description — ware View Agent feature requires 1 ie. It has 5 of 5 subf subfeatures require d drive.	features selected.
stall to: \Program Files\VMw	are\VMware View\A	gent\		Change

1

6. Click Install.

VMware View Agent			
Ready to Install the Program			
The wizard is ready to begin installat	ion.		
VMware View Agent will be installed i	n:		
C:\Program Files\VMware\VMware	View\Agent\		
Click Install to begin the installation of	or Cancel to exit the v	vizard.	
			10
	< Back	Instal	Cancel

Install Additional Software

- **1.** Install additional software required for your base windows image. We installed the following software:
- MS Office 2010 was installed for test environment.
- The VSI Target software package was installed to facilitate workload testing. (Optional)
- **2**. Reboot the virtual machine.
- **3.** Install the service packs and hot fixes required for the additional software components that were added.
- 4. Shut down the virtual machine.

Perform Additional View 5.2 Configuration

Create a Snapshot for the Virtual Machine

- 1. Shut down the MS Windows 7 Golden Image virtual machine to take a snapshot.
- **2.** Right-click Windows 7 Golden Image Virtual Machine, click Snapshot, then Take Snapshot to take a snapshot. This snapshot is required for the virtual desktop deployment.
- 3. Provide the name and description for the snapshot and click OK.
- 4. Click OK.

Name			
Win-7-Golden-I	mage-SnapShot for	VDI-Deployment	
Description			
Min-7-Coldon-1			
			ment
win-z-Golden-	mage-SnapSnot fo	r VDI-View-Deploy	ment
wiii-z-Golden-	mage-SnapSnot fo	r VDI-View-Depioyi	ment
			ment
Snapshot the v	rirtual machine's me	emory	
Snapshot the v		emory	

Create Customization Specification for Virtual Desktops

- 1. From vCenter, Right-click the powered off virtual machine after taking a snapshot and select Convert to Template.
- 2. Provide a name for the template and provide the host /cluster, data store details.
- 3. Convert the template back to a virtual machine or deploy a virtual machine from the template.
- 4. Provide a name and select the data center, click Next.
- 5. Select the cluster for the virtual machine.
- 6. Select the virtual machine host.
- 7. Select the datastore.
- **8**. Select Guest Customization and check the radio button for Customize using the Customization Wizard.
- 9. Click Next.

🔗 Deploy Template				_ 🗆 X
Guest Customizati Select the custo	on mizaton option for the guest operating system			
Hame and Locaton biost. Cluster Strate B Guese Sectors Ready to Complete	 Power on this virtual machine after Select the option to use in customizing the guest operating system of the Do not customize Customize using the Customization Wizard Customize using an existing customization 			
Help		< Back	Next >	Cancel

1

10. Select the appropriate name and organization. Click Next.

🔗 vSphere Client Windows Guest C	Customization			×
Registration Information Specify registration information	on for this copy of the gu	uest operating system.		
Registration Information Computer Name Windows License Administrator Password Time Zone	Type in the owner	er's name and organization.		
Run Once Network Workgroup or Domain Operating System Options Save Specification Ready to Complete	Organization:	vdiab-vspex.local		
Нер			< Back N	ext > Cancel

11. Select the radio button for Use the virtual machine name. Click Next.

Redistration Information Computer Name Minimovis License Administrator Password Time Zone Run Once Network Workgroup or Domain Operating System Option Save Specification Ready to Complete	NetBIOS Name Priter a name The name cannot exceed 15 characters. F Append a numeric value to ensure uniqueness The name will be truncated if combined with the numeric Use the virtual machine name If the name exceed 15 characters, it will be truncated. C Enter a name in the Deploy wizard C Generate a name using the custom application configured with	
	Argument:	

12. Specify the Volume License Key for Windows 7 and select Per seat or Per server Maximum. Click Next.

Registration Information	Enter the Windows lice	nsing information. If th	nis virtual machine de	oes not require licensing	information, leave thes	e fields
Computer Name Windows License Administrator Password	blank. Product Key:					
Time Zone Run Once	✓ Include Server Licer	nse Information (Requ	ired for customizing	a server quest OS)		
Vetwork Workgroup or Domain Dperating System Option Save Specification Ready to Complete	Server License	C Per seat C Per server Maximum	5			

13. Enter the credential for the administrator account. Click Next.

Γ

💋 vSphere Client Windows	Cont Contaction	-11		×
Administrator Passwor	rd	option for the Administrator account.		_
Redistration Information Computer Name Variations License Malministrator Passwor Take Zone Network Workgroup or Doman Operating System Option Save Specification Ready to Complete	Password: Confirm	sword for the Administrator account.		
Help			< Back Next >	Cancel

1

14. Select the appropriate time zone, Click Next.

💋 vSphere Client Window	s Guest C	ustomization			×
Time Zone Select a time zone f	or this virt	ual machine.			
Resistration Information Computer Name Windows License Administrator Password The Zone Network Workgroup or Domain Operating System Option Save Specification Ready to Complete	Time	(GMT-0800) Tijuana, Los Angeles, Seattle, Vancouver			<u>_</u>
Heip			<u>≤</u> Back	Next ≥	Cancel

15. For Network, select Typical Setting for the virtual desktop networking. Click Next.

🖉 vSphere Client Window	s Guest Customization	×
Network Select if you want to	o customize the software settings for each network interface.	
Resistration Information Computer Name Administrator Password Time Zone Rin Once Workproup or Domain Operating System Option Save Specification Ready to Complete	This guest operating system should use the following network settings:	
Help	< Back Next >	Cancel

- **16.** For Workgroup or Domain, select the radio button for Windows Server. Enter the domain for environment.
- 17. Specify the user account name password. Click Next.

Workgroup or Domain This virtual machine	may belong to a workgrou	n or domain		
The Fitter Indefinite	may beenig to a nonkgrou	p or domain.		
egistration Information				
Computer Name	How will this virtual mach	nine participate in a network?		
Vindows License	Workgroup:	WORKGROUP		
dministrator Password ime Zone	Windows Server	vdlab-vspex.local		
tun Once			44	
etwork Vorkgroup or Domain			dd a computer to the domain.	
perating System Option	Username:	Administrator		
ave Specification teady to Complete	Password:	******		
to complete	Confirm	******		
•				

18. Select the checkbox to generate the new security ID. Click Next.

Γ

🕢 vSphere Client Window	s Guest Customization		X
Operating System Op Configure these op	tions tional parameters for the guest operating system.		
Redistration Information Computer Name Windows License Administrator Password Time Zone Histopas Workpath Operating System Opt Swe Specification Ready to Complete	Generate New Security ID (SID) Select this item to generate a new security identity.		
Help		< Back Next >	Cancel

19. Select the checkbox to Save the customization specification for later use and provide a name.

1

🕗 vSphere Client Windows	Guest Customization	×
Save Specification Would you like to save	ve this customization specification for later use? It can be accessed from the Customization Specification Manager.	
Registration Information Computer Name Windows License Administrator Password Time Zone Run Once	Very Save this customization specification for later use Name: WIN-7-GOLDEN-IMAGE-VDI-CUSTOMIZATION-SPECIFICATIONS Description:	
Networks Worksroup or Doman Operating System Option Save Specification Ready to Complete	WIN-7-GOLDEN-IMAGE-VDI-CUSTOMIZATION-SPECIFICATIONS-CLUSTER	
• •		
Help	< Back Next > Cano	el

20. Verify and click Finish.

Registration Information Computer Name	Review this summary an	d dick Einish	
Windows License Admisistack Password Time Zone Rutwork Network of Company Network of Company Workaroup or Domain Operating System Option Ready to Complete	Generate new SID	Administrator vdlab-vspex.local Per Server 5 ****** (GMT-0800) Tijuana, Los Angeles, Seattle, Vancouver Typical vdlab-vspex.local Administrator true WIN-7-GOLDEN-IMAGE-VDI-CUSTOMIZATION-SPECIFICATIONS	

21. To edit or modify the customization specification, log into vCenter Client with vCenter server IP and credentials. Go to the Home screen and select Customization Specification Manager. Select Saved customization, right -click and select edit.

Configure the View Desktop Pools and Options.

Desktop Pools are the containment object in View 5.2 Administrator that hold the configuration and the provisioned linked clones in the View environment.

The maximum recommended number of virtual machines in a VMware ESXi cluster is 1000. Therefore, we created two View 5.2 pools with identical settings to match up with our two ESXi 5.1 clusters for VDI described earlier in this document.

The following sections describe how we configured our View 5.2 environment.

Create the Desktop Pools

1. Log into View Administrator console. on the left side; from drop menu for Inventory select Pools. Click Add to create a new desktop pool.

Updated 7/11/2013 11:28 AM	Pools					
Remote Sessions 0 Local Sessions 0 Problem Desktops 0	Add Edit Delete Entitlements • Status • Folder • More Commands					
Events 0 0 0 0 0 System Health 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Filter •	Find Cle				
Inventory	ID III	Display Name	Type Automated Pool	Source	User Assi.	
	WDI-CL1	VDI-CL1		vCenter (linked clone)	Floating	
R Dashboard	WDI-CL2	VDI-CL2	Automated Pool	vCenter (linked clone)	Floating	
🐣 Users and Groups						
# Inventory						
🛄 Pools						
🔂 Desktops						
Persistent Disks						
📌 ThinApps						
 Monitoring 						
▶ Policies						
▼ View Configuration						

There are three types of Desktop Pools you can create and descriptions for each type is given on the right side of the screen.

2. Select Automated Pool and click Next.



There are two types of User Assignment options available:

- Dedicated (desktops that are manually or automatically assigned to users)
- Floating (desktops that are randomly assigned to users from the pool.



For the purpose of testing, the Floating user assignment is used.

3. Select Floating. Click Next.



4. Select the radio button for either Full Vitual Machine or view composer linked clones. Click Next.

<u>Note</u>

For this study, we chose View Composer linked clones.

Updated 8/2/2013 12:16 PM 🤕	Pools					
Remote Sessions 0 Local Sessions 0 Problem Desktops 0	Add Edit Delete			itatus 👻 🔻 Folder	More Commands	
Events 🚯 0 🖄 0 System Health 🔲 🗐 🗐	Add Pool ()					
77 0 0 0	Pool Definition	vCenter Server				
Inventory	Type User Assignment	O Full virtual m			View Composer View Composer linked clones	
Solution Contract Con	vCenter Server Setting	View Compo vCenter Se		View Composer	share the same base image and use less storage space than full virtual machines.	
Torentory CP pool Constance Prost Prost Prontoring Production Product Licensing and Usage Global Settings Registered Desktop Sources Administrators ThinApp Configuration	Pool Identification Pool Settings Provisioning Settings View Composer Disks Storage Optimization vicenter Settings Advanced Storage Options Guest Customization Ready to Complete	vcenter.vdilab v.local(adminis		vewcompserv.vdiab- v.local	The user profile for linked dones can be redirected to persistent disks that will be unaffected by OS updates and refreshes. Supported Features Local Mode PCOP Storage savings Recompose and refresh QuickProp quest	
Event Configuration		Description: More			customization Sysprep guest customization (vSphere 4.1 or higher) Persona management 	

5. Enter a unique pool ID and Display name optionally, select a folder for the Desktops. Click Next.

Updated 8/2/2013 12:16 PM 🥭	Pools						
Remote Sessions 0 Local Sessions 0 Problem Desktops 0 Events 0 System Health 0	Add Edite Entitlements Folder More Commands Add Pool - VDI-CL3 0 <td< th=""></td<>						
77 0 0 0	Pool Definition	Pool Identificatio	n				
77 0 0 0 Inventory	Type User Assignment	ID:	VDI-CL3	ID The pool ID is the unique name			
R Dashboard	vCenter Server	Display name:	VDI-CL3	used to identify this pool.			
🐸 Users and Groups	Setting	View folder:	/	Display Name			
Inventory Pools Desktops Persistent Disks IninApps	Pool Identification Pool Settings Provisioning Settings View Composer Disks Storage Optimization	Description:	VMware View 5.2 Horizon Virtual Machines Deployment Pool	The display name is the name that users will see when they connect to View Client. If the display name is left blank, the ID will be used. View Folder			
Monitoring	vCenter Settings						
 Policies View Configuration Servers Product Licensing and Usage 	Advanced Storage Options Guest Customization Ready to Complete			View folders can organize the pools in your organization. The can also be used for delegated administration.			
Global Settings				Description			
Registered Desktop Sources Administrators ThinApp Configuration				This description is only shown on the Settings tab for a pool within View Administrator.			

Γ

6. Configure the Pool Settings as needed. Select all default settings except the Remote Desktop Power Policy. Select Ensure deskstops are always powered on. Click Next.



- 7. On the Provisioning Settings page, set the following options:
- Basic: Enable provisioning and Stop provisioning at error.
- Virtual Machine Naming: Use naming pattern.

۵, Note

Use $\{n\}$ to deploy multiple desktops with same naming pattern. In case of name used VM- $\{n\}$ deployed desktops will be VM-1, VM-2 VM-10

• Pool Sizing: Select maximum number of desktops, number of powered on desktops and how to provision the desktops

۵, Note

For this study, we provisioned the entire desktops up front.

8. Select the radio button to Redirect disposable files to a non-persistent disk, set the Drive size for the disk, and select a Drive. Click Next.



9. Check the box for Select separate datastore for replica disk and OS disk. Click Next.



10. Select parent image (Golden Image), associated snapshot with GI image, location for VM if any specific folder was created, Host or Cluster where desktops are going to provision, Resource Pool, Linked Clone datastore, Replica disk datastores.



I

For our testing we created 2 Pools with 1000 desktops in each. One Pool was created with Cluster1 as host Resource Pool. 8 VMFS5 datastores for Linked Clones and one Replica disk datastore were selected. The second Pool was configured similarly with the remaining 8 VMFS5 datastores for Linked Clones and the remaining Replica VMFS5 datastore for the Replica disk.

(ated 7/11/2013 11:28 AM 🥭 🗛	Add Pool - VDI-CL3					
	ool Definition	vCenter Settings				
oblem Desktops 0	Type User Assignment	Default Image				
rents 🛛 🖗 0 🔔 0 rstem Health 📕 🗐 🗐	vCenter Server	1 Parent VM:	/vD1-2000/vm/G1	Browse		
73 0 0 0	etting Pool Identification	2 Snapshot:	/WIN7-Snashoot-CLS1-0509	Browse		
	Pool Settings	Virtual Machine Location				
Dashboard	Provisioning Settings View Composer Disks	3 VM folder location:	//DI-2000/vm///DI-CL1	Browse		
nventory	Storage Optimization vCenter Settings	Resource Settings				
Desktops	Advanced Storage Options Guest Customization	4 Host or cluster:	/VDI-2000/host/VDI-Desktops-Pool1	Browse		
Persistent Disks P ThinApps	Ready to Complete	5 Resource pool:	/vDI-2000/host/vDI-Desktops-Pool1/R	Browse		
fonitoring folicies		6 Linked clone datastores:	8 selected	Browse		
liew Configuration Servers Product Licensing and Usage		7 Replica disk datastores:	1 selected	Browse		

11. On the Advanced Storage Options page, check box to enable Use Storage Accelerator and add Blackout time if necessary. Click Next.



 Browse to select the AD container to be used for the provisioned machines. Select the radio button for Use a customization specification and select customization created from the Parent Windows 7 image VM.

1

ool Definition	Guest Customization			
Type User Assignment vCenter Server	Domain:	vdi-vspex.com(administ	rator) 🛛 🔻	6
etting Pool Identification	AD container:	CN=Computers	Browse	
Pool Settings	Allow reuse of pre-e	existing computer accounts 📀		
Provisioning Settings View Composer Disks	Use QuickPrep			
Storage Optimization	Power-off script nam	ne:		
vCenter Settings				
Advanced Storage Options	Power-off script para	ameters:		Example: p1 p2 p3
Guest Customization Ready to Complete	Post-synchronization	n script name:		
	Post-synchronization	h script parameters:		Example: p1 p2 p3
	 Use a customization 	specification (Sysprep)		
	Name	e Guest OS	De	scription
	Win7-opt	Windows		

13. Verify all the details provided for the pool settings and check box to entitle specific users and groups to provide access to the desktops in the Pool and click Finish.

	Add Pool - VDI-CL3					
dated 7/11/2013 11:28 AM 🥭	Pool Definition	Ready to Complete				
Remote Sessions 0 Local Sessions 0	Type User Assignment		Entitle users after this wizard finishe			
Problem Desktops 0	vCenter Server	Type:	Automated			
System Health	Setting	User assignment:	Floating assignment			
73 0 0 0	Pool Identification	vCenter Server:	vcenter.vdilab-v.local(administrator)			
Pool Settings	Pool Settings	Use View Composer:	Yes			
ventory	nd Groups vCenter Settings Y Advanced Storage Options	Unique ID:	VDI-CL3			
Dashboard		Display name:	VDI-CL1			
Users and Groups		View Folder:	1			
Inventory		Desktop pool state:	Enabled			
I Pools		Remote Desktop Power Policy:	Ensure desktops are always powered on			
Desktops	Guest Customization Ready to Complete	Automatic logoff after disconnect:	Never			
P ThinApps		Connection Server restrictions:	None			
Monitoring	itoring cles Configuration	Allow users to reset their desktop:	No			
View Configuration		Allow multiple sessions per user:	No			
Servers Product Licensing and Usage		Delete or refresh desktop on logoff:	Refresh Immediately			
Global Settings		Default display protocol:	PCoIP			
Registered Desktop Sources		Allow users to choose protocol:	Yes			
Administrators		3D Renderer:	Disabled			
ThinApp Configuration Event Configuration		Max number of monitors:	1			
Event Configuration		Max resolution of any one monitor:	1920×1200			
		HTML Access:	Disabled			
		Adobe Flash quality:	Disabled			
		Enable provisioning:	Yes			
		Stop provisioning on error:	Yes			
		Virtual Machine Naming:	Use a naming pattern			
		VM naming pattern:	VDI-CL3			
		Provision all desktops up-front:	Yes			
		Max number of desktops:	1,000			
		Number of spare (powered on) desktops:	1,000			
		Minimum number of ready (provisioned) desktops during View Composer maintenance	0			

14. On the Entitlements page, click Add.

Γ

Domain	Email

- **15.** Enter a name for the users or groups who will be authorized to use View desktops in the pool. Click Find.
- **16.** Select the appropriate users and group from the list. Click OK.

ype:	✓ Users	Groups		
Domain:	Entire Directory			
Name/User name:	Contains 🛛 🔻	Login_VSI		
Description:	Contains 🗸 🔻			
		Find		
Displaying the first :	100 results that match ye	Find our criteria. Refir	e your search criteria	to see additional results
Displaying the first :	100 results that match yo		e your search criteria	to see additional results
Name		our criteria. Refir		
Name Login_VSI_TS	User Name	our criteria. Refir		In Folder
Name Login_VSI_TS Login_VSI1	User Name Login_VSI_TS/vdilab	our criteria. Refir	Description	In Folder vdilab-v.local/Login_
Name Login_VSI_TS Login_VSI1 Login_VSI10	User Name Login_VSI_TS/vdilab Login_VSI1@vdilab-v	our criteria. Refir	Description Login VSI	In Folder vdilab-v.local/Login_ vdilab-v.local/Login_
	User Name Login_VSI_TS/vdilab Login_VSI1@vdilab-v Login_VSI10@vdilab-	our criteria. Refir	Description Login VSI Login VSI	In Folder vdilab-v.local/Login_ vdilab-v.local/Login_ vdilab-v.local/Login_

17. When the pool is Enabled and has Entitlements, both the columns will turn green.

VMware View Admi									ut Help Logout (ed	
Ipdated 12/11/2012 5:30 PM 🖉	Pools									
Remote Sessions 0 Local Sessions 0 Problem Desktops 0	Add	Add								
Events System Health 29 0 0 0	Filter •		Find Clea	r Folder:	a					
	ID	Display Name	Type	Source	User Assi	vCenter Server	Entitled	Enabled	Sessions	
Dashboard Busers and Groups Inventory	VDI-VMs	VD1-VMs	Automated Pool	vCenter (linked clor	Dedicated	vcenter.vdi-vspex.com	0	~	0 Remote, 0 Local	
Pools										
🔂 Desktops 🚍 Persistent Disks 🎤 ThinApps										
Monitoring										
Policies										
► View Configuration										

After the completion of the pool setting, a replica from the parent VM is created and the provisioning of the desktops as per the pool settings begins.

 Image: WDI-Desktops-Pool2

 Image: WDI-Desktops-Pool2
 </t

Test Setup and Configurations

In this project, we tested a single Cisco UCS B200 M3 blade in a single chassis and fourteen Cisco UCS B200 M3 blades in two chassis to illustrate linear scalability.

Cisco UCS Test Configuration for Single Blade Scalability

Figure 18 illustrates the Cisco UCS test configuration single-blade scalability.

Figure 18 Cisco UCS B200 M3 Blade Server for Single Server Scalability



Hardware components

- 1 X Cisco UCS B200-M3 (2 X E5-2690 @ 2.9 GHz) blade server with 256GB of memory (16 GB X 16 DIMMS @ 1666 MHz) Windows 7 SP1 Virtual Desktop hosts
- 2 X Cisco UCS B250-M2 (2 X 5680 @ 3.333 GHz) blade servers with 96 GB of memory (4 GB X 24 DIMMS @ 1333 MHz) Infrastructure Servers
- 4 X Cisco UCS B250-M2 (2 X 5680 @ 3.333 GHz) blade servers with 192 GB of memory (4 GB X 48 DIMMS @ 1333 MHz) Load Generators
- 2 X M81KR (Palo) Converged Network Adapter/Blade (B250 M2)
- 1X VIC1240 Converged Network Adapter/Blade (B200 M3)
- 2 X Cisco Fabric Interconnect 6248UPs
- 2 X Cisco Nexus 5548UP Access Switches
- 1 X EMC VNX System storage array, two controllers, two Datamovers, 2 x dual port 8GB FC cards, 2 x dual port 10 GbE cards, 4 x 200GB Flash Drives for EMC Fast Cache, 30 x 300GB SAS drives for VMFS datastores, 8 x 600GB SAS Drives for Infrastructure and Boot LUNs and 2 x 300GB SAS drives and 1 200GB Flash Drive for hot spares

Software components

- Cisco UCS firmware 2.1(1a)
- Cisco Nexus 1000V virtual distributed switch
- VMware ESXi 5.1 for VDI Hosts
- Horizon View 5.2
- Windows 7 SP1 32 bit, 1vCPU, 1 GB of memory, 18 GB/VM

Cisco UCS Configuration for Two Chassis—Fourteen Blade Test

Figure 19 illustrates the two chassis test configuration.

Figure 19 Two Chassis Test Configuration-14 x B200 M3 Blade Servers



Hardware components

- 14 X Cisco UCS B200-M3 (2 X E5-2690 @ 2.9 GHz) blade server with 256GB of memory (16 GB X 16 DIMMS @ 1666 MHz) Windows 7 SP1 Virtual Desktop hosts
- 2 X Cisco UCS B250-M2 (2 X 5680 @ 3.333 GHz) blade servers with 96 GB of memory (4 GB X 24 DIMMS @ 1333 MHz) Infrastructure Servers
- 6 X Cisco UCS B250-M2 (2 X 5680 @ 3.333 GHz) blade servers with 192 GB of memory (4 GB X 48 DIMMS @ 1333 MHz) Load Generators
- 2 X M81KR (Palo) Converged Network Adapter/Blade (B250 M2)
- 1X VIC1240 Converged Network Adapter/Blade (B200 M3)
- 2 X Cisco Fabric Interconnect 6248UPs
- 2 X Cisco Nexus 5548UP Access Switches
- 1 X EMC VNX System storage array, two controllers, two Datamovers, 2 x dual port 8GB FC cards, 2 x dual port 10 GbE cards, 4 x 200GB Flash Drives for EMC Fast Cache, 30 x 300GB SAS drives for VMFS datastores, 8 x 600GB SAS Drives for Infrastructure and Boot LUNs and 2 x 600GB SAS drives and 1 200GB Flash Drive for hot spares

Software components

- Cisco UCS firmware 2.1(1a)
- Cisco Nexus 1000V virtual distributed switch
- VMware ESXi 5.1 for VDI Hosts
- Horizon View 5.2
- Windows 7 SP1 32 bit, 1vCPU, 1.5 GB of memory, 18 GB/VM

Testing Methodology and Success Criteria

All validation testing was conducted on-site within the Cisco Labs with joint support from both Cisco and EMC resources.
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.

Load Generation

Within each test environment, load generators were utilized to put demand on the system to simulate multiple users accessing the Horizon View 5.2 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 Horizon View 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 Horizon View 5.2 via a VMware Horizon View PCoIP protocol connection.

User Workload Simulation—LoginVSI From Login Consultants

One of the most critical factors of validating a Horizon View 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 allows customers to easily replicate the testing results in their environment.



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 two minutes.
- The medium workload opens up to five apps simultaneously.
- The type rate is 160ms for each character.
- Approximately two 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.



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

Testing Procedure

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

Pre-Test Setup for Single and Multi-Blade Testing

- All virtual machines were shut down utilizing the vCenter.
- 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 5.1 VDI host blades to be tested were restarted prior to each test cycle.

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 155 single server users or 2000 full scale test users to become active within 2 minutes after the session is launched.

For each of the three consecutive runs on single blade (155 User) and 14-blade (2000 User) tests, the same process was followed:

- 1. Time 0:00:00 Started ESXtop Logging on the following systems:
 - VDI Host Blades used in test run
 - Profile Servers used in test run
 - SQL Servers used in test run
 - 7 or 80 Launcher VMs
- 2. Time 0:00:10 Started EMC Basic Performance Logging on SPs
- 3. Time 0:00:15 Started EMC NFS Performance Logging on Datamovers
- 4. Time 0:05 Take 155 or 2000 desktops out of maintenance mode on Horizon View Admin Console
- 5. Time 0:06 First machines boot
- 6. Time 0:33 155 or 2000 desktops booted on 1 or 14 blades
- 7. Time 0:35 155 or 2000 desktops available on 1 or 14 blades
- 8. Time 0:50 Start Login VSI 3.6 Test with 155 or 2000 desktops utilizing 7 or 80 Launchers
- 9. Time 1:20 155 or 2000 desktops launched
- **10**. Time 1:22 155 or 2000 desktops active
- **11.** Time 1:35 Login VSI Test Ends
- 12. Time 1:50 155 or 2000 desktops logged off
- 13. Time 2:00 All logging terminated

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.

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.



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 percent decrease in the number of users passing the test versus Login VSI 2.0 on the same server and storage hardware.

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.

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.

Five 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:

Activity (RowName)	Result (ms)	Weight (%)	Weighted Result (ms)
Refresh document (RFS)	160	100%	160
Start Word with new doc (LOAD)	1400	33.3%	467
File Open Dialogue (OPEN)	350	100%	350
Start Notepad (NOTEPAD)	50	300%	150
Print Dialogue (PRINT)	220	200%	440
Replace Dialogue (FIND)	10	400%	40
Zip 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 $1800 \times 125\% + 3000 = 5250$ ms.

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.

Determining VSIMax

The Login VSI analyzer will automatically identify the "VSImax". In the example below the VSImax is 99. 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 20 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)



We discovered a technical issue with the VSIMax dynamic calculation in our testing on Cisco B200 M3 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 is as 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 VMware Horizon View Desktop Administrator will be monitored throughout the steady state to make sure 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.

The purpose of this testing is to provide the data needed to validate VMware View 5.2 automated pool, floating assignment linked clone virtual desktops using ESXi 5.1 and vCenter 5.1 to virtualize Microsoft Windows 7 SP1 desktops on Cisco UCS B200 M3 blade servers using a EMC VNX5500 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 View 5.2 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 in the next section of the document.

Cisco UCS Test Configuration for Single-Server Scalability Test Results

This section details the results from the View 5.2 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% 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.

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.

The charts below present our recommended maximum Login VSI Medium workload loading on a single blade server.





The following graphs detail CPU, Memory, Disk and Network performance on the Single Cisco UCS B200-M3 Blades







Figure 23 155 User Single B200 M3 Available Memory Boot Phase



Figure 24 155 User Single B200 M3 Cisco VIC1240 MLOM Mbps Received/TransmittedBoot Phase



Figure 25 155 User Single B200 M3 Cisco VIC1240 MLOM Physical Disk Adapter MBps Read/Write Boot Phase



Figure 26 155 User Single B200 M3 CPU Core Utilization - Test Phase





Figure 27 155 User Single B200 M3 CPU Processor Total Utilization Time - Test Phase





Figure 29 155 User Single B200 M3 Cisco VIC1240 MLOM Mbps Received/Transmitted Test Phase



Figure 30 155 User Single B200 M3 Cisco VIC1240 MLOM Mbps Read/Written Test Phase



The following charts details for VIEW Connection Server performance during the single blade, 155 User test: Boot Phase



Figure 31 155 User View Connection Server 5.2 CPU Utilization



Figure 32 155 User View Connection Server 5.2 Available Memory



ſ





Figure 34 155 User View Connection Server 5.2 Bytes Sent/Second









Figure 36 155 User View 5.2 - View Connection Total User Time- TEST Phase

Figure 37 155 User View 5.2 - View Connection Server Available Memory









Figure 39 155 User View 5.2 View Connection Server Bytes Sent

Cisco UCS Test Configuration for 2000 Desktop Two-Cluster Scalability Test Results

This section details the results from the View 5.2 Hosted VDI seven blade server, two-cluster, 2000 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 below 143 users per blade across the system. Two ESX Clusters, each containing seven B200 M3s ran the entire workload. In fact the fourteen blade test harness provides N+1 server fault tolerance on a system 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 143 user sessions below. We have provided performance charts for all 14 blades in Appendix B to illustrate this point.

Given adequate storage capability, the blade CPU utilization determined the maximum recommended VM density per blade for the 2000 user environment.

We also present performance information on key infrastructure virtual machines with the tested blade data.

For the large scale test, we are including the EMC VNX5500 performance metrics as well.



Figure 40 2000 Desktop Sessions on VMware ESXi 5.1 below 4000 ms

The following graphs detail CPU, Memory, Disk and Network performance on a representative Cisco UCS B200 M3 Blade during the fourteen blade, 2000 User test. (Representative results for all fourteen blades in one of the vCenter clusters can be found in Appendix B.)

Figure 41 2000 User Single B200 M3 Core CPU Utilization Boot Phase





Figure 42 2000 User Single B200 M3 CPU Utilization Boot Phase

Figure 43 2000 User Single Cisco UCS B200 M3 Cisco NonKernel Mbytes Available Boot Phase







Figure 45 2000 User Single Cisco UCS B200 M3 Cisco VIC1240 MLOM VIC Mbps Receive/Transmit Boot Phase



Figure 46 2000 User Single Cisco UCS B200 M3 CPU Utilization Test Phase



Figure 47 2000 User Single Cisco UCS B200 M3 Cisco VIC1240 MLOM Network Adapter Mbps Receive/Transmit Test Phase



Figure 48 2000 User Single Cisco UCS B200 M3 Cisco VIC1240 MLOM Physical Disk Adapter MBps Read/Write Test Phase



Figure 49 2000 User Single Cisco UCS B200 M3 Cisco VIC1240 MLOM VIC Mbps Receive/Transmit Test Phase



Figure 50 2000 User Single Cisco UCS B200 M3 Cisco Non-Kernel Mbytes Avaaible



The following charts detail the VNX5500 performance during the fourteen blade, 2000 User test:



Figure 51 2000 Users EMC VNX5500 SP Utilization Boot Phase









ſ















Figure 57 2000 Users EMC VNX5500 SP Total Response Time Test Phase

The following charts detail infrastructure server performance during the fourteen blades, 2000 User test:

Figure 58 2000 User View Connection Server 5.2 CPU Utilization Test Phase





ſ























I

The following charts detail infrastructure server performance during the fourteen blades, 2000 User test:







Figure 66 2000 User View Connection Server 5.2 Available Memory Test Phase











Scalability Considerations and Guidelines

There are many factors to consider when you begin to scale beyond 2000 User, six chassis, 14 VDI host server configuration, which this reference architecture has successfully tested. In this section we give guidance to scale beyond the 2000 user system.

Cisco UCS System Configuration Considerations

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 6248 and 6296 models. Our single UCS domain can grow to 160 half-width blades.
- With Cisco UCS 2.1 management software, released late in November 2012, each Cisco UCS 2.1 Management domain is ostensibly manageable by Cisco UCS Central, our new manager of managers, vastly increasing the reach of the Cisco UCS system.

- As scale grows, the value of the combined Cisco 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 Cisco 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 Cisco UCS B200 M3 VDI blade server and one Cisco UCS B200 M3 Infrastructure blades servers in each chassis.

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

VMware View 5.2 Considerations

VMware View Composer can create and provision up to 1000 desktops per pool when deployed on vSphere 4.1 or later. View Composer can also perform a recompose operation on up to 1,000 desktops at a time. Desktop pool size is limited by the following factors:

- Each desktop pool can contain only one ESX/ESXi cluster.
- With View 5.2 and later and vSphere 5.0 and later, an ESXi cluster can contain more than 8 ESXi hosts (up to 32), but you must store the linked-clone replica disks on NFS datastores.
- Each CPU core has compute capacity for 8 to 10 virtual desktops.

A single VMware View Connection server can host up to 2000 simultaneous connections over any supported connection type. Seven View Connection Servers (5 active plus 2 spares) can host up to 10000 direct, RDP or PCoIP connections simultaneously. The sever View Connection Server cluster configuration should not be clustered across WAN links.

VMware View deployments can use VMware HA clusters to guard against physical server failures. With View 5.2 and later and vSphere 5 and later, if you use View Composer and store replica disks on NFS datastores, the cluster can contain up to 32 servers, or nodes.

With vCenter 4.1 and 5.0, each vCenter Server can support up to 10,000 virtual machines.

For more information on VMware View 5.2 configuration and guidelines, see Chapter 11 References.

EMC VNX Storage Guidelines for Horizon View 5.2 Provisioned 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".

VMware ESXi 5.1 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 the References section of this document.

References

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

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_C ODE=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 B200 M3 Blade Server Resources

http://www.cisco.com/en/US/partner/products/ps12288/index.html

Cisco UCS 6200 Series Fabric Interconnects

http://www.cisco.com/en/US/partner/products/ps11544/index.html

Cisco Nexus 1000V Series Switches Resources

http://www.cisco.com/en/US/partner/products/ps9902/index.html

Cisco Nexus 5500 Series Switches Resources

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

Download Driver Software for Cisco UCS B200 M3 Blade Server

http://software.cisco.com/download/release.html?mdfid=283612660&flowid=22121&softwareid=283655658&release=2.1%281a%29&relind=AVAILABLE&rellifecycle=&reltype=latest

Download Cisco UCS Manager and Blade Software Version 2.1(1b)

http://software.cisco.com/download/release.html?mdfid=283612660&flowid=22121&softwareid=283655658&release=2.1%281a%29&relind=AVAILABLE&rellifecycle=&reltype=latest

Download Cisco UCS Central Software Version 1.0(1a)

http://software.cisco.com/download/cart.html?imageGuId=8CAAAD77B3A1DB35B157BE84ED109A 4703849F53&i=rs

VMware View Reference Documents

View 5 Documents

Performance and Best Practices

http://www.vmware.com/files/pdf/view/vmware-horizon-view-best-practices-performance-study.pdf

View 5.2 Architecture and Planning https://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-architecture-planning.pdf

View 5 with PCoIP Network Optimization Guide

http://www.vmware.com/files/pdf/view/VMware-View-5-PCoIP-Network-Optimization-Guide.pdf

Virtual Desktop

Windows 7 Optimization Guide http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

EMC Reference Documents

• Sizing EMC VNX Series for VDI Workload - An Architectural Guideline

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&exter nalId=1021514
- VMware vSphere ESXi and vCenter Server 5 Documentation: http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.upgrade.doc%2FG UID-200B9E03-D46B-44A9-9B0E-4863D067CFFF.html
- VMware vCenter Management Webservices features do not function properly: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&exter nalId=1039180
- VMware® vCenter ServerTM 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_vSphere5.1.pdf

Appendix

Click the following link to open the Appendix: http://www.cisco.com/en/US/docs/unified_computing/ucs/UCS_CVDs/ucs_vspex_vview5.2_2000_app endix.pdf.

Γ