

Cisco UCS M-Series with Citrix XenApp 7.6

Last Updated: November 16, 2015



About Cisco Validated Designs

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

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

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

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

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

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

© 2015 Cisco Systems, Inc. All rights reserved.

Table of Contents

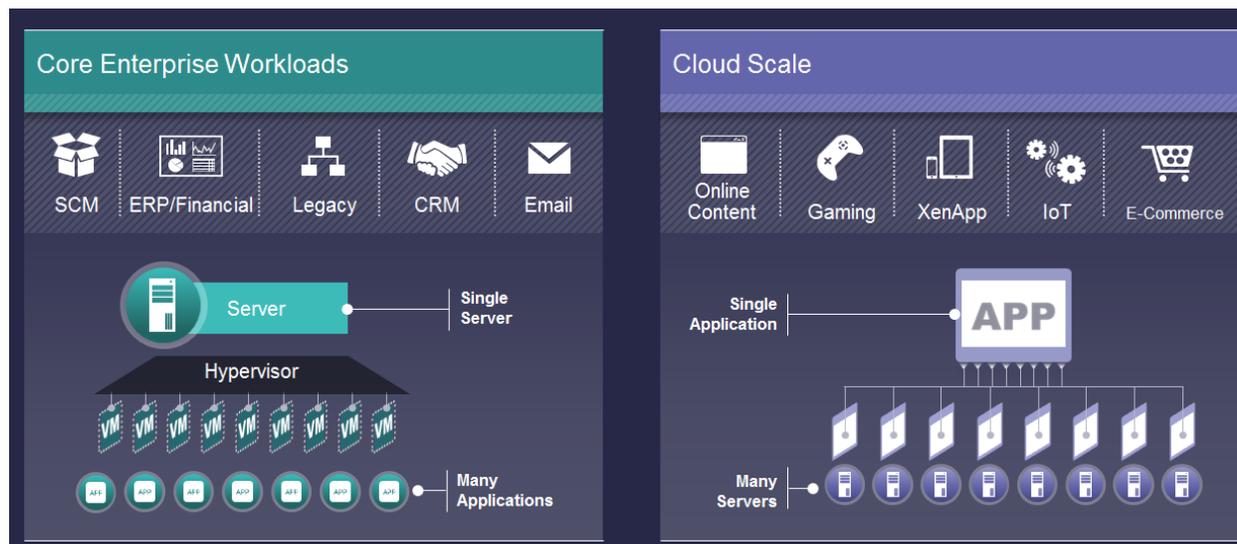
About Cisco Validated Designs	2
Executive Summary	6
Solution Overview.....	7
Introduction	7
Cisco UCS M-Series Bare Metal XenApp 7.6 Deployment.....	7
Audience	8
Solution Summary.....	8
Technology Overview	10
Cisco Unified Computing System (UCS)	10
Cisco Unified Computing System Components.....	10
Cisco UCS M-Series.....	11
Cisco UCS M4308 Modular Server Chassis	11
Cisco UCS 6248UP Fabric Interconnect.....	13
Cisco Nexus Physical Switching	14
Citrix XenApp 7.6	14
Solution Design.....	16
Cisco M-Series Bare Meta XenApp 7.6 Solution.....	16
Cisco UCS 6248UP Fabric Interconnect.....	16
Cisco UCS M4308 Modular Server Chassis	17
Cisco UCS M142 Cartridge Server	17
Cisco UCS System Link Technology	18
Virtualized Shared Local Storage	19
Virtualized Storage Controller	21
Building the Complete Server through System Link Technology	21
Citrix XenApp 7.6	23
Citrix Provisioning Services 7.6.....	23
Citrix Desktop Studio for XenApp 7.6	23
Benefits for Desktop Administrators.....	24
Citrix Provisioning Services Solution	24
Citrix Provisioning Services Infrastructure	25
Architecture.....	26
Deployment Hardware and Software	27
Hardware Deployed	27

Configuration Guidelines	28
Base Cisco UCS System Configuration	28
Add a Block of IP Addresses for Out-of-Band KVM Access	30
Acknowledge Cisco UCS Chassis	31
Create MAC Address Pools	32
Create UUID Suffix Pool	33
Create Server Pool	34
Create VLANs	35
Create Host Firmware Package	36
Create Disk Group Policy	39
Create Storage Profiles	40
Create Boot Policies	42
Create Service Profile Template	45
Citrix Infrastructure Configuration	49
Installing and Configuring Citrix Provisioning Server 7.6	61
Create the Provisioning Services Master Image	85
Install the PVS Target Device Software	94
Creating PVS vDisks	97
Install the XenApp Virtual Desktop Agent to the Master vDisk Image	103
Configure Local Hard Disks for PVS Write Cache with Script	108
Configure Local Hard Disks for PVS Write Cache Manually	114
Import the Service Profiles as Machines and Create the XenDesktop Catalog and Group	119
Citrix XenDesktop Policies and Profile Management	133
Configuring Citrix XenDesktop Policies	133
Configuring User Profile Management	134
Validation	136
Test Setup and Configuration	136
Cisco UCS Test Configuration for Single Blade Scalability	136
Cisco UCS Configuration for Scale Testing	137
Testing Methodology and Success Criteria	138
Testing Procedure	139
Success Criteria	140
VSImax 4.1.x Description	141
Server-Side Response Time Measurements	141
Calculating VSImax v4.1.x	141

Single-Server Recommended Maximum Workload	145
Test Results	146
Full Scale Testing	148
Scalability Considerations and Guidelines	150
Cisco UCS System Scalability	150
Scalability of Citrix XenDesktop 7.6 Configuration	150
Conclusion	152
About the Authors	153
Acknowledgements	153
Appendix A – Scripts for Configuring Local Write Cache	154
Registry Keys for Automated Write Cache Deployment	157
Windows Registry Editor Version 5.00	157
Appendix B – Complete Performance Charts for all Cartridges	163

Executive Summary

Cisco introduced an exciting new technology to support Cloud-Scale Computing called Cisco UCS M-Series. Cloud Scale workloads invert the typical core enterprise workload model where single servers support multiple applications.



This document provides a Reference Architecture for a Citrix XenApp 7.6 hosted shared desktop design using built on Cisco UCS M-Series Modular Server and Cisco UCS 6248UP Fabric Interconnects. The single application, Citrix XenApp run on Microsoft Windows 2012 R2 Operating Systems streamed to the Cisco UCS M142-M4 Cartridge servers using Citrix Provisioning Services 7.6's bare metal provisioning capability.

With the landscape of desktop and application virtualization constantly changing, the new Cisco UCS M-Series Modular servers running Citrix XenApp 7.6 offers a low cost, small foot print solution for high density XenApp workloads. Because of the unique architecture of Cisco UCS M-Series, our customers can actually add server shared desktops and applications into an existing environment with almost no (less than 400GB) requirement for additional external storage.

This document provides the architecture and design of a virtual desktop environment for up to 960 (840 with cartridge level fault tolerance) XenApp RDS hosted shared desktops. The XenApp 7.6 RDS hosted shared desktops are the only workloads running on the Cisco UCS M-Series chassis.

The supporting infrastructure is 100 percent virtualized and separate from the Cisco UCS M4308 chassis. The Citrix Virtual Desktop infrastructure runs on four virtual machines on Cisco UCS B200-M4 blades servers in an external chassis.

Where applicable, this document provides best practice recommendations and sizing guidelines for customer deployments of this solution.

Solution Overview

Introduction

Cisco UCS M-Series Bare Metal XenApp 7.6 Deployment

Enterprises are seeking to balance the need for large, centralized data centers and the need for excellent user experiences in remote and branch offices with larger user communities. Small and medium-sized businesses are seeking ways to run a compact, self-contained computing infrastructure that is economical and efficient and that offers the potential for growth.

Desktop virtualization, particularly server shared desktops, can help meet these challenges. Providing excellent performance for remote offices or branch offices over slow WAN links creates additional challenges. For midsize customers, one of the main barriers to entry is the capital expense required to deploy a solution that typically requires dedicated storage. For smaller customers, deployment of a desktop virtualization system for fewer than 300 users is cost prohibitive.

To overcome these entry-point barriers, Cisco has developed a self-contained desktop virtualization solution that can host up to 960 Citrix XenApp hosted shared desktops with a very modest external storage requirement (less than 450GB.) This architecture uses non-persistent remote desktop service (RDS) server desktops on an eight Cisco UCS M142-M4 cartridge, sixteen servers Cisco UCS M-Series platform with local storage.

The following infrastructure components reside outside of the Cisco UCS M-Series chassis and run on an existing infrastructure cluster of Cisco UCS B200 M4 Blade Servers:

- Microsoft Active Directory 2008 R2 or later domain controllers
- Microsoft SQL Server 2008 R2 or later clustered or Always On servers
- Microsoft file server or external storage for user data and user profiles

To add this solution to the existing infrastructure, you will need to add the following:

- Two Citrix XenApp 7.6 desktop brokers (Virtual machines - 50GB each)
- Two Citrix Provisioning Services 7.6 (virtual machines - 50GB each)
- Two Citrix Storefront Servers (virtual machines - 25GB each)
- Storage for Citrix XenApp vDisks (up to 200GB total)
- Cisco UCS M-Series 4308 2RU Chassis and up to 8 Cisco UCS M142 blade server cartridges

The Cisco UCS M-Series configuration used to validate the configuration is as follows:

- 1 Cisco UCS 4308 Cartridge Server Chassis
- 2 Cisco UCS 6248UP Fabric Interconnects
- 8 Cisco UCS M-Series 142-M4 Cartridges (2 Servers per Cartridge)

- Intel® Xeon® processor E3-1275L-v3, 4-core 2.7-GHz CPUs: 1 per blade
- 32-GB 1866-MHz DIMMs (4 x 8 GB): 1 per cartridge

Audience

This document describes the architecture and deployment procedures of an infrastructure comprised of Cisco and Citrix 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 to deploy Citrix XenApp 7.6 RDS workloads on Cisco UCS M-Series Modular Server Chassis.

Solution Summary

This solution is Cisco's Modular Server design for Virtual Desktop sessions providing our customers with a turnkey physical and virtual infrastructure specifically designed to support up to 960 remote desktop session users, 840 in a highly available proven design. This architecture is well suited for small to midsize deployments and enterprise-edge environments for RDS/hosted shared desktops .

The combination of technologies from Cisco Systems, Inc., Citrix Systems, Inc., and Microsoft, Inc. produced a highly efficient, robust and affordable desktop virtualization solution for a hosted shared desktop deployment supporting different use cases. Key components of the solution include the following:

- Great horsepower, tiny footprint. Cisco UCS M-Series Modular M142-M4 Cartridge Servers with a single quad core 2.7 GHz Intel Xeon (E3-1275L v3) processor and 32GB of memory for Citrix XenApp hosts provide the ideal bare-metal platform for Citrix XenApp 7.6 RDS on Microsoft Windows 2012 R2 physical hosts. The Intel Xeon E3-1275L v3 quad core processors used in this study provided a balance between excellent server performance and cost.
- Fault-tolerance with high availability built into the design. The design is based on using one Cisco Unified Computing System M4308 2 rack unit chassis with up to 8 Cisco UCS M142-M4 cartridges for hosted shared/RDS desktops. The design provides N+1 cartridge fault tolerance for the hosted shared desktops.
- Stress-tested to the limits during aggressive boot scenario. The 960 hosted shared desktop environment booted and registered with the XenApp 7.6 Delivery Controllers in under 15 minutes, providing our customers with an extremely fast, reliable cold-start desktop virtualization system.
- Stress-tested to the limits during simulated login storms. All 960 simulated users logged in and started running workloads up to steady state in 48-minutes without overwhelming the processors, exhausting memory or exhausting the storage subsystems, providing customers with a desktop virtualization system that can easily handle the most demanding login and startup storms.
- Ultra-condensed computing for the datacenter. The rack space required to support the system is just two rack units and is totally self-contained solution for RDS using on-board storage for Provisioning Services write cache.
- Cisco maintains industry leadership with the new Cisco UCS Manager 2.5(2a) software that simplifies **scaling, guarantees consistency, and eases maintenance**. Cisco's ongoing development efforts with Cisco UCS Manager, Cisco UCS Central, and Cisco UCS Director insure that customer environments are consistent locally, across Cisco UCS Domains and across the globe, our software suite offers

increasingly simplified operational and deployment management and it continues to widen the span of **control for customer organizations' subject matter experts** in compute, storage and network.

- Our 10G unified fabric story gets additional validation on 6200 Series Fabric Interconnects as Cisco runs more challenging workload testing, while maintaining unsurpassed user response times.
- Cisco System Link technology extends the Cisco UCS fabric inside the server for Cisco UCS M-Series. It is the first compute platform to separate CPU and memory from the rest of the server components. This technology allows up to 16 servers in 8 compact cartridges to share power, cooling, disks, disk controller and network over the Cisco UCS M-Series chassis midplane. This architecture is a perfect fit for scale-out Citrix XenApp on Microsoft Server 2012 R2.
- **Latest and greatest virtual desktop and application product. Citrix XenApp™ 7.6** follows a new unified product architecture that supports both hosted-shared desktops and applications (RDS) and complete virtual desktops (VDI). This new XenApp release simplifies tasks associated with small to very large-scale RDS/hosted shared desktop management. This modular solution supports seamless delivery of Windows apps and desktops as the number of users increase. In addition, HDX enhancements help to optimize performance and improve the user experience across a variety of endpoint device types, from workstations to mobile devices including laptops, tablets, and smartphones.
- Optimized to achieve the best possible performance and scale. For hosted shared desktop sessions, the best performance was achieved when 4 CPU cores are available to the XenApp 7.6 RDS physical machines. Each Microsoft Windows 2012 R2 host was configured with 32GB of memory for maximum density without paging.
- Provisioning desktop machines made easy. Citrix Provisioning Services 7.6 created hosted virtual desktops as well as hosted shared desktops for this solution using a single method for both, **the “PVS XenApp Setup Wizard.”** The addition of the feature **“Cache in RAM with overflow on hard disk”** greatly reduced the number of IOPS experienced by the onboard storage.

Technology Overview

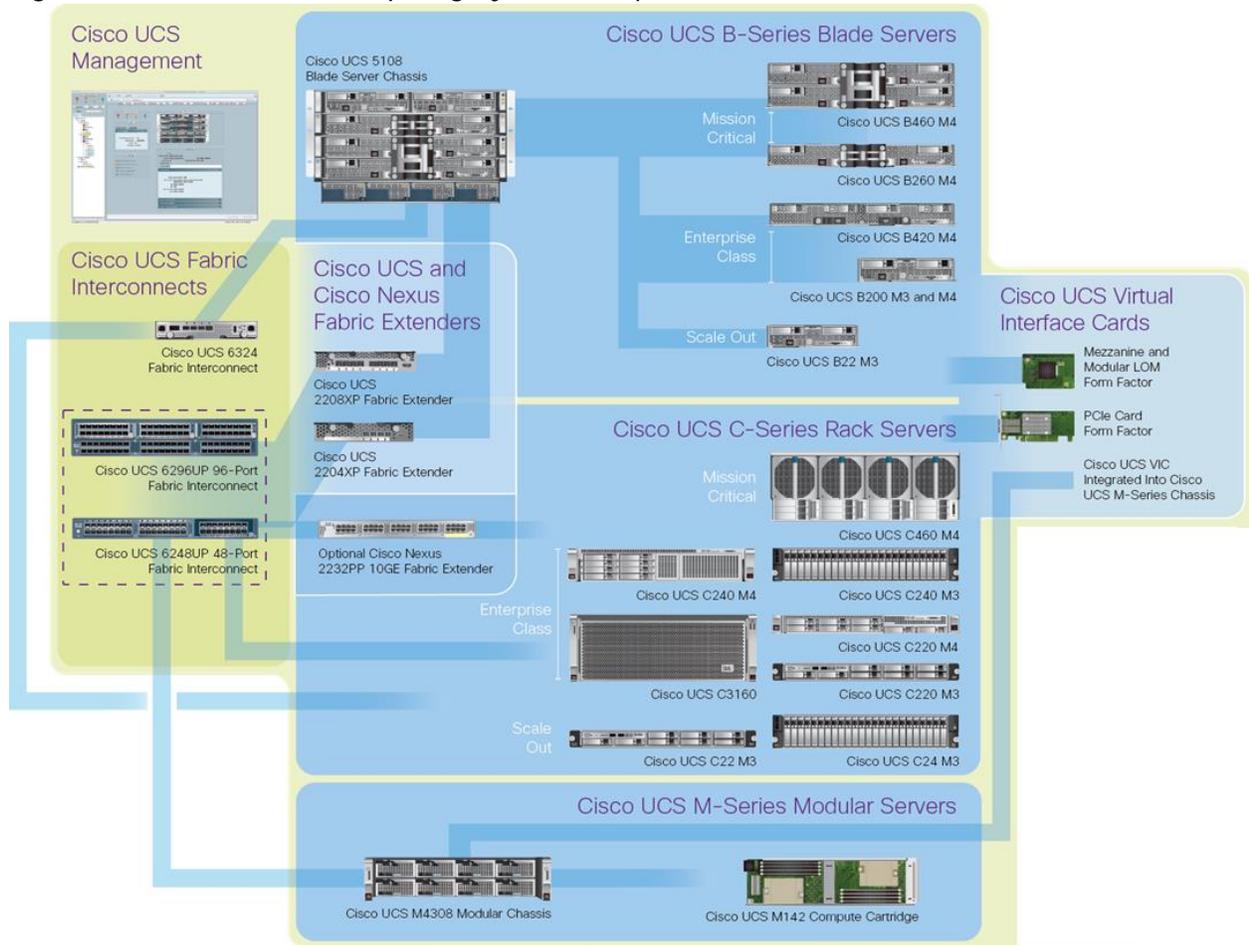
Cisco Unified Computing System (UCS)

Cisco 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.

Cisco Unified Computing System Components

Cisco UCS components are shown in Figure 1.

Figure 1 Cisco Unified Computing System Components



The Cisco UCS 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.

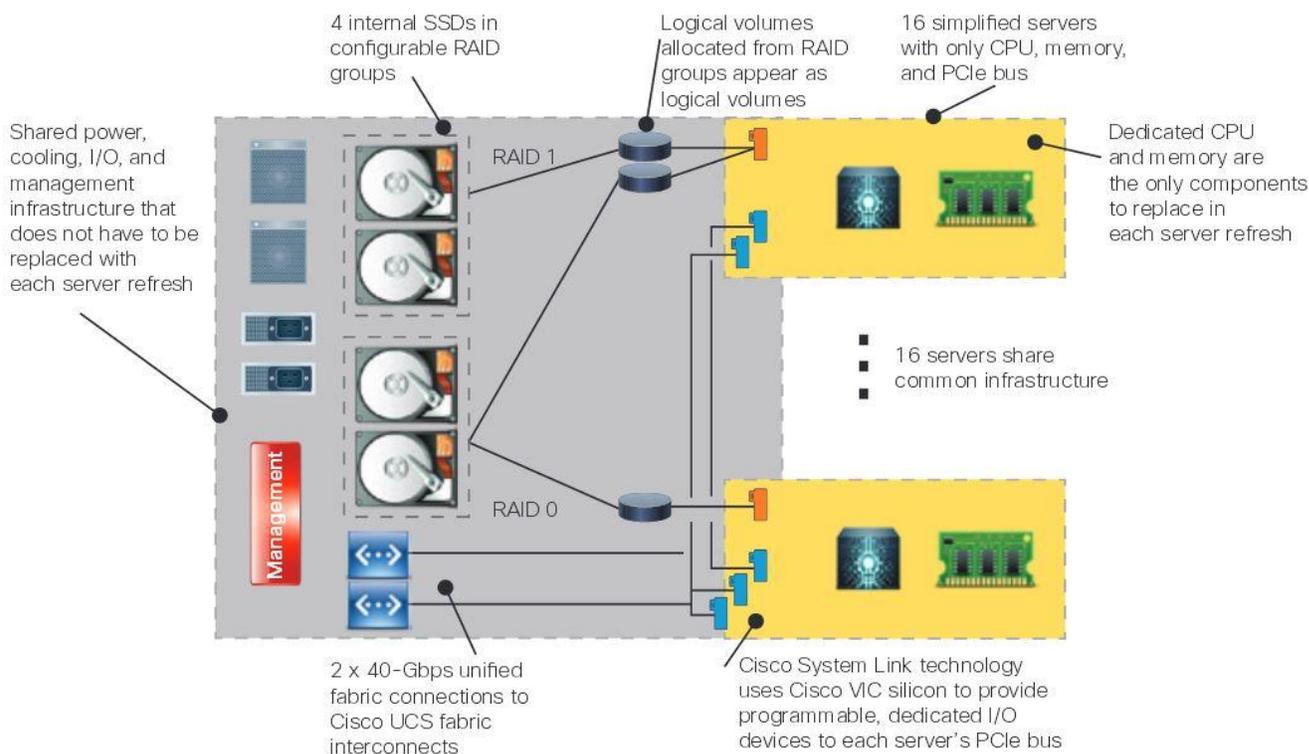
With model-based management, administrators manipulate a model of a desired system configuration, **associate a model's service profile with hardware resources and the system configures itself to match the model**. This automation speeds provisioning and workload migration with accurate and rapid scalability. 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.

Cisco UCS M-Series

Cisco UCS M-Series Modular Servers were designed for customers who want a solution with a smaller data center footprint with the density of a traditional blade solution, but still wants the robust management capabilities that come with Cisco UCS Manager. This solution delivers, servers, storage and networking in an easy to deploy, compact form factor.

Figure 2 Cisco UCS M-Series Overview



Cisco UCS M4308 Modular Server Chassis

The Cisco UCS M4308 Modular Chassis is the building block, the unit of scale, for the new Cisco UCS M-Series Modular Server platform. It delivers the benefits of this radically different architecture to Cisco UCS

M-Series Compute Cartridges and provides easy scalability to meet the needs of your applications without over-provisioning.

Features and Capabilities

The Cisco UCS M4308 Modular Chassis platform delivers a unique new infrastructure to meet the needs of today's highly parallelized and distributed applications.

This unique design allows Cisco to abstract server sub-systems fully into the infrastructure, completely off the compute nodes. The disaggregated sub-components are:

- Power
- Cooling
- I/O
- Hard drives
- Management

This separation of components in the M4308 lets users decouple the lifecycles of the sub-systems. Now every sub-component can be refreshed independently, on its own lifecycle schedule, without provoking a major platform refresh.

This 'independent resource' strategy can enable Cisco to optimize and more efficiently deliver infrastructure to meet the specific needs of your applications.

You no longer need costly and time-consuming professional services just to expand your compute capacity. With the M4308 and the M-Series solution, scaling is now easy and affordable.

The M4308 design also allows for smaller increments of scale, so your applications can have the number of compute nodes that they require to achieve the desired performance and availability. No more over-provisioning. No more wasted resources. Everything rests under a single management tool for easy scale and management transparency.

With this groundbreaking design, the Cisco UCS M-Series provides a highly dense, modular, and power-efficient platform de-signed to meet the needs of parallelized workloads. It provides for optimal:

- Performance and Watt usage
- Compute capacity and rack unit space

The Cisco UCS M-Series Modular Server system features a new 2 rack-unit (RU) chassis built on the foundation of Cisco innovation in virtual interface card (VIC) technology. All Cisco UCS M4308 chassis connect to a pair of Cisco UCS Fabric Interconnects with Cisco UCS Manager, providing easy, fast scalability with industry-leading Cisco UCS management.

The award-winning Cisco UCS Manager provides management for the M-Series with consistency and simplicity in device management. Cisco UCS Manager is a model-based, automated tool for element management that allows for easy integration with higher-level tools using our open XML API.

Specifications at a Glance

Cisco UCS M4308 Key Features

Unit of scale	By M4308 chassis
Chassis size	2 rack units
Compute cartridges per chassis	Up to 8 independent front-load cartridges
Compute nodes per chassis	Up to 16 nodes (servers) per chassis
Nodes (servers) per cartridge	1 or 2 independent servers (nodes) per cartridge 1 x Intel® Xeon® E3 v3 processor; 4 core; up to 32 GB memory
Processors per node	2 x Intel® Xeon® E5 v3 processor; up to 10 cores; up to 256 GB memory
Hard drives per chassis	4 x SSD - Scale from 480 GB SATA to 6.4 TB SAS
I/O per chassis	2 x 40 Gbps uplinks per chassis
Power	2 x 1400 Watt power supplies
Management and connectivity	Cisco UCS Manager and UCS 6200 Fabric Interconnects

Cisco UCS 6248UP Fabric Interconnect

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

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

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. 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 Nexus Physical Switching

The Cisco Nexus product family includes lines of physical unified port layer 2, 10 GB switches, fabric extenders, and virtual distributed switching technologies. In our study, we utilized Cisco Nexus 9372TX physical switches.

Citrix XenApp 7.6

Enterprise IT organizations are tasked with the challenge of provisioning Microsoft Windows apps and desktops while managing cost, centralizing control, and enforcing corporate security policy. Deploying Windows apps to users in any location, regardless of the device type and available network bandwidth, **enables a mobile workforce that can improve productivity. With Citrix XenApp™ 7.6, IT can effectively** control app and desktop provisioning while securing data assets and lowering capital and operating expenses.

The XenApp™ 7.6 release offers the following benefits:

- Comprehensive virtual desktop delivery for any use case. The XenApp 7.6 release incorporates the full power of XenApp, delivering full desktops or just applications to users. Administrators can deploy both XenApp published applications and desktops (to maximize IT control at low cost) or personalized VDI desktops (with simplified image management) from the same management console. Citrix XenApp 7.6 leverages common policies and cohesive tools to govern both infrastructure resources and user access.
- Simplified support and choice of BYO (Bring Your Own) devices. XenApp 7.6 brings thousands of corporate Microsoft Windows-based applications to mobile devices with a native-touch experience and **optimized performance. HDX technologies create a “high definition” user experience, even for graphics intensive design and engineering applications.**
- Lower cost and complexity of application and desktop management. XenApp 7.6 helps IT organizations take advantage of agile and cost-effective cloud offerings, allowing the virtualized infrastructure to flex and meet seasonal demands or the need for sudden capacity changes. IT organizations can deploy

XenApp application and desktop workloads to private or public clouds, including Amazon AWS, Citrix Cloud Platform, and (in the near future) Microsoft Azure.

- Protection of sensitive information through centralization. XenApp decreases the risk of corporate data loss, enabling access while securing intellectual property and centralizing applications since assets reside in the datacenter.

Solution Design

Cisco M-Series Bare Meta XenApp 7.6 Solution

With Cisco UCS M-Series Modular Server was architected specifically for the highly parallelized workloads typically found in cloud, online gaming, multi-variable computing, HPC and now XenApp 7.6 RDS workloads.

This new design eliminates the complexity of traditional servers by disaggregating the underlying component parts. Under-utilized and over-provisioned local resources that have historically been found inside traditional servers such as hard disk drives, I/O, base board and network controllers that are now aggregated and shared across multiple compute nodes.

Using XenApp 7.6 with the Cisco UCS M-Series Modular server allows Citrix administrators to move XenApp 7.6 workloads to a 2RU appliance and offload the workloads to the local storage resources and remove them from expensive SAN appliances. The performance and density of XenApp 7.6 workloads on the E3-1275L processors also provides phenomenal performance on a lower bin processors providing a better ROI.

The solution includes these components:

- Cisco UCS 6248UP Fabric Interconnect: 48-Port Fabric Interconnect is a core part of the Cisco Unified Computing System. Typically deployed in redundant pairs, the Cisco UCS 6248UP Fabric Interconnects provide uniform access to both networks and storage.
- Cisco UCS M4308 Modular Server Chassis: the building block, the unit of scale, for the new Cisco UCS M-Series Modular Server platform. It delivers the benefits of this radically different architecture to Cisco UCS M-Series Compute Cartridges and provides easy scalability to meet the needs of your applications without over-provisioning.
- Cisco UCS M142 M4 Cartridge Servers: Compute Cartridge eliminates the complexity of the traditional server unit, delivering discreet compute and memory, fully separated from the infrastructure components provided by the M4308 Chassis.
- Cisco UCS System Link Technology
- Cisco UCS Manager: Cisco UCS Manager provides unified, embedded management of all software and hardware components in a Cisco UCS M-Series solution.

Cisco UCS 6248UP Fabric Interconnect

The Cisco UCS 6248UP Fabric Interconnect Fabric Interconnect provides the management and LAN connectivity for the Cisco UCS M4308 Server Chassis and direct-connect rack-mount servers. It provides the same full-featured Cisco UCS management capabilities and XML API as the full-scale Cisco UCS solution in addition to integrating with Cisco UCS Central Software and Cisco UCS Director.

Figure 3 Cisco UCS 6248UP Fabric Interconnect



Cisco UCS M4308 Modular Server Chassis

The Cisco UCS M4308 Modular Chassis provides the shared midplane resources for up to eight Cisco UCS M142 M4 cartridges, each containing two discrete servers.

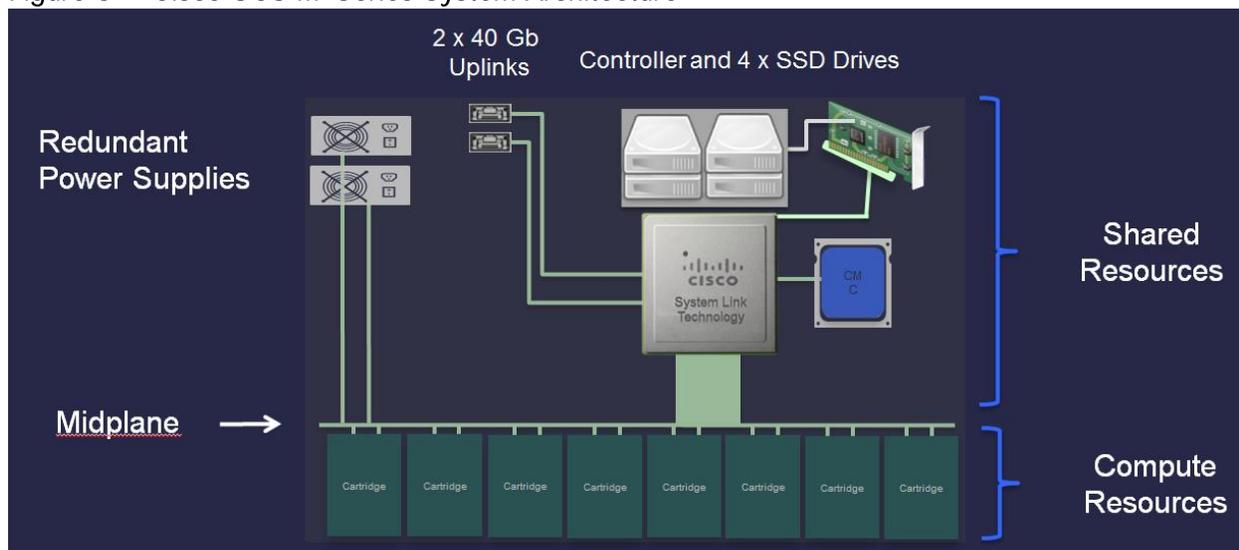
Figure 4 Cisco UCS M-Series Chasses M4308 with Cartridges-Front View



Figure 5 Cisco UCS M-Series Chasses with 4-400GB SSD Drives
4 x SSD – Scale from 480 GB SATA to 6.4 TB SAS



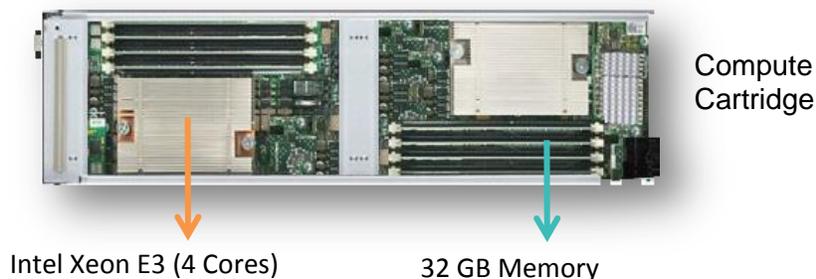
Figure 6 Cisco UCS M-Series System Architecture



Cisco UCS M142 Cartridge Server

Cisco UCS M142 Compute Cartridge eliminates the complexity of the traditional server unit, delivering discreet compute and memory, fully separated from the infrastructure components provided by the M4308 Chassis. The Cisco UCS M-Series Compute Cartridges and Cisco UCS M4308 Modular Chassis provide easy scalability to meet the needs of your applications without over-provisioning.

Figure 7 Cisco UCS M142 Compute Cartridge Layout



Specifications at a Glance

Cisco UCS M142 Key Features

Processors per node (server)	1 x Intel® Xeon® Processor E3-1200 v3, quad core
Compute nodes (servers) per cartridge	2 independent nodes (servers) per cartridge
Memory per node and per cartridge	32 GB memory per node with 64 GB per cartridge
Compute cartridges per chassis	8 independent front-load cartridges per chassis
Disk Drives	4 x SSD - scaling from 480 GB SATA to 6.4 TB SAS provided by a M4308 Modular Chassis
I/O	2 x 40 Gbps provided by a M4308 Modular Chassis
Power	2 x 1400 Watts provided by a M4308 Modular Chassis
Management	Stateless model-based management by Cisco UCS Manager provided by UCS 6200 Series Fabric Interconnects

Cisco UCS System Link Technology

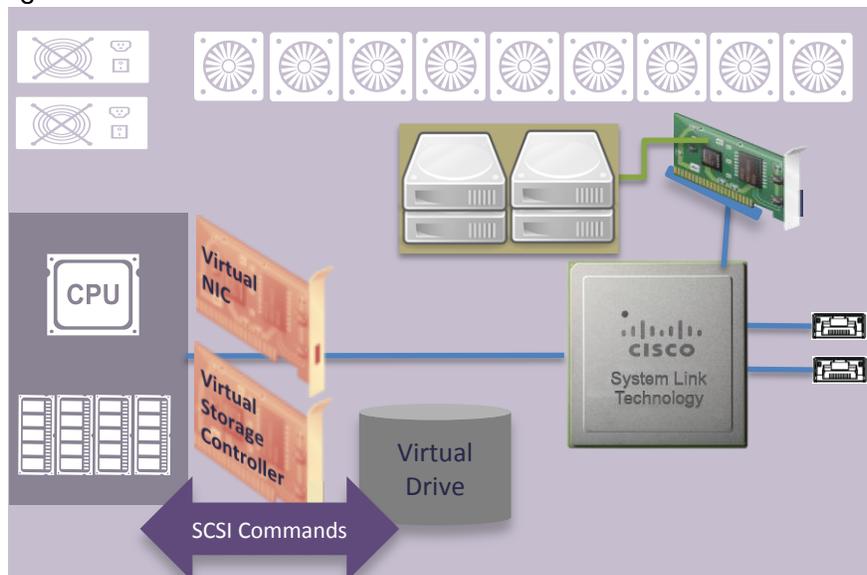
The Cisco UCS platform is built around the concept of a converged fabric that allows flexibility and scalability of re-sources. The foundation of the Cisco UCS converged architecture has always been the functionality provided by the Cisco UCS Virtual Interface Card (VIC) through a Cisco ASIC. The Cisco technology behind the VIC has been extended in the latest-generation ASIC to provide multiple PCIe buses that connect to multiple servers simultaneously. This third-generation Cisco ASIC provides the System Link Technology, which extends a PCIe bus to each of the servers, creating a virtual device on the PCIe host interface for use by the local CPU complex. The OS sees this as a local PCIe device, and I/O traffic is passed up the host

PCIe lanes to the ASIC. From there it is mapped to the appropriate shared resource—the local storage or the networking interface.

This overall technology is not new to Cisco UCS. In fact, it is core to the infrastructure flexibility provided in the Cisco UCS architecture. Those familiar with Cisco UCS know that the VIC allows administrators to configure the appropriate Ethernet or storage interfaces to be provided to the host OS. These are known as virtual network interface cards (vNICs) and virtual host bus adapters (vHBAs) within the construct of Cisco UCS Manager. To the OS, the vNIC and vHBA are seen as PCIe end devices, and the OS communicates with them as it would with any physical PCIe device.

Cisco UCS M-Series platforms continue to provide vNIC capabilities, but in addition the System Link Technology provides a new capability with its virtualized shared local storage. Figure 8 illustrates how the System Link Technology provides a virtual network interface and a virtual storage controller to the system for I/O.

Figure 8 Virtual I/O Devices



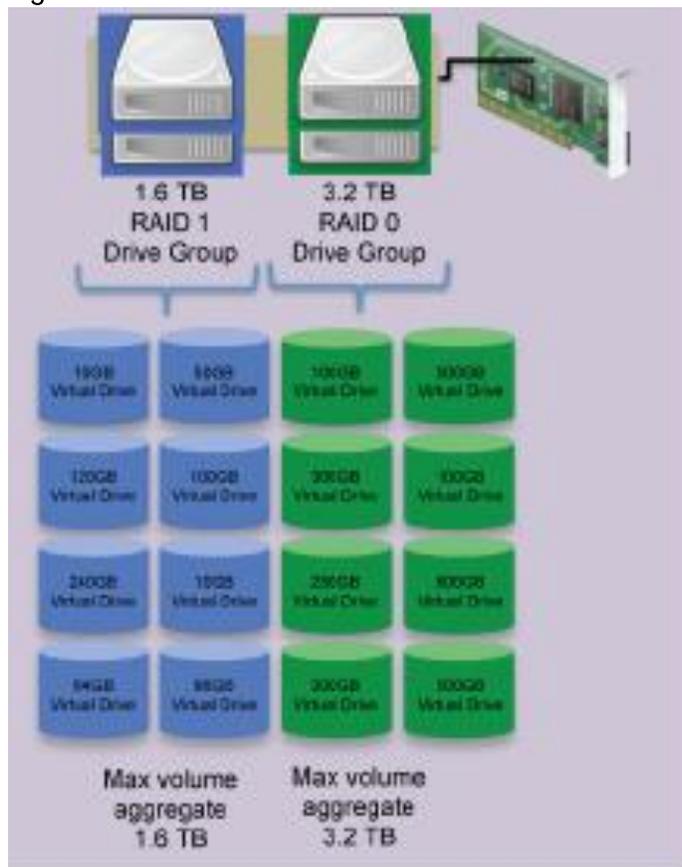
This virtual storage controller provides access to a virtual drive that is provided to the server via the shared storage controller and hard drives in the chassis. The virtual storage controller introduces a new PCIe device, known as a SCSI NIC (sNIC), that will be presented to the OS. The OS will view these items as locally attached SCSI devices.

Virtualized Shared Local Storage

The shared local storage is enabled through two major components. At the server level is the sNIC, which is the virtualized storage controller. At the chassis level is the physical storage controller. These two components are tightly integrated to provide each server with a virtual drive that will be referred to as a logical unit number (LUN) within the Cisco UCS Manager management structure and referenced as a virtual drive by the controller. Virtual drives can be carved out of a RAID drive group that is configured on the physical drives in the M-Series chassis. The Cisco UCS Manager allows for the centralized policy-based creation of this storage and their mapping to the service profiles. The virtual drives presented by these drive

groups will be available for consumption by servers installed in the chassis. Figure 9 illustrates the configuration of multiple drive groups and virtual drives within the shared storage resource.

Figure 9 Virtual Drives in the Cisco UCS M-Series



The construct starts with the introduction of a drive group policy within the service profile. The drive group defines the number of drives, the RAID type, and striping, write-back characteristics, etc. Within a chassis you can have a single or multiple drive groups, depending on how you would like the protection and performance needs of the virtual drive to be presented to the OS. In this example we are splitting the four available solid-state drives (SSDs) in the Cisco UCS M-Series chassis into two drive groups. The first drive group is RAID 1 so that we have protection in the event of a drive failure. This group could be used for boot disk or other data that needs to be protected. The second drive group will be a RAID 0 group to provide maximum space and performance for the virtual drives. In this example this group could be a workspace required by the application. The key takeaway here is that the system provides flexibility in the types of protection and the read/write characteristics of the data that is presented to the server.

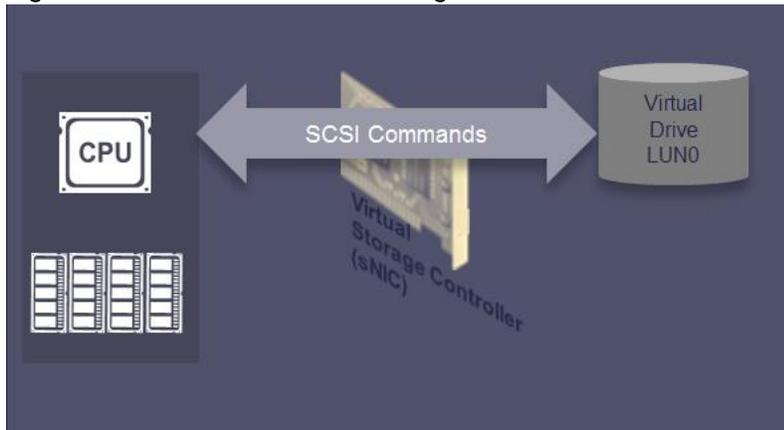
Initially, the controller will support a configuration of up to 64 virtual drives; these can be presented to the servers within that chassis. A server can be configured with multiple virtual drives based on the needs of the application. The virtual drive instantiation and binding is a function of the service profile within Cisco UCS Manager. When creating a server, administrators will create and assign the virtual drive to the server by creating a storage LUN for that service profile and selecting a drive group where it will be created. As long as that drive group exists (or can be created by the Cisco UCS Manager process), and there is enough available space, the virtual drive will be created on the chassis and linked to the service profile. When the

virtual drive is created and assigned to a server via a service profile, it will be accessible only by the physical server that is bound to that service profile. These assignments are kept segmented by the PCIe lane mappings within the fabric and not through a shared broadcast medium.

Virtualized Storage Controller

The virtualized storage controller, or sNIC, is a PCIe device presented to the OS. As shown in Figure 9, it is this device that provides the pathway for SCSI commands from the server to the virtual drive. This controller is a new device to the OS and will use a sNIC driver that will be loaded into the OS. Being a new PCIe device, the sNIC driver will not be part of some OS distributions. When that is the case, the sNIC driver will have to be loaded at the time of installation in order to see the storage device on the server. This driver, like the eNIC and fNIC drivers, will be certified by the OS vendor and eventually included as part of the core OS install package. When the driver is present, the virtual drive will be visible to the OS and is presented as a standard hard drive connected through a RAID controller. The driver does not alter the SCSI command set as it is sent to the controller, but instead provides a method for presenting the storage controller to the OS and the appropriate framing to carry the commands to the controller.

Figure 10 sNIC as a Virtual Storage Controller

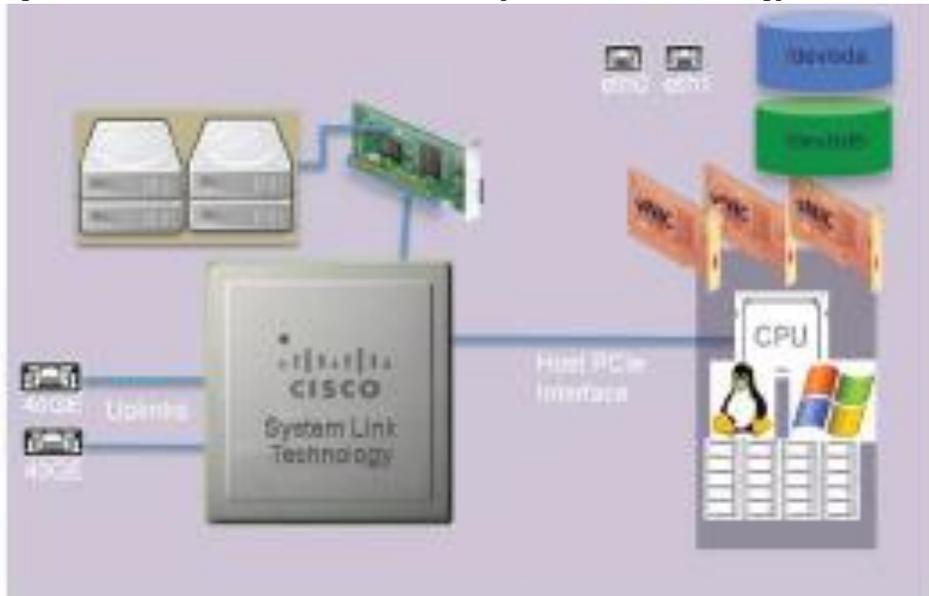


Building the Complete Server through System Link Technology

The Cisco UCS platform is built around the concept of a converged fabric that allows flexibility and scalability of re-sources. The foundation of this architecture has always been the Cisco ASIC technology within the virtual interface cards. The cornerstone of the M-Series platform is a third-generation ASIC based on this same innovative technology. This ASIC enables the System Link Technology that presents the vNIC (Ethernet interfaces) and the sNIC (storage controller) to the OS as a dedicated PCIe device for that server. In addition to presenting these PCIe de-vices to the OS, the System Link Technology provides a method for mapping the vNIC to a specific uplink port from the chassis. It also provides quality-of-service (QoS) policy, rate-limiting policy, and VLAN mappings. For the sNIC, the System Link Technology provides a mapping of virtual drive resources on a chassis storage controller drive group to a specific server. This is the core technology that provides flexible resource sharing and configuration in the Cisco UCS M-Series server.

The System Link Technology is based on standard PCIe functionality. Figure 11 shows the three major components of the PCIe connection.

Figure 11 PCIe Architecture of Cisco System Link Technology



First is a PCIe root complex that connects to the storage controller, which is a PCIe endpoint. Next, each server is connected to the PCIe infrastructure via a host interface, which provides root access for the virtual PCIe devices (vNIC and sNIC) created on the ASIC for that server. The host interface consists of x2 PCIe Gen3 lanes for the first generation of servers. The System Link Technology and M-Series chassis were designed for flexibility and longevity, so the number of PCIe lanes available in a slot is not completely static. Two 40-Gbps uplinks provide network connectivity for the vNICs.

While this ASIC is capable of PCIe single-root I/O virtualization (SR-IOV), that functionality is not in play on these servers, as shown in Figure 11. The key to Cisco interface virtualization technology, as it has been since the first generation, is that the vNIC and sNIC are represented as PCIe physical functions (devices), not virtual functions (devices) created on the PCIe tree for the individual server. This allows the OS to see each vNIC as a uniquely configurable and manageable Ethernet interface and each storage controller as a specific device capable of communicating with mapped virtual drives within the infrastructure. In contrast, SR-IOV devices are virtual functions (devices) within a physical function (device). A virtual function is not a full-featured resource, as it relies on the physical function for all configuration resources. An SR-IOV device also requires software support in the OS.

Within Cisco virtualization technologies, the sNIC and vNIC are presented to the OS as fully configurable physical functions that require no SR-IOV support.

While not as obvious in Figure 11, it is important to note that System Link Technology does not incorporate PCIe multi-root I/O virtualization (MR-IOV) to provide the servers access to the shared resource of the RAID controller.

MR-IOV is an emerging technology that allows root complexes from multiple hosts to share PCIe endpoint devices. With the System Link Technology, this is not necessary, because both the sNIC and the controller are part of the same fabric. From the perspective of the storage controller, all I/O requests to the virtual drive are coming from a single host, the system ASIC. The ASIC, in turn, is translating and mapping requests from the individual sNICs, which also exist in the ASIC, to the virtual drives presented by the controller. This means that there is no requirement by the controller or the OS to support MR-IOV functionality. System Link

Technology is the foundational building block of Cisco UCS M-Series and provides a seamless method for disaggregating and sharing resources across all of the compute nodes (servers) within the chassis.

Citrix XenApp 7.6

Enterprise IT organizations are tasked with the challenge of provisioning Microsoft Windows apps and desktops while managing cost, centralizing control, and enforcing corporate security policy. Deploying Windows apps to users in any location, regardless of the device type and available network bandwidth, **enables a mobile workforce that can improve productivity. With Citrix XenApp™ 7.6, IT can effectively** control app and desktop provisioning while securing data assets and lowering capital and operating expenses.

Citrix Provisioning Services 7.6

Most enterprises struggle to keep up with the proliferation and management of computers in their environments. Each computer, whether it is a desktop PC, a server in a data center, or a kiosk-type device, must be managed as an individual entity. The benefits of distributed processing come at the cost of distributed management. It costs time and money to set up, update, support, and ultimately decommission each computer. The initial cost of the machine is often dwarfed by operating costs.

Citrix PVS takes a very different approach from traditional imaging solutions by fundamentally changing the relationship between hardware and the software that runs on it. By streaming a single shared disk image (vDisk) rather than copying images to individual machines, PVS enables organizations to reduce the number of disk images that they manage, even as the number of machines continues to grow, simultaneously providing the efficiency of centralized management and the benefits of distributed processing.

In addition, because machines are streaming disk data dynamically and in real time from a single shared image, machine image consistency is essentially ensured. At the same time, the configuration, applications, and even the OS of large pools of machines can be completely changed in the time it takes the machines to reboot.

Using PVS, any vDisk can be configured in standard-image mode. A vDisk in standard-image mode allows many computers to boot from it simultaneously, greatly reducing the number of images that must be maintained and the amount of storage that is required. The vDisk is in read-only format, and the image cannot be changed by target devices.

These same benefits apply to vDisks that are streamed to bare metal servers, which is the way we utilized PVS in this study.

Citrix Desktop Studio for XenApp 7.6

If you manage a pool of servers that work as a farm, such as Citrix XenApp servers or web servers, maintaining a uniform patch level on your servers can be difficult and time consuming. With traditional imaging solutions, you start with a clean golden master image, but as soon as a server is built with the master image, you must patch that individual server along with all the other individual servers. Rolling out patches to individual servers in your farm is not only inefficient, but the results can also be unreliable. Patches often fail on an individual server, and you may not realize you have a problem until users start complaining or the server has an outage. After that happens, getting the server resynchronized with the rest of the farm can be challenging, and sometimes a full reimaging of the machine is required.

With Citrix PVS, patch management for server farms is simple and reliable. You start by managing your golden image, and you continue to manage that single golden image. All patching is performed in one place and then streamed to your servers when they boot. Server build consistency is assured because all your servers use a single shared copy of the disk image. If a server becomes corrupted, simply reboot it, and it is instantly back to the known good state of your master image. Upgrades are extremely fast to implement. After you have your updated image ready for production, you simply assign the new image version to the servers and reboot them. You can deploy the new image to any number of servers in the time it takes them to reboot. Just as important, rollback can be performed in the same way, so problems with new images do not need to take your servers or your users out of commission for an extended period of time.

Benefits for Desktop Administrators

Since **Citrix PVS is part of Citrix XenApp, desktop administrators can use PVS's streaming technology** to simplify, consolidate, and reduce the costs of both physical and virtual desktop delivery. Many organizations **are beginning to explore desktop virtualization. Although virtualization addresses many of IT's needs for consolidation and simplified management,** deploying it also requires deployment of supporting infrastructure. Without PVS, storage costs can make desktop virtualization too costly for the IT budget. However, with PVS, IT can reduce the amount of storage required for VDI by as much as 90 percent. And with a single image to manage instead of hundreds or thousands of desktops, PVS significantly reduces the cost, effort, and complexity for desktop administration.

Different types of workers across the enterprise need different types of desktops. Some require simplicity and standardization, and others require high performance and personalization. XenApp can meet these requirements in a single solution using Citrix FlexCast delivery technology. With FlexCast, IT can deliver every type of virtual desktop, each specifically tailored to meet the performance, security, and flexibility requirements of each individual user.

Not all desktops applications can be supported by virtual desktops. For these scenarios, IT can still reap the benefits of consolidation and single-image management. Desktop images are stored and managed centrally in the data center and streamed to physical desktops on demand. This model works particularly well for standardized desktops such as those in lab and training environments and call centers and thin-client devices used to access virtual desktops.

Citrix Provisioning Services Solution

Citrix PVS streaming technology allows computers to be provisioned and re-provisioned in real time from a single shared disk image. With this approach, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is performed on the master image. The local hard drive of each system can be used for runtime data caching or, in some scenarios, removed from the system entirely, which reduces power use, system failure rate, and security risk.

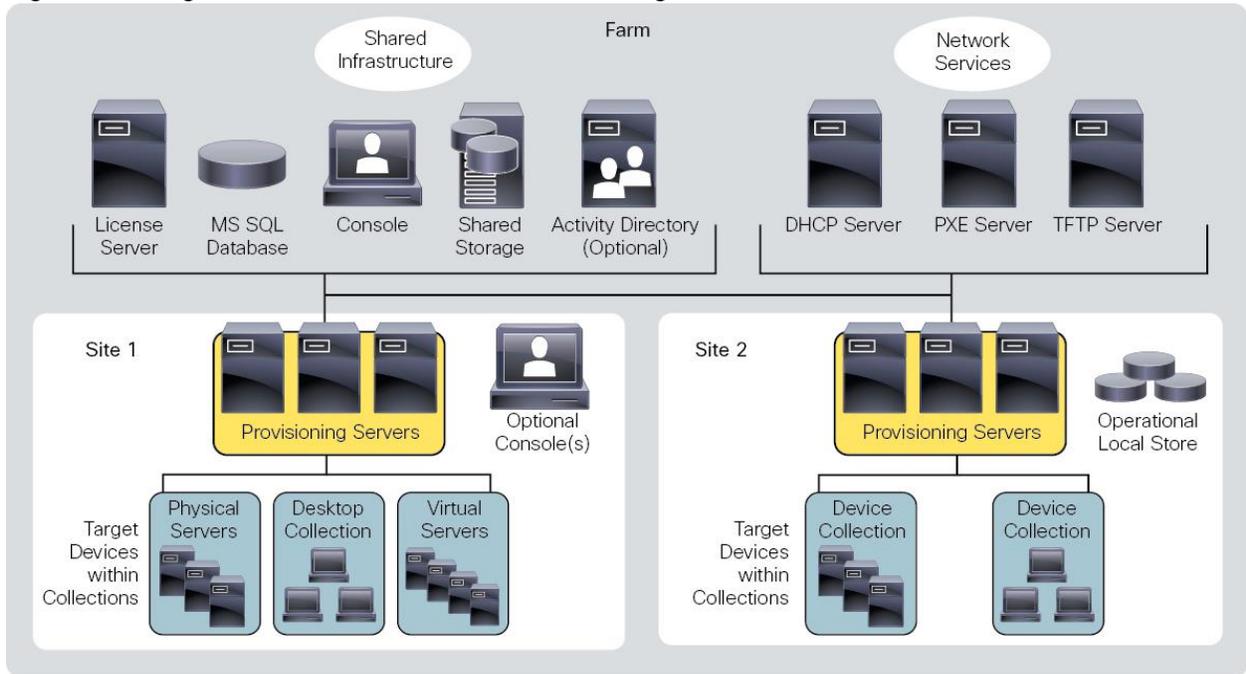
The PVS solution's infrastructure is based on software-streaming technology. After PVS components are installed and configured, **a vDisk is created from a device's hard drive by** taking a snapshot of the OS and application image and then storing that image as a vDisk file on the network. A device used for this process is referred to as a master target device. The devices that use the vDisks are called target devices. vDisks can exist on a PVS, file share, or in larger deployments, on a storage system with which PVS can communicate (iSCSI, SAN, network-attached storage [NAS], and Common Internet File System [CIFS]). vDisks can be assigned to a single target device in private-image mode, or to multiple target devices in standard-image mode.

Citrix Provisioning Services Infrastructure

The Citrix PVS infrastructure design directly relates to administrative roles within a PVS farm. The PVS administrator role determines which components that administrator can manage or view in the console.

A PVS farm contains several components. Figure 12 provides a high-level view of a basic PVS infrastructure and shows how PVS components might appear within that implementation.

Figure 12 Logical Architecture of Citrix Provisioning Services



Architecture

Figure 13 Physical Topology

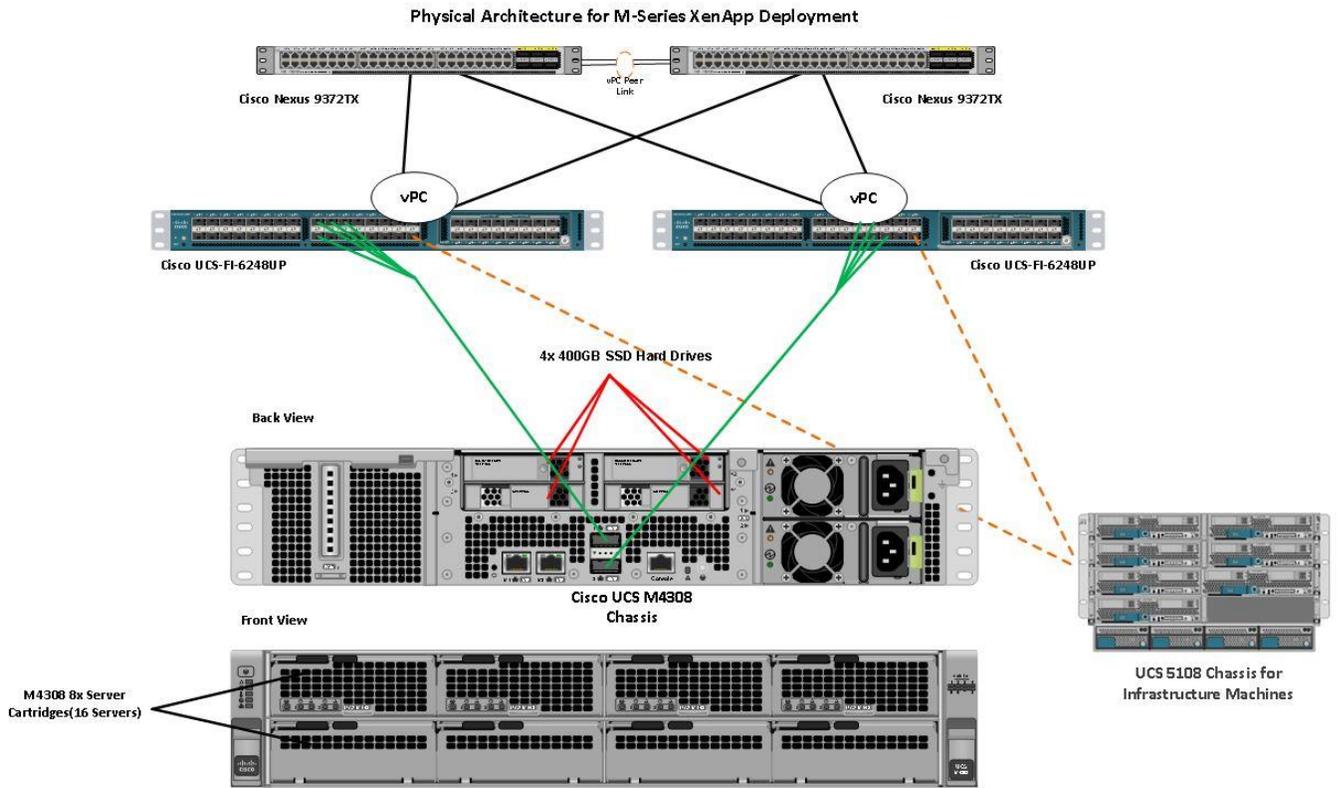
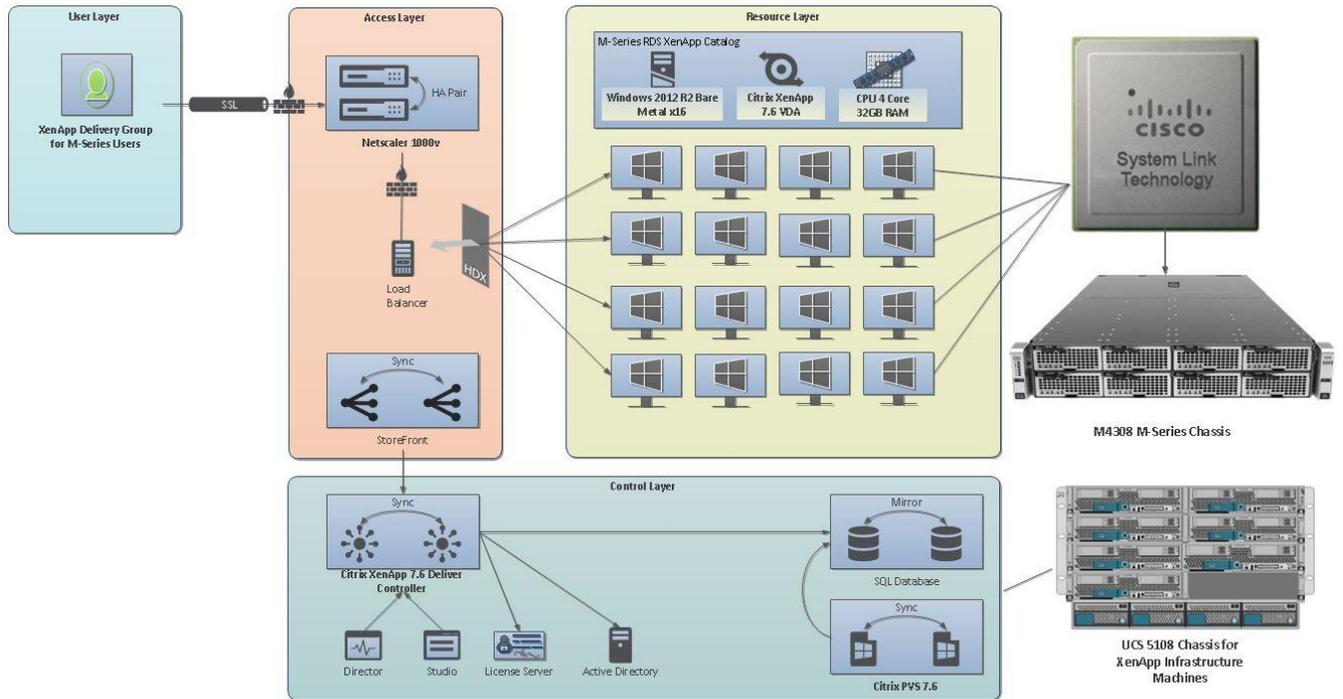


Figure 14 Logical Topology



Deployment Hardware and Software

Hardware Deployed

The architecture deployed is highly modular. While each customer's environment might vary in its exact configuration, once the reference architecture contained in this document is built, it can easily be scaled as requirements and demands change.

The solution includes Cisco networking and Cisco UCS, which efficiently fits into a single data center rack, including the access layer network switches.

This validated design document details the deployment of the hardware configurations extending up to 960 users for a XenApp workload.

The hardware deployed in this solution includes the following:

- Two Cisco Nexus 9372 Layer 2 Access Switches
- Two Cisco UCS 6248UP Fabric Interconnects
- One Cisco UCS M4308 Modular Server Chassis
- Eight Cisco UCS M142-M4 Cartridges with a total of 16 compute nodes.
- Each compute nodes contain a single Intel Xeon E3-1275L 2.7 GHz Quad-Core processor, 32GB RAM 1600MHz.

The software components deployed in this solution includes the following:

- Citrix XenApp Hosted Shared Desktops (RDS) with PVS write cache on local storage in the chassis
- Citrix Provisioning Server
- Citrix XenApp
- Citrix User Profile Manager
- Citrix StoreFront
- Microsoft Windows Server 2012 R2
- Microsoft SQL Server 2012

Table 1 Software Revisions

Software	Version
UCSM Firmware	2.5(2a)
Windows Server	2012 R2
Citrix XenApp	7.6

Software	Version
Citrix Provisioning Services	7.6
Citrix Storefront	3.0
Citrix User Profile Manager	5.2.1
Login VSI	4.1.4

Configuration Guidelines



This document is intended to allow the reader to configure the M-Series XenApp solution to be added to an existing infrastructure including Active Directory, DNS, DHCP, Citrix StoreFront, Provisioning Services, File Servers for user profile data, Licensing and XenApp Delivery Controllers.

Base Cisco UCS System Configuration

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

1. Bring up the Fabric Interconnect (FI) and from a serial console connection set the IP address, gateway, and the hostname of the primary fabric interconnect. Now bring up the second fabric interconnect after connecting the dual cables between them. The second fabric interconnect automatically recognizes the primary and ask if you want to be part of the cluster, answer yes and set the IP address, gateway and the hostname. Once this is done all access to the FI can be done remotely. You will also configure the virtual IP address to connect to the FI, you need a total of three IP address to bring it online. You can also wire up the chassis to the FI, using either 1, 2, 4 or 8 links per IO Module, depending on your application bandwidth requirement. We connected four links to each module.
2. Connect using your favorite browser to the Virtual IP and launch the Cisco UCS Manager (UCSM). The Java based UCSM will let you do everything that you could do from the CLI. We will highlight the GUI methodology.
3. First check the firmware on the system and see if it is current. Visit: [Download Software for Cisco UCS Infrastructure and Cisco UCS Manager Software](#) 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 2.5.2a.

Name	Type	State	Vendor
ucs-k9-bundle-infra.2.5.1a.A.bin	Infrastructure Bundle	Active	2.5(1a)A
ucs-k9-bundle-infra.2.5.1b.A.bin	Infrastructure Bundle	Active	2.5(1b)A
ucs-k9-bundle-infra.2.5.2a.A.bin	Infrastructure Bundle	Active	2.5(2a)A
ucs-k9-bundle-m-series.2.5.1a.M.bin	M Series Bundle	Active	2.5(1a)M
ucs-k9-bundle-m-series.2.5.1b.M.bin	M Series Bundle	Active	2.5(1b)M
ucs-k9-bundle-m-series.2.5.2a.M.bin	M Series Bundle	Active	2.5(2a)M

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.
5. To enable server and uplink ports, complete the following steps:
 - a. In Cisco UCS Manager, in the navigation pane, click the Equipment tab.
 - b. Select Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module.
 - c. Expand Ethernet Ports.
 - d. Select ports 1 through 4 that are connected to the Cisco Nexus 9372 switches, right-click them, and select Configure as Uplink Port.
 - e. Click Yes to confirm uplink ports and click OK.
 - f. In the left pane, navigate to Fabric Interconnect A. In the right pane, navigate to the Physical Ports tab > Ethernet Ports tab. Confirm that ports have been configured correctly in the If Role column.

Port	Port ID	MAC Address	Role	Physical	Uplink
Port 1	1	00:2A:6A:D9:04:A8	Server	Physical	Sfp Not Pres
Port 2	2	00:2A:6A:D9:04:A9	Server	Physical	Sfp Not Pres
Port 3	3	00:2A:6A:D9:04:AA	Server	Physical	Sfp Not Pres
Port 4	4	00:2A:6A:D9:04:AB	Server	Physical	Sfp Not Pres
Port 5	5	00:2A:6A:D9:04:AC	Server	Physical	Up
Port 6	6	00:2A:6A:D9:04:AD	Server	Physical	Up
Port 7	7	00:2A:6A:D9:04:AE	Server	Physical	Up
Port 8	8	00:2A:6A:D9:04:AF	Server	Physical	Up
Port 9	9	00:2A:6A:D9:04:B0	Server	Physical	Up
Port 10	10	00:2A:6A:D9:04:B1	Server	Physical	Up
Port 11	11	00:2A:6A:D9:04:B2	Server	Physical	Up
Port 12	12	00:2A:6A:D9:04:B3	Server	Physical	Up
Port 13	13	00:2A:6A:D9:04:B4	Unconfigured	Physical	Sfp Not Pres
Port 14	14	00:2A:6A:D9:04:B5	Unconfigured	Physical	Sfp Not Pres
Port 15	15	00:2A:6A:D9:04:B6	Unconfigured	Physical	Sfp Not Pres
Port 16	16	00:2A:6A:D9:04:B7	Unconfigured	Physical	Sfp Not Pres
Port 17	17	00:2A:6A:D9:04:B8	Unconfigured	Physical	Sfp Not Pres

6. Configure FI Server ports for uplink from the UCS M-Series Chassis.
7. Repeat the above steps for Fabric Interconnect B.

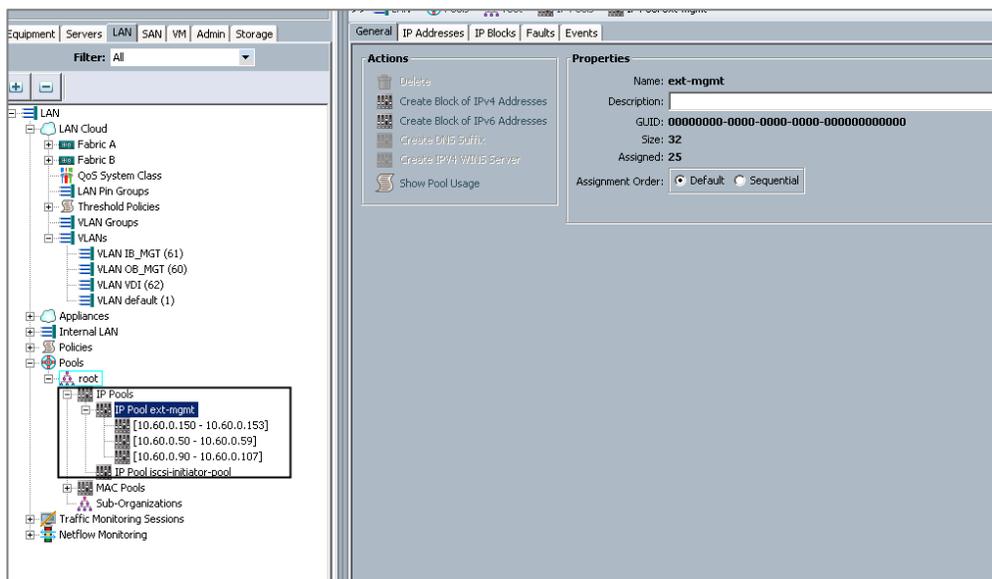
Add a Block of IP Addresses for Out-of-Band KVM Access

To create a block of IP addresses for server keyboard, video, mouse (KVM) access in the Cisco UCS environment, complete the following steps:

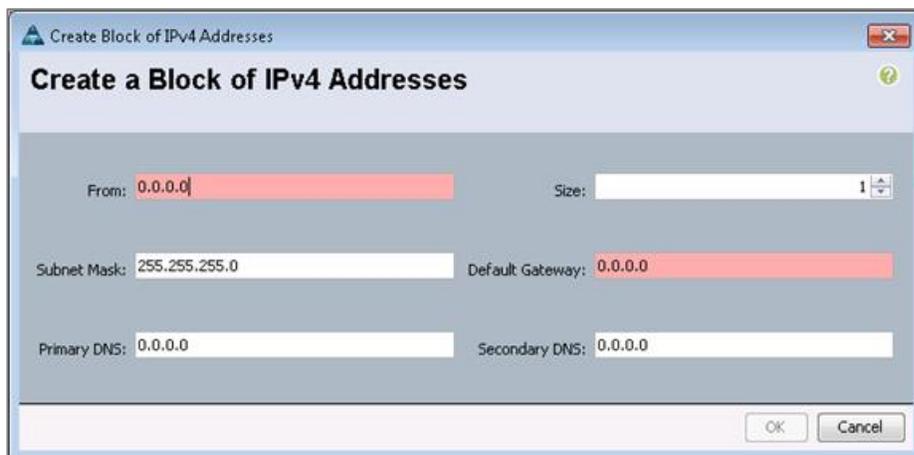


This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.

1. In Cisco UCS Manager, in the navigation pane, click the LAN tab.
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.

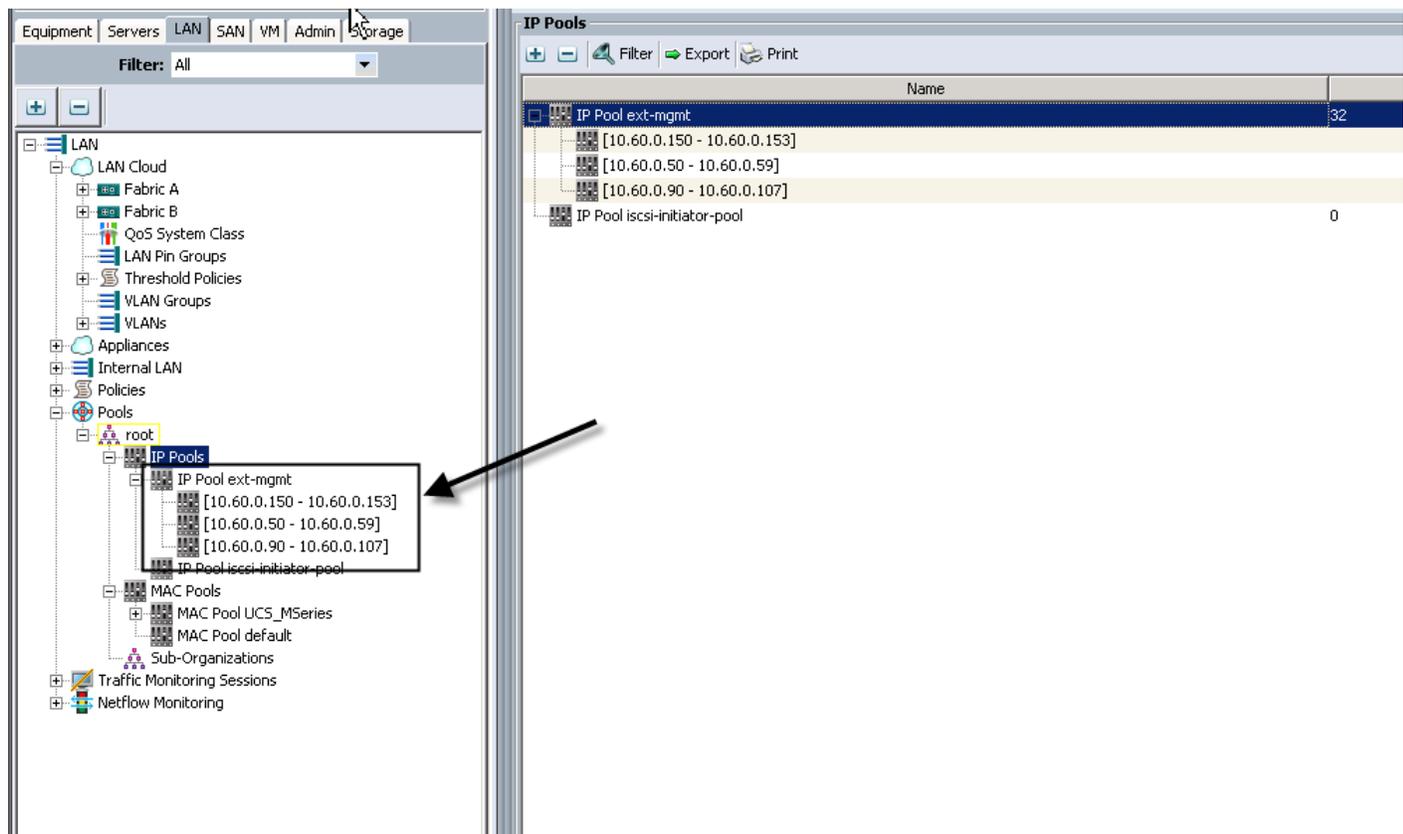


3. In the Actions pane, select Create Block of IP Addresses.
4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.



5. Click OK to create the IP block.

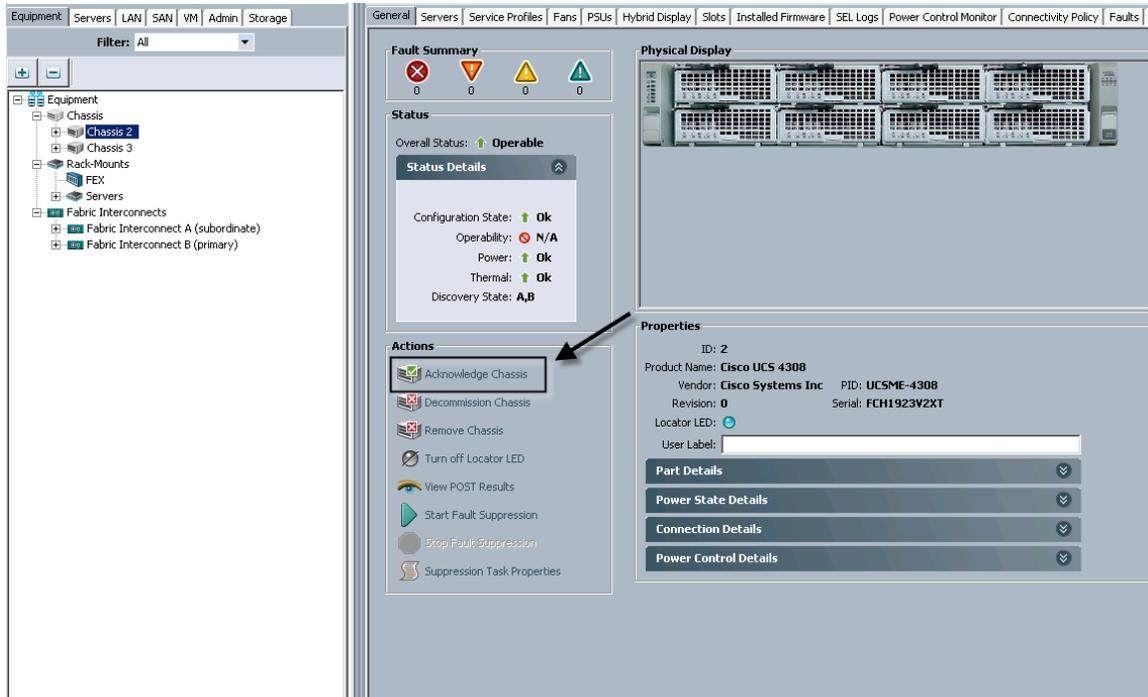
6. Click OK in the confirmation message.



Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the Equipment tab.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.



4. Click Yes and then click OK to complete acknowledging the chassis.
5. Create Resource Pools.
6. This section details how to create the MAC address, iSCSI IQN, iSCSI IP, UUID suffix and server pools.

Create MAC Address Pools

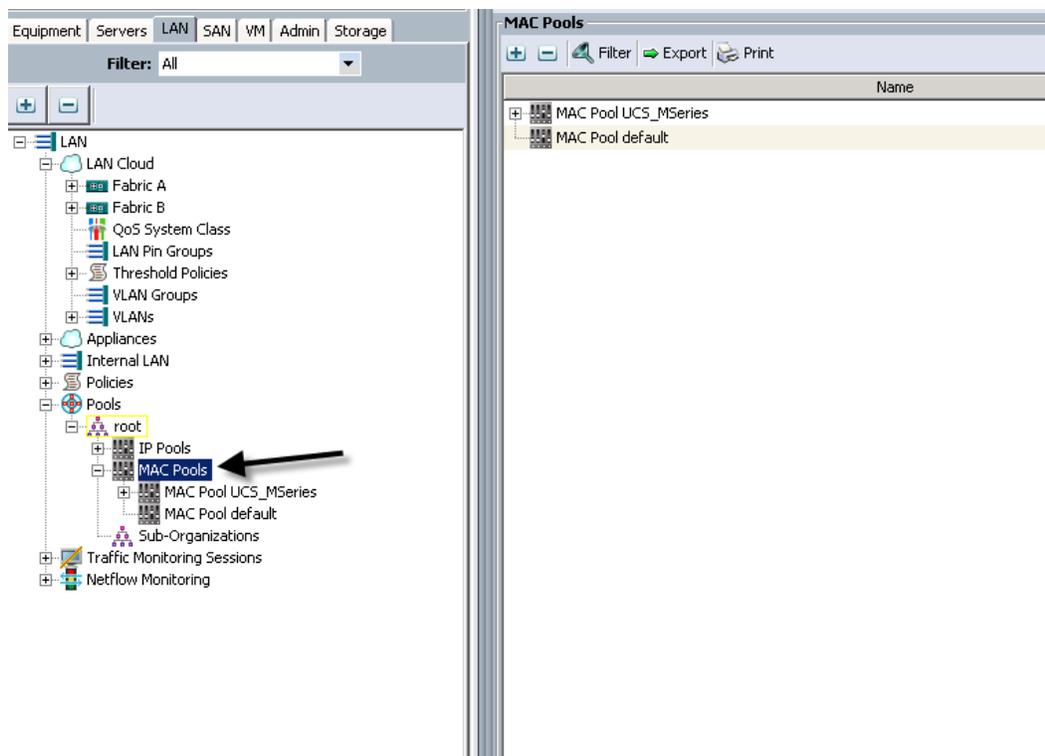
To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter UCS_MSeries_A as the name for MAC pool.
6. Optional: Enter a description for the MAC pool.



Keep the Assignment Order at Default.

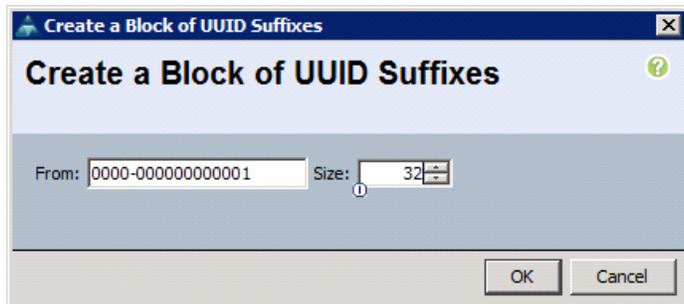
7. Click Next.



Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter UUID_Pool as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Click Next.
9. Click Add to add a block of UUIDs.
10. Keep the From field at the default setting.
11. Specify a size for the UUID block that is sufficient to support the available blade or server re-sources.



Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:



Consider creating unique server pools to achieve the granularity that is required in your environment.

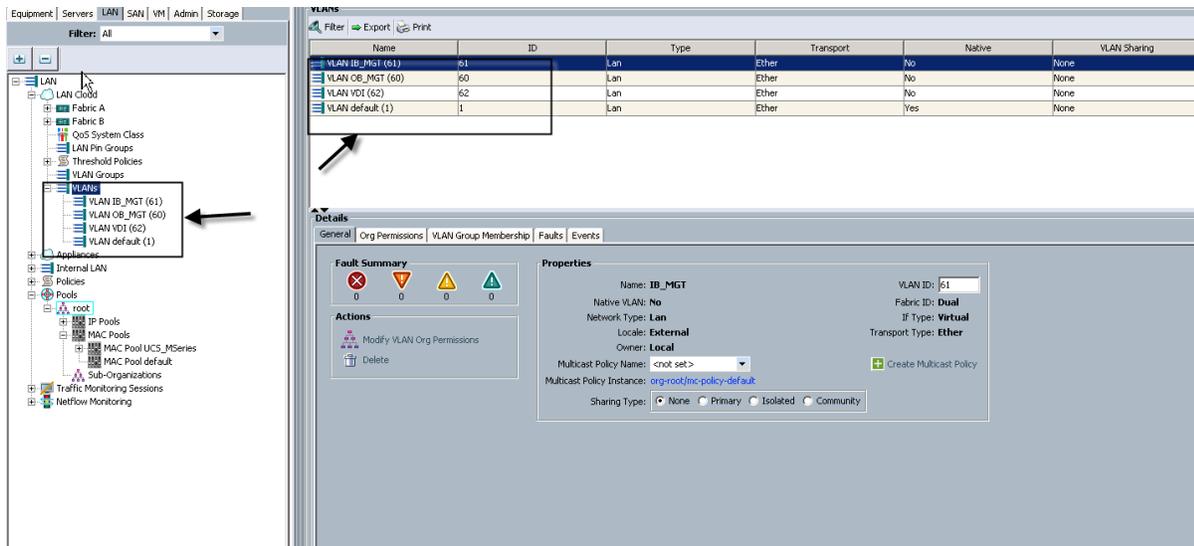
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter 'CH2-MSERIES' as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Click Finish.
9. Click OK.

Name	
Server Pool CH2-MSERIES	16
Server Pool CH3-M-Series	12
Server Pool UCS-MSeries	0
Server Pool default	0

Create VLANs

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter IB_MGMT as the name of the VLAN to be used for in-band management traffic.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter <<var_mgmt_id>> as the ID of the management VLAN.
8. Keep the Sharing Type as None.
9. Click OK, and then click OK again.



10. Repeat the above steps to create all VLANs and configure the Default VLAN as native.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter MSeries as the name of the host firmware package.
6. Leave Simple selected.
7. Select the version 2.5(2a) for both the Blade Package.
8. Click OK to create the host firmware package.

Create Host Firmware Package

Name:

Description:

How would you like to configure the Host Firmware Package? Simple Advanced

Blade Package:

Rack Package:

M-Series Package:

9. Server Pool Qual.

Name	Max	Model
UCS-MSeries-E3		
Processor qualification		UCS-CPU-E31275LD
all-chassis		
Chassis id range [1 - 40]		

10. Server Pool Policy.

Server Pool Policies

Name	
Server Pool Policy M-SERIES-POOL	org-root/compute-pool-UCS-
Server Pool Policy M-SERIES-POOL	org-root/compute-pool-UCS-

Create Server Pool Policy

Name: M-SERIES-POOL

Description:

Target Pool: Server Pool UCS-MSeries

Qualification: UCS-MSeries-E3

OK Cancel

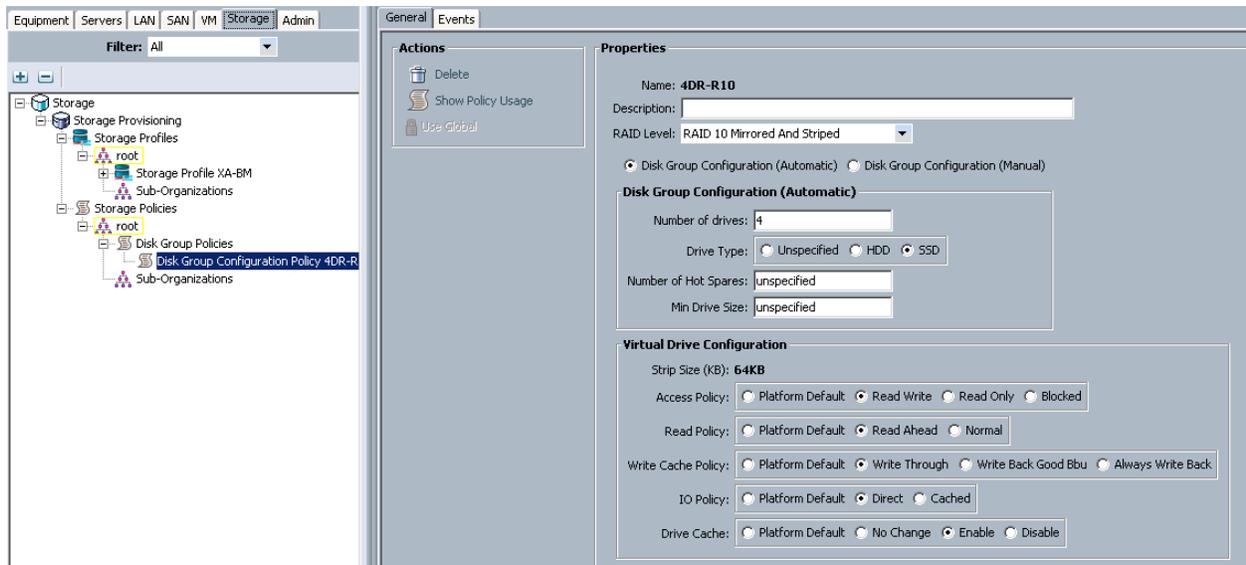
11. vNIC Templates for A and B.

vNIC Templates

Name	
vNIC Template MSeries-A	
Network VDI	VDI
vNIC Template MSeries-B	
Network VDI	VDI

Create Disk Group Policy

To configure the necessary Disk Groups to utilize the local hard disks in the chassis complete the following steps:



1. In Cisco UCS Manager, click the Storage tab in the navigation pane.
2. Select Storage Policies > root > Disk Group Policies.
3. Right-click Disk Group Policies.
4. Select Create Disk Group Policy.
5. Enter '4DR-R10' as the name of the disk group.
6. Optional: Enter a description for the disk group.
7. Select RAID Level 'RAID 10' Mirrored and Striped.
8. Under Number of Drives, enter '4'.
9. Select SSD radio button.
10. Leave next two fields as 'unspecified'.
11. Access Policy is 'Read Write'.
12. Read Policy is 'Read Ahead'.
13. Write Cache Policy is 'Write Through'.
14. IO policy is 'Direct'.

15. Drive Cache is 'Platform Default'.

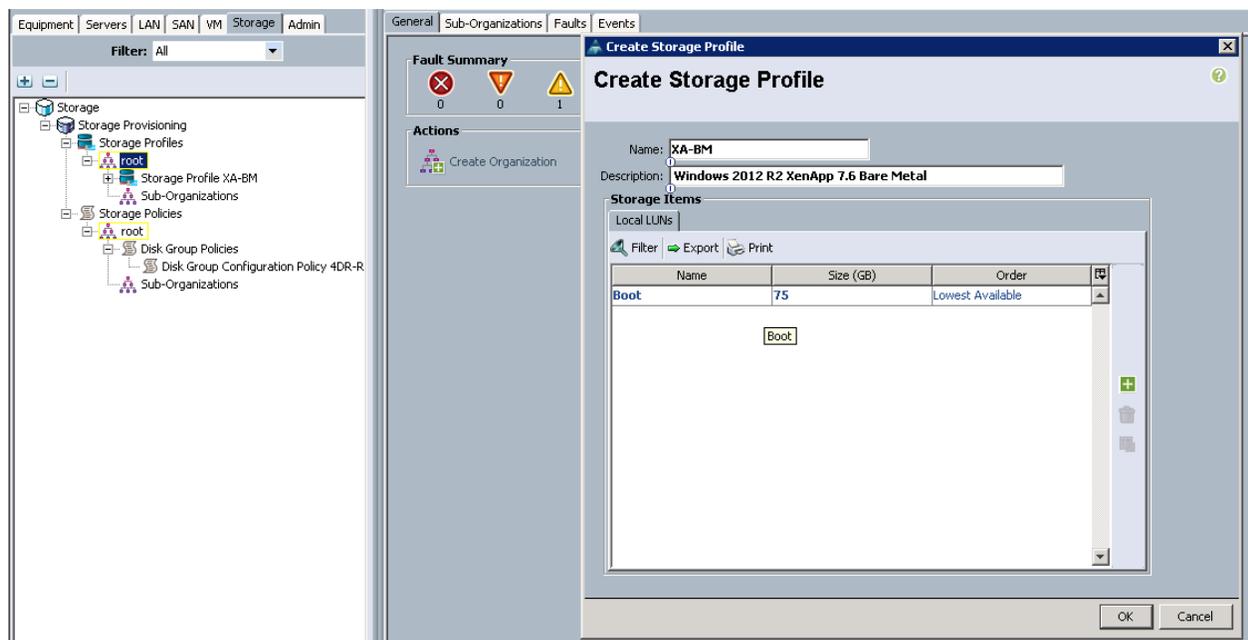
16. Click Next.

17. Click Finish.

18. Click OK.

Create Storage Profiles

To configure the necessary Storage Policy to define the LUNs that will use the Disk Groups created in the prior steps. Define the virtual disks that will be provisioned through the Service Profile Templates to the Cisco UCS Servers. These drives can be configured as boot drives or secondary drives. To create storage profiles, complete the following steps:



1. In Cisco UCS Manager, click the Storage tab in the navigation pane.
2. Select Storage Profiles > root.
3. Right-click Storage Profiles.
4. Select Create Storage Profile.
5. Enter XA-BM as the name of the Storage profile.
6. Optional: Enter a description.
7. Click the green '+' sign to create a Local LUN.

8. Enter the name of the LUN.
9. Enter LUN size in GB.
10. In 'Order' leave lowest-available.
11. Keep Auto-Deploy.
12. Select the Disk Group Policy created in the prior step from the drop-down.
13. Click OK.
14. Click OK.



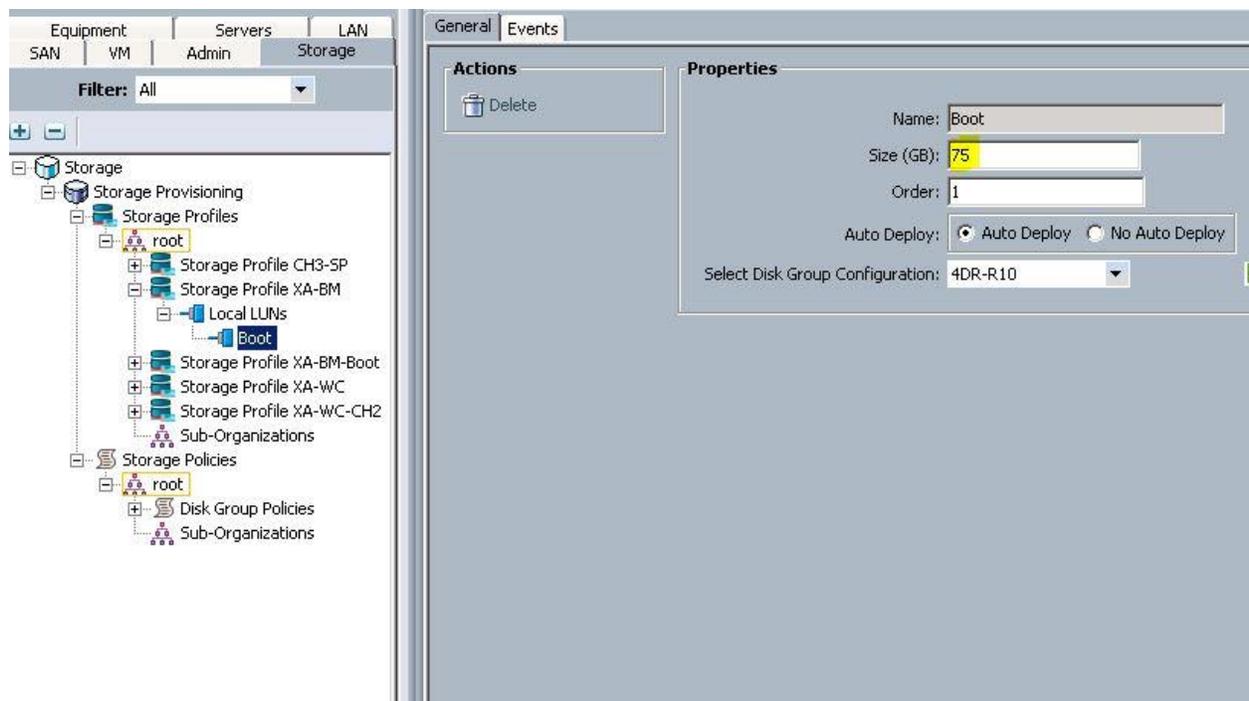
In this solution, we created an initial LUN that was bootable to install our master Windows 2012 R2 image on to be imaged with Citrix Provisioning Services 7.6. When we obtained the master image, the second policy created was for non-bootable LUNs specifically for Write Cache on the cartridge servers.

15. Create a second Storage Profile for the Citrix PVS Write Cache Drive using the same method above with a 40GB LUN.



This process will be demonstrated in the section "Configure Local Hard Disks for PVS Write Cache."

The screen shot below shows the Storage Profile with a configured boot LUN for the master imaging of the server.

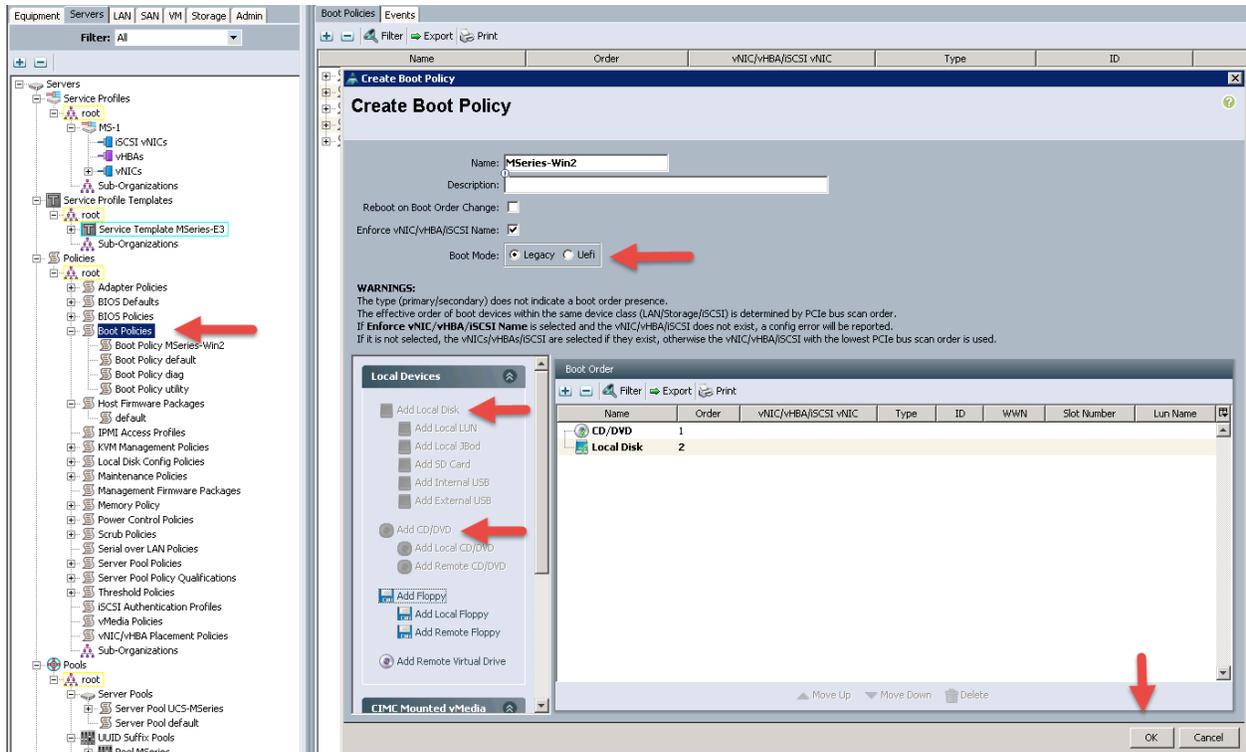


Create Boot Policies

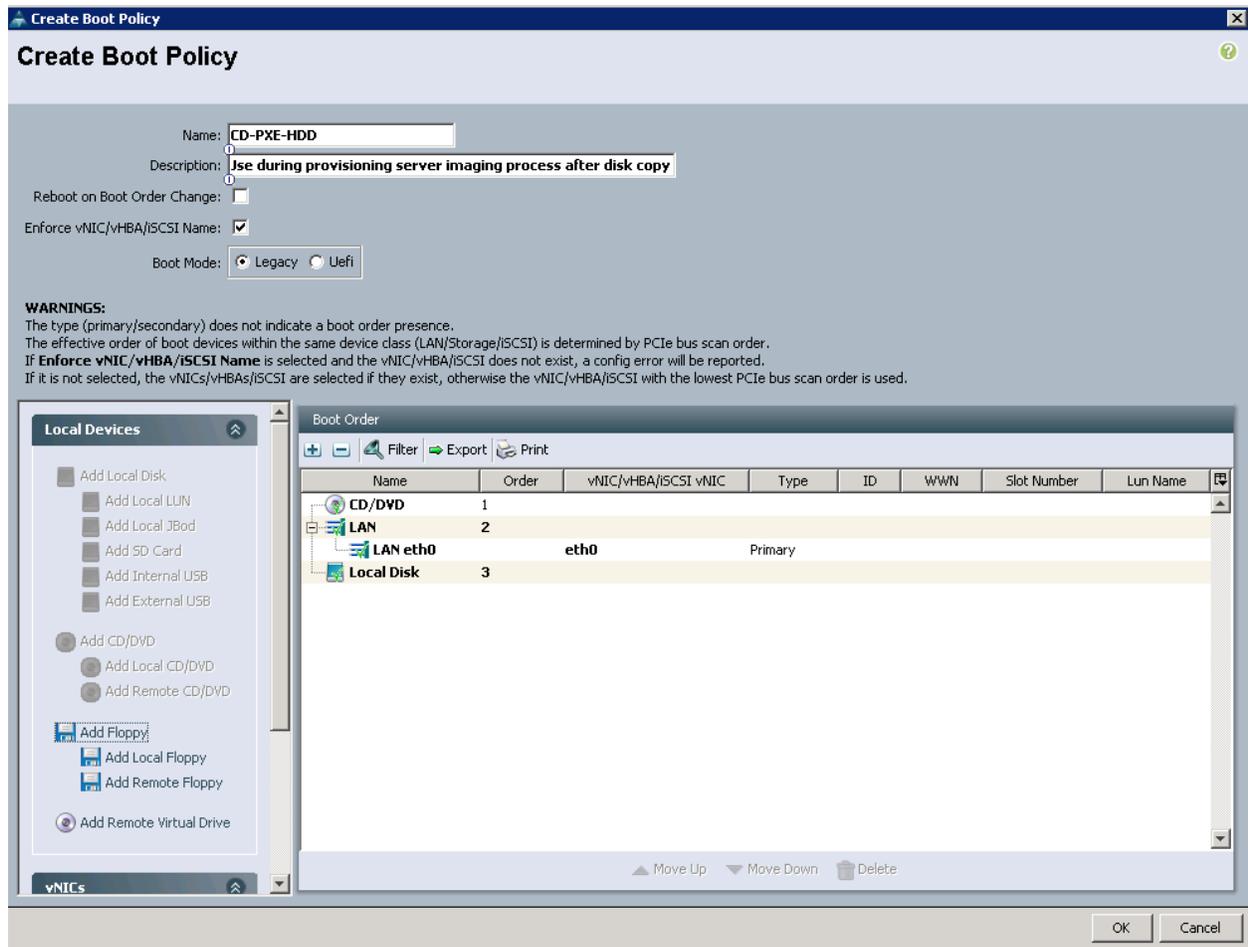
You will need a total of three boot policies when you are setting up your master image and then converting to PVS Boot:

- MSeries-Win2: Allows a bare metal install of Windows 2012 R2 and all other required components
- CD-PXE-HDD: After PVS disk copy is complete, the server connects to PVS, then boots to the hard disk drive, creates a snapshot and seals the image.
- PXE Boot: This policy includes a CD-ROM in case you need it, but boots exclusively from PXE.

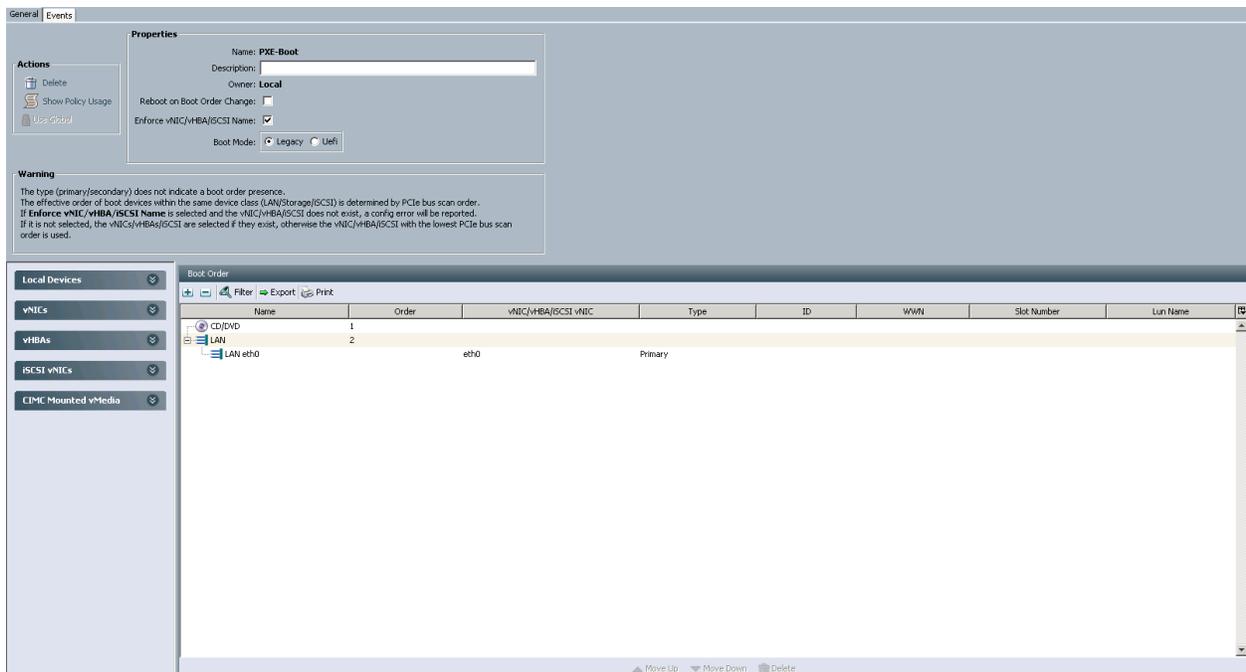
To create the bare metal MSeries-Win2 policy, complete the following steps:



1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > Boot Policies.
3. Right-click Boot Policies.
4. Name the Policy accordingly.
5. **Boot Mode (for boot LUNs) Select 'Legacy' radio button.**
6. For the first boot device select CD/DVD.
7. For the second device select Local Disk.
8. For the second policy, use the following settings:



- Next, our second policy will have CD/DVD, LAN/PXE, then Local Disk to allow for the Citrix PVS imaging software to take the master image.
- For the third boot policy, we will setup the PXE only PVS bare metal boot.



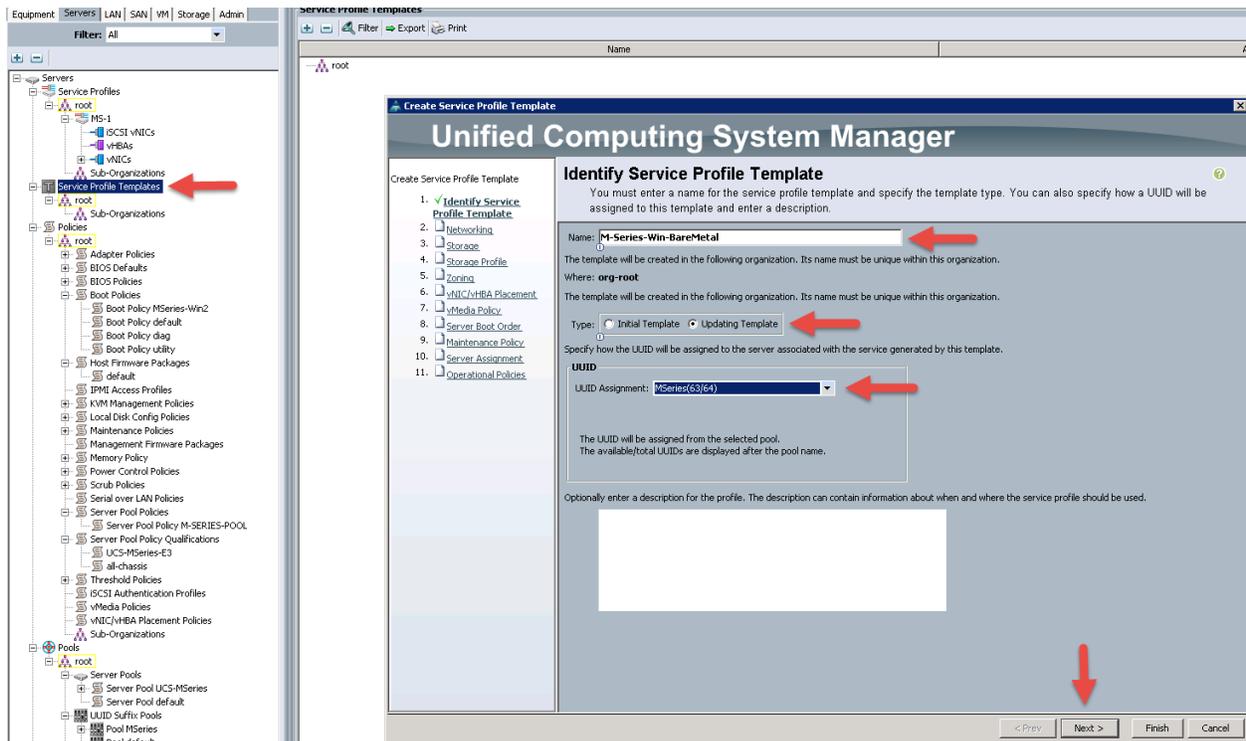
11. The final boot policy will only include LAN/PXE options to boot the cartridges from the Citrix PVS 7.6 master images and there will be a non-bootable LUN for local write cache.

Create Service Profile Template

To configure the necessary Service Profile Template to utilize the local resources in the chassis, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template.
5. Enter **'M-Series-PVS-WC-CH3'** as the name of the Svc Profile Template.
6. Select **'Updating Template'** radio button.
7. Select UUID Pool created earlier.
8. Click Next.
9. On the Networking page, select **'Use Connectivity Policy'** create earlier.
10. On the Storage page, select **'No vHBAs'** to bypass Storage config.
11. On the Storage Profile page, select the **'Storage Profile Policy'** tab and select the Storage Profile created in an earlier step from the drop-down menu.

12. Click Next on Zoning to bypass configuration.
13. Click Next to accept defaults on the vNIC Placement and vMedia Policy pages.
14. In the Server Boot Order tab, select the Boot Order Policies that we created earlier that match up with the task you are completing. I.e. If doing the initial install, select MSeries-Win2. If running the Citrix PVS Imaging Wizard, Select the CD-PXE-HDD, and finally if all initial imaging tasks are completed and you are ready to run your XenApp workloads, select PXE-Boot.
15. Alternatively, you can use the SP Wizard to Create a SP Template for the nodes in the chassis as shown in the screen shots below:



Service Profile Templates

Unified Computing System Manager

Create Service Profile Template

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

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default) Create Dynamic vNIC Connection Policy

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

LAN Connectivity Policy: MSeries_LAN Create LAN Connectivity Policy

Initiator Name
Initiator Name Assignment: cnot_set

Create iQN Suffix Pool
WARNING: The selected pool does not contain any available entries. You can select it, but it is recommended that you add entries to it.

< Prev Next > Finish Cancel

Service Profile Templates

Unified Computing System Manager

Create Service Profile Template

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

Select a local disk configuration policy.

Local Storage: Select Local Storage Policy to use Create Local Disk Configuration Policy

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

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

This server associated with this service profile will not be connected to a storage area network.

< Prev Next > Finish Cancel

Unified Computing System Manager

Create Service Profile Template

- Identify Service Profile Template
- Networking
- Storage
- Storage Profile
- Zoning
- vNIC/vHBA Placement
- vMedia Policy
- Server Boot Order
- Maintenance Policy
- Server Assignment
- Operational Policies

Storage Profile

Optionally specify or create a Storage Profile.

Specific Storage Profile: Storage Profile Policy

Storage Profile: XA-BM

Name: XA-BM

Description: XenApp 7.6 on Windows 2012 R2 Bare Metal

Storage Items

Name	Size (GB)	Order
Boot	75	1

< Prev Next > Finish Cancel



No configuration is required for the Zoning, vNIC/vHBA Placement or the vMedia nodes of the Wizard.

Unified Computing System Manager

Create Service Profile Template

- Identify Service Profile Template
- Networking
- Storage
- Storage Profile
- Zoning
- vNIC/vHBA Placement
- vMedia Policy
- Server Boot Order
- Maintenance Policy
- Server Assignment
- Operational Policies

Server Boot Order

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: MSeries-Win2

Name: MSeries-Win2

Description:

Reboot on Boot Order Change: No

Enforce vNIC/vHBA/iSCSI Name: Yes

Boot Mode: Legacy

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

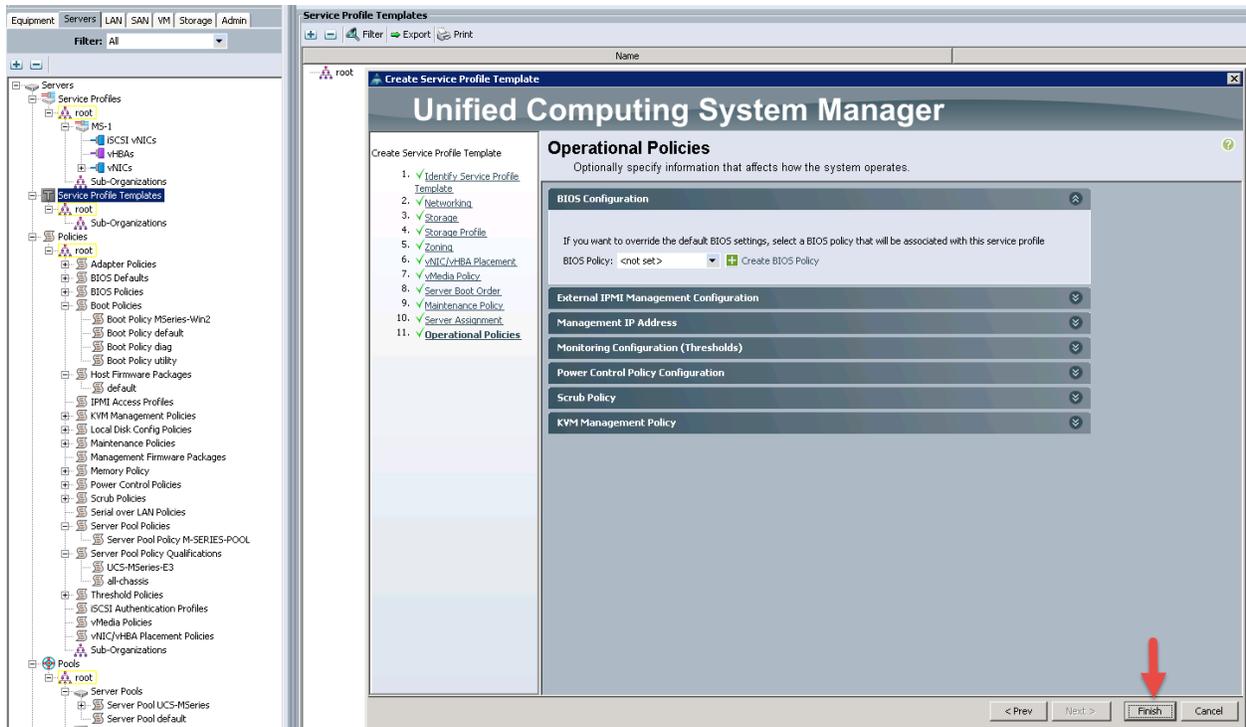
Boot Order

Name	Order	vNIC/vHBA/iSCSI	Type	ID	WWN	Slot Number	Lun Name
CD/DVD	1						
Local Disk	2						

< Prev Next > Finish Cancel



No configuration is required for the Maintenance Policy, Server Assignment or Operational Policies nodes of the wizard to get a basic SP template.



16. Create the appropriate number of SPs from the template per normal operating method.

Citrix Infrastructure Configuration

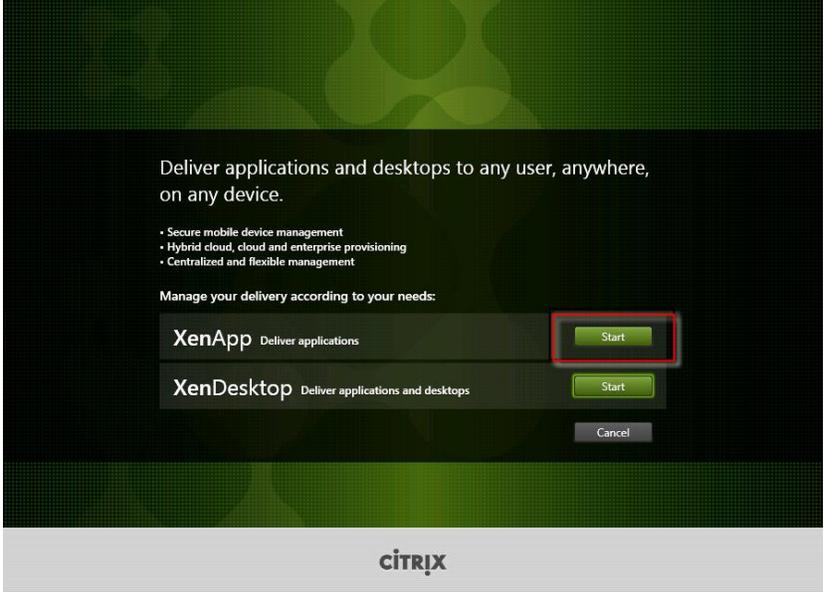
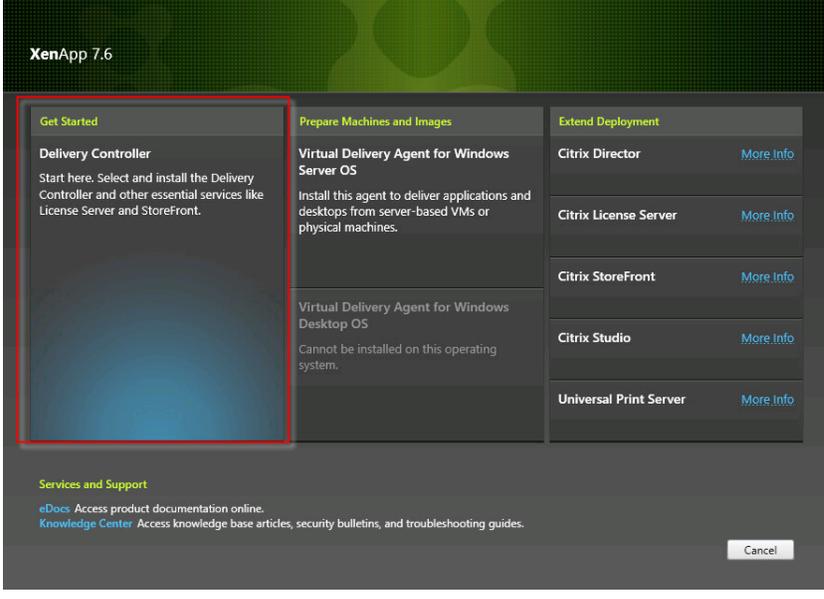
Each Citrix Infrastructure component runs on a VMware ESXi 6 virtual Windows 2012 R2 virtual machine on the Customer's existing infrastructure. The configuration for each virtual machine is as follows:

- Citrix XenApp Delivery Controllers (2) 2 vCPUs, 16GB RAM, 1 10Gb vNIC, 50GB Thick Provisioned vDisk
- Citrix Licensing Server (1) 1 vCPU, 4GB RAM, 1 10Gb vNIC, 30GB Thick Provisioned vDisk
- Citrix StoreFront Server (2) 2 vCPU, 4GB RAM, 1 10Gb vNIC, 30GB Thick Provisioned vDisk
- Citrix Provisioning Server (2) 2 vCPU 32GB RAM, 1 10Gb vNIC, 50GB Thick Provisioned vDisk

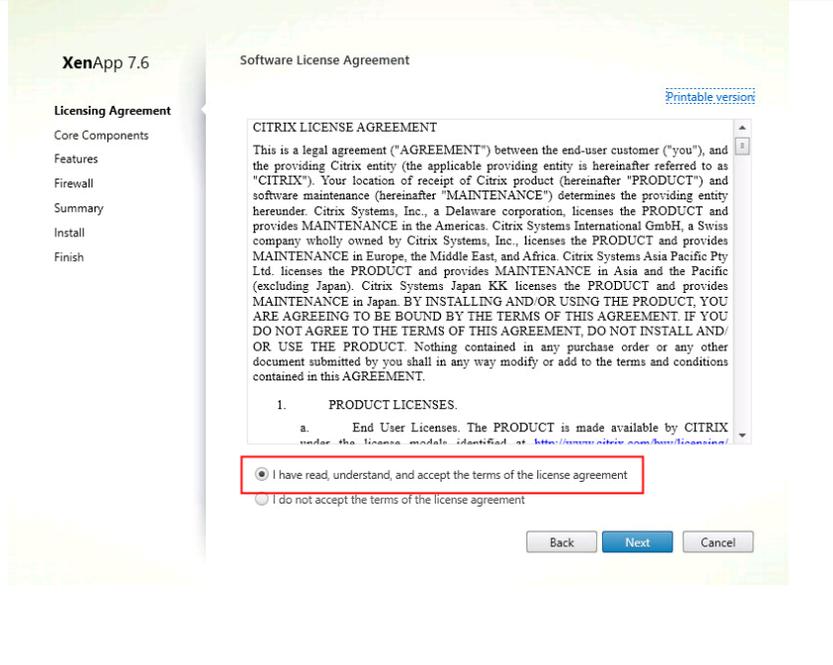
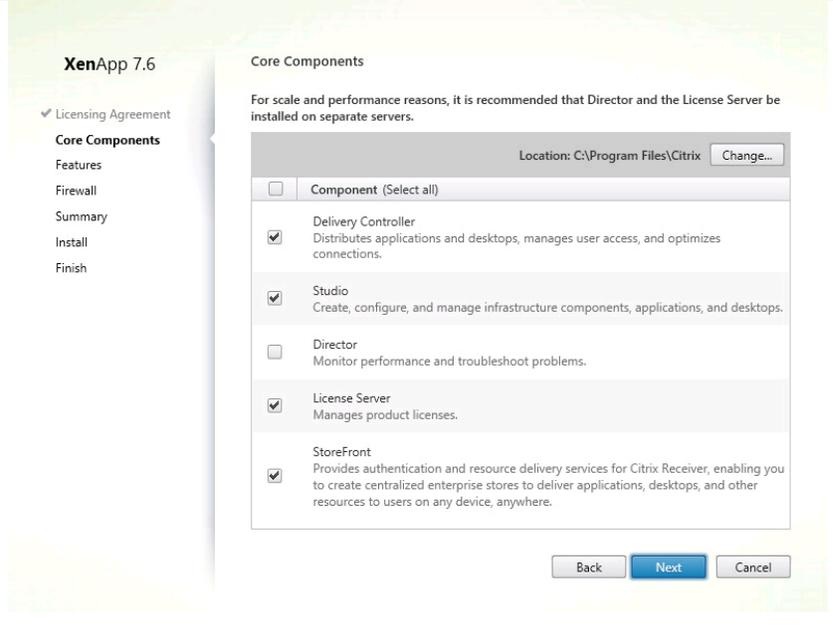
Install XenApp Delivery Controller, Citrix Licensing and StoreFront

The process of installing the XenApp Delivery Controller also installs other key XenApp software components, including Studio, which is used to create and manage infrastructure components, and Director, which is used to monitor performance and troubleshoot problems.

Instructions	Visual
--------------	--------

Instructions	Visual
<p>1. To begin the installation, connect to the first XenApp server and launch the installer from the Citrix XenApp 7.6 ISO.</p> <p>2. Click Start</p>	
<p>The installation wizard presents a menu with three subsections.</p> <p>3. Click “Get Started - Delivery Controller.”</p>	

Instructions	Visual
--------------	--------

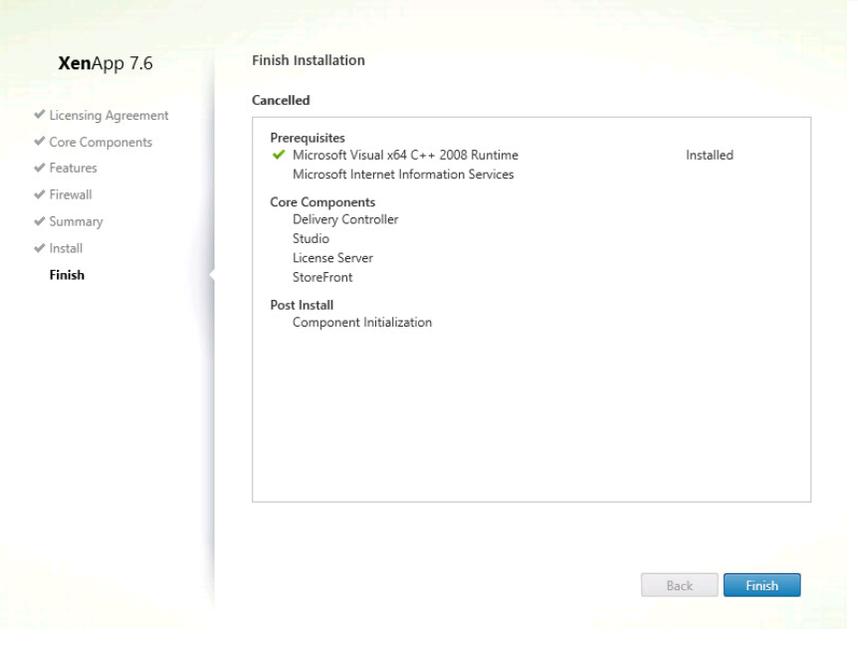
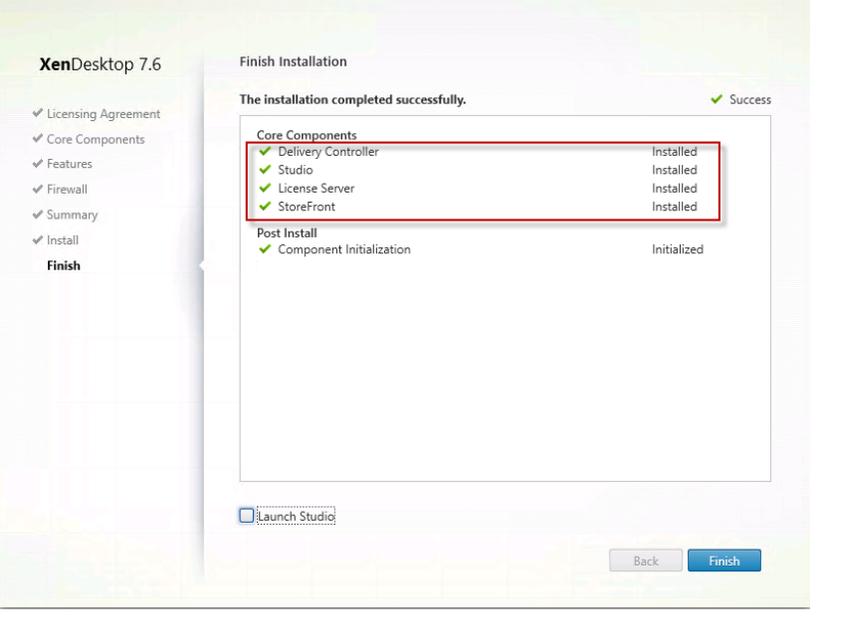
<p>Instructions</p>	<p>Visual</p>
<p>1. Read the Citrix License Agreement.</p> <p>2. If acceptable, indicate your acceptance of the license by selecting the “I have read, understand, and accept the terms of the license agreement” radio button.</p> <p>3. Click Next</p>	
<p>4. Select the components to be installed:</p> <ul style="list-style-type: none"> • Delivery Controller • Studio • License Server • StoreFront <p>5. Click Next</p>	

<p>Instructions</p>	<p>Visual</p>
---------------------	---------------

Instructions	Visual
<p>1. Since a SQL Server will be used to Store the Database, leave “Install Microsoft SQL Server 2012 SP1 Express” unchecked.</p> <p>2. Click Next</p>	<p>XenApp 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components Features Firewall Summary Install Finish <p>Features</p> <p><input type="checkbox"/> Feature (Select all)</p> <p><input type="checkbox"/> Install Microsoft SQL Server 2012 SP1 Express This is an optional component. If you have an existing SQL Server for storing desktop and application configurations and settings, do not select this option.</p> <p><input checked="" type="checkbox"/> Install Windows Remote Assistance Select this only if you need the shadowing feature of Director Server.</p> <p>Back Next Cancel</p>

Instructions	Visual															
<p>3. Select the default ports and automatically configured firewall rules.</p> <p>4. Click Next</p>	<p>XenApp 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components ✓ Features Firewall Summary Install Finish <p>Firewall</p> <p>The default ports are listed below. Printable version</p> <table border="1"> <thead> <tr> <th>Delivery Controller</th> <th>License Server</th> <th>StoreFront</th> </tr> </thead> <tbody> <tr> <td>80 TCP</td> <td>7279 TCP</td> <td>80, 443 TCP</td> </tr> <tr> <td>443 TCP</td> <td>27000 TCP</td> <td></td> </tr> <tr> <td></td> <td>8083 TCP</td> <td></td> </tr> <tr> <td></td> <td>8082 TCP</td> <td></td> </tr> </tbody> </table> <p>Configure firewall rules:</p> <p><input checked="" type="radio"/> Automatically Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.</p> <p><input type="radio"/> Manually Select this option if you are not using Windows Firewall or if you want to create the rules yourself.</p> <p>Back Next Cancel</p>	Delivery Controller	License Server	StoreFront	80 TCP	7279 TCP	80, 443 TCP	443 TCP	27000 TCP			8083 TCP			8082 TCP	
Delivery Controller	License Server	StoreFront														
80 TCP	7279 TCP	80, 443 TCP														
443 TCP	27000 TCP															
	8083 TCP															
	8082 TCP															

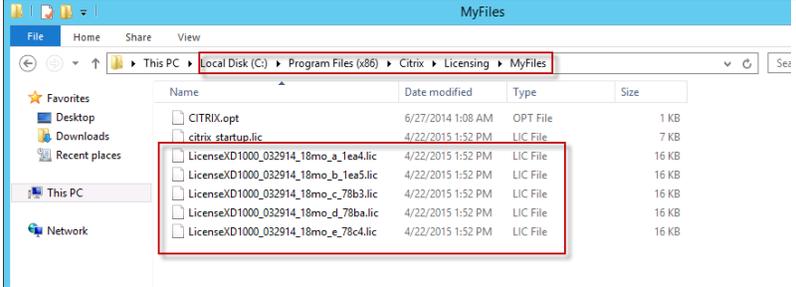
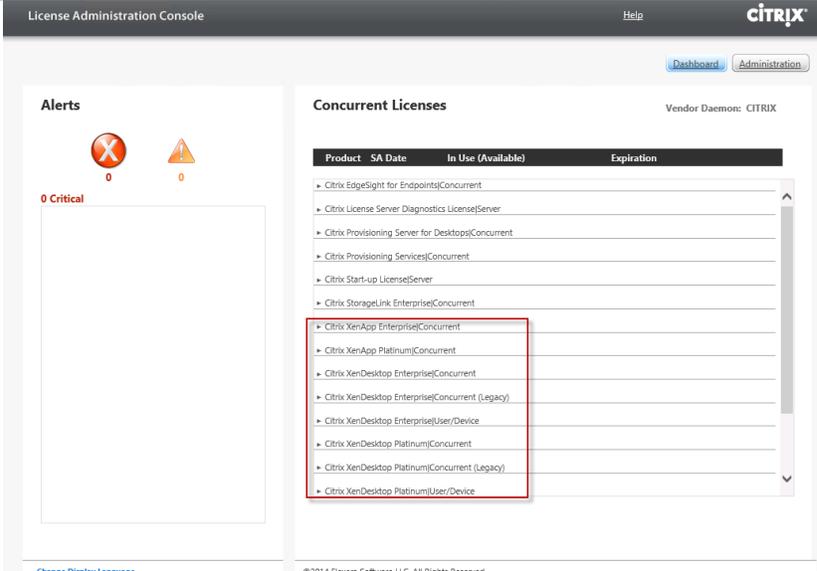
Instructions	Visual
--------------	--------

Instructions	Visual
<p>The Summary screen is shown.</p> <ol style="list-style-type: none"> 1. Click the Install button to begin the installation. 	 <p>XenApp 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components ✓ Features ✓ Firewall ✓ Summary ✓ Install Finish <p>Finish Installation</p> <p>Cancelled</p> <p>Prerequisites</p> <ul style="list-style-type: none"> ✓ Microsoft Visual x64 C++ 2008 Runtime Installed Microsoft Internet Information Services <p>Core Components</p> <ul style="list-style-type: none"> Delivery Controller Studio License Server StoreFront <p>Post Install</p> <ul style="list-style-type: none"> Component Initialization <p>Back Finish</p>
<p>The installer displays a message when the installation is complete</p> <ol style="list-style-type: none"> 2. Click Finish 3. (Optional) Check Launch Studio to launch Citrix Studio Console. 	 <p>XenDesktop 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components ✓ Features ✓ Firewall ✓ Summary ✓ Install Finish <p>Finish Installation</p> <p>The installation completed successfully. ✓ Success</p> <p>Core Components</p> <ul style="list-style-type: none"> ✓ Delivery Controller Installed ✓ Studio Installed ✓ License Server Installed ✓ StoreFront Installed <p>Post Install</p> <ul style="list-style-type: none"> ✓ Component Initialization Initialized <p><input type="checkbox"/> Launch Studio</p> <p>Back Finish</p>

Installing Citrix Licenses

Before moving forward with configuring XenApp, we will begin by installing the Citrix Licenses.

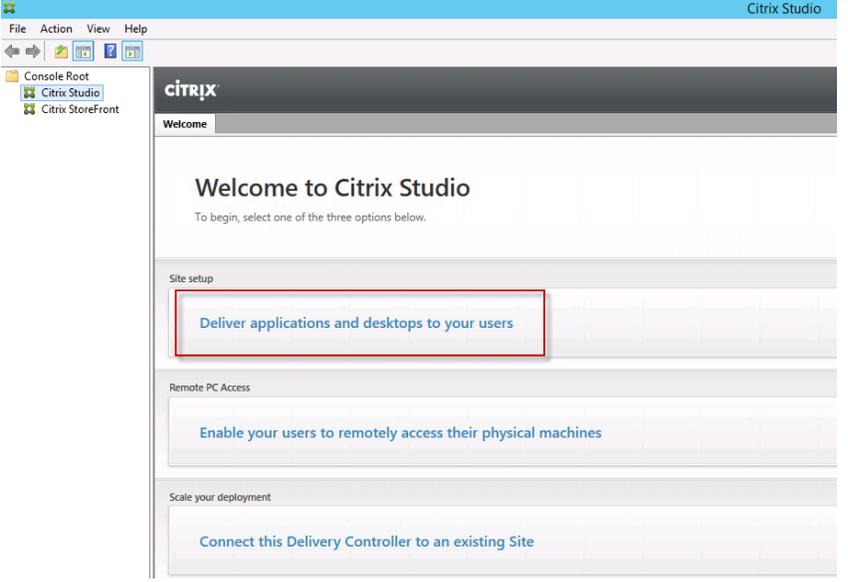
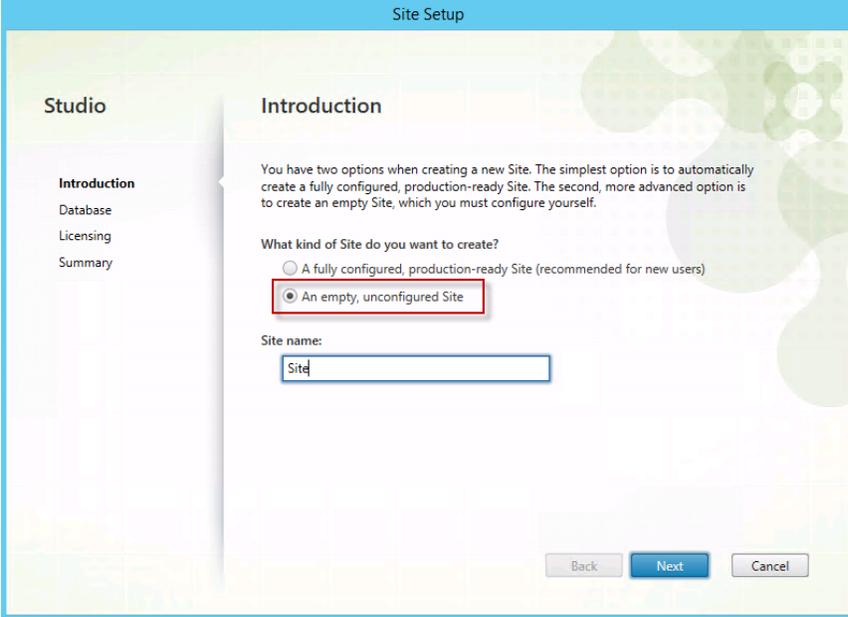
Instructions	Visual
--------------	--------

Instructions	Visual
<p>1. Copy the license files to the default location (C:\Program Files (x86)\Citrix\Licensing\ MyFiles) on the license server</p> <p>2. Restart the server or licensing services so that the licenses are activated.</p>	
<p>3. Run the application Citrix License Administration Console</p>	
<p>4. Confirm that the license files have been read and enabled correctly.</p>	

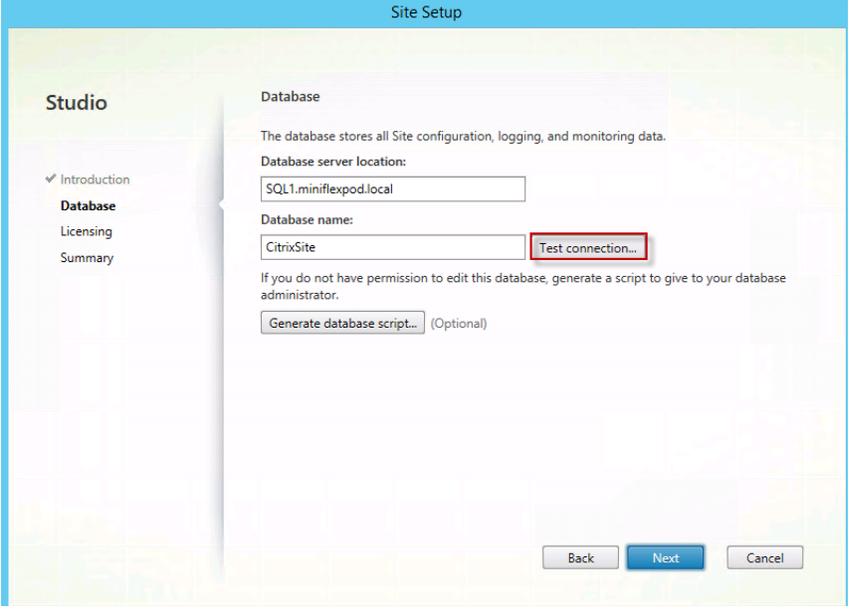
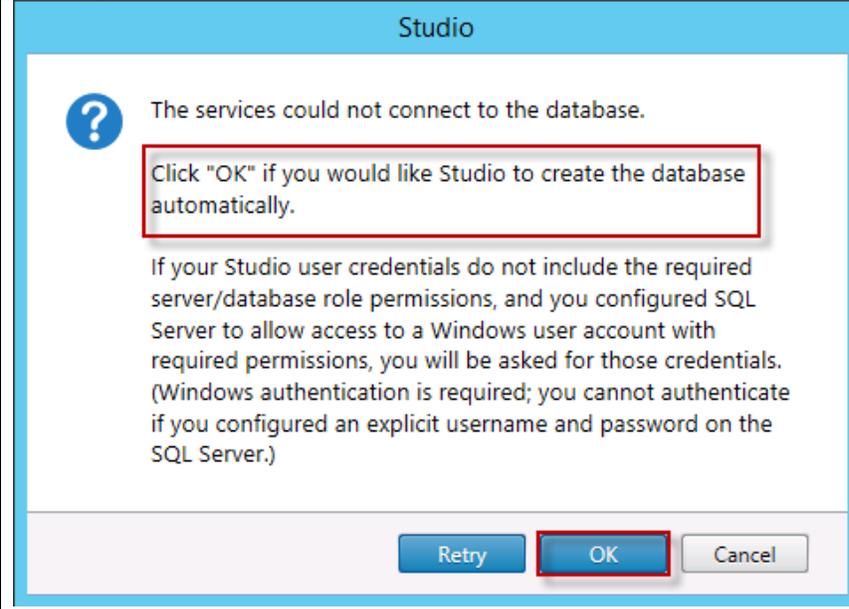
Configure the XenApp Site

Citrix Studio is a management console that allows you to create and manage infrastructure and resources to deliver desktops and applications. Replacing Desktop Studio from earlier releases, it provides wizards to set up your environment, create workloads to host applications and desktops, and assign applications and desktops to users.

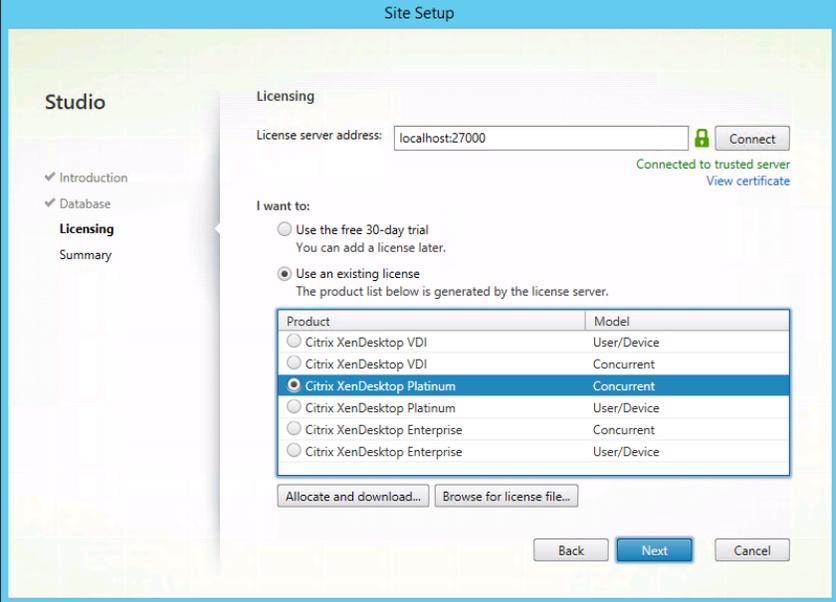
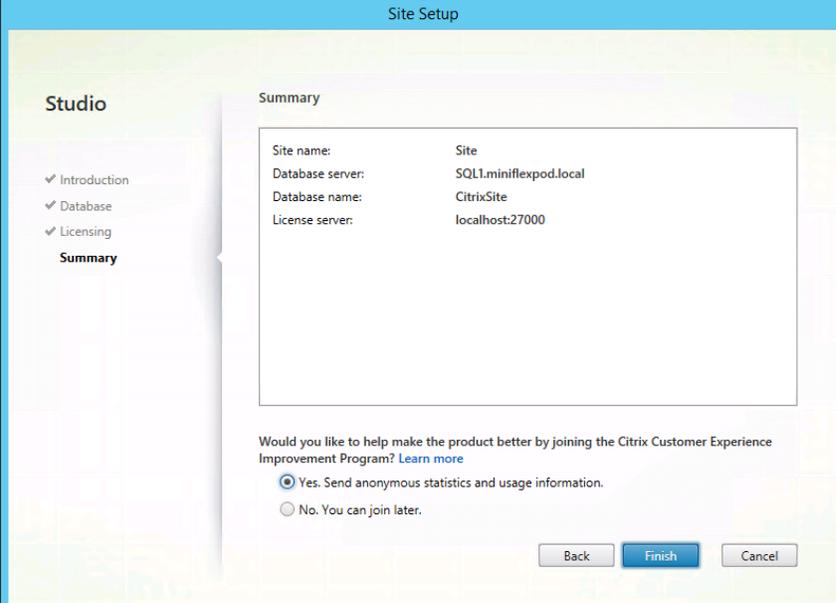
Citrix Studio launches automatically after the XenApp Delivery Controller installation, or if necessary, it can be launched manually. Studio is used to create a Site, which is the core XenApp 7.6 environment consisting of the Delivery Controller and the Database.

<p>Instructions</p>	<p>Visual</p>
<p>1. Click the Deliver applications and desktops to your users button.</p>	 <p>The screenshot shows the Citrix Studio 'Welcome' screen. On the left is a navigation pane with 'Console Root', 'Citrix Studio', and 'Citrix StoreFront'. The main area has a 'Welcome to Citrix Studio' header and three options: 'Deliver applications and desktops to your users' (highlighted with a red box), 'Enable your users to remotely access their physical machines', and 'Connect this Delivery Controller to an existing Site'.</p>
<p>2. Select the “An empty, unconfigured Site” radio button.</p> <p>3. Enter a site name.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Site Setup' screen. On the left is a sidebar with 'Introduction', 'Database', 'Licensing', and 'Summary'. The main area has an 'Introduction' section with text about creating a new Site. Under 'What kind of Site do you want to create?', the 'An empty, unconfigured Site' radio button is selected and highlighted with a red box. Below it, the 'Site name:' field contains the text 'Site'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.</p>

<p>Instructions</p>	<p>Visual</p>
---------------------	---------------

<p>Instructions</p>	<p>Visual</p>
<p>1. Provide the Database Server location.</p> <p>2. Click the Test connection... button to verify that the database is accessible.</p>	
<p>3. Click OK to have the installer create the database.</p>	

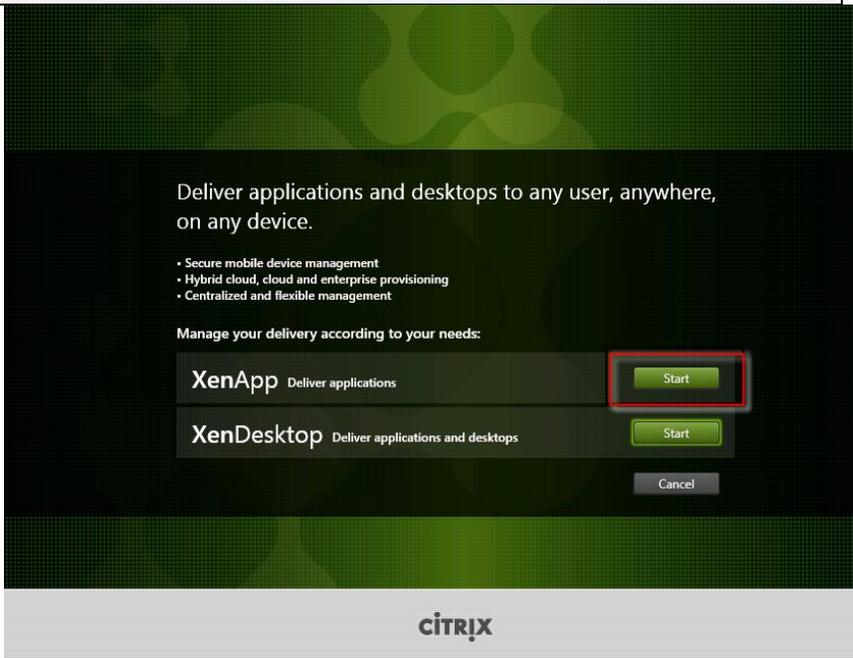
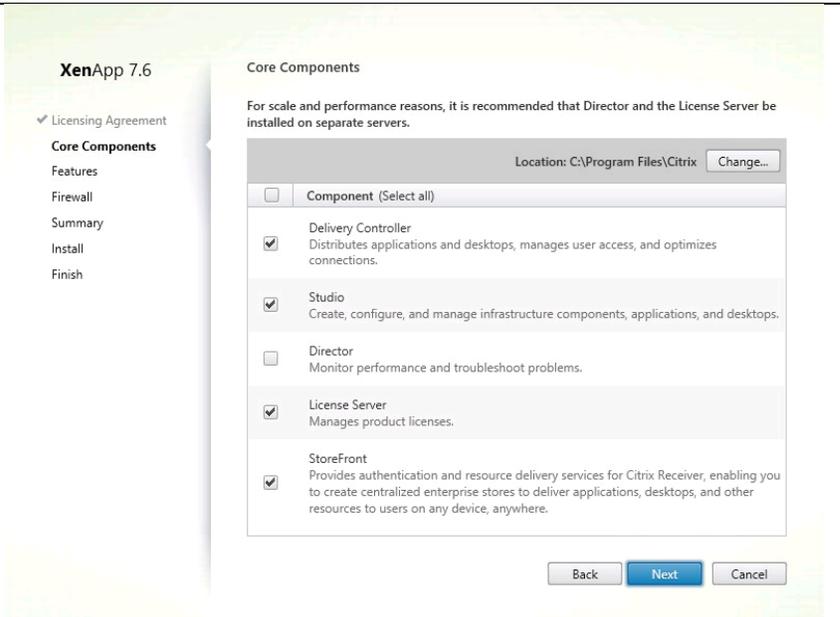
<p>Instructions</p>	<p>Visual</p>
---------------------	---------------

Instructions	Visual														
<p>1. Provide the FQDN of the license server.</p> <p>2. Click Connect to validate and retrieve any licenses from the server.</p> <hr/> <p> If no licenses are available, you can use the 30-day free trial or activate a license file.</p> <p>3. Select the appropriate product edition using the license radio button</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Site Setup' window with the 'Licensing' tab selected. The 'License server address' is 'localhost:27000'. Under 'I want to:', the 'Use an existing license' option is selected. A table lists product editions:</p> <table border="1" data-bbox="885 562 1399 730"> <thead> <tr> <th>Product</th> <th>Model</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/> Citrix XenDesktop VDI</td> <td>User/Device</td> </tr> <tr> <td><input type="radio"/> Citrix XenDesktop VDI</td> <td>Concurrent</td> </tr> <tr> <td><input checked="" type="radio"/> Citrix XenDesktop Platinum</td> <td>Concurrent</td> </tr> <tr> <td><input type="radio"/> Citrix XenDesktop Platinum</td> <td>User/Device</td> </tr> <tr> <td><input type="radio"/> Citrix XenDesktop Enterprise</td> <td>Concurrent</td> </tr> <tr> <td><input type="radio"/> Citrix XenDesktop Enterprise</td> <td>User/Device</td> </tr> </tbody> </table>	Product	Model	<input type="radio"/> Citrix XenDesktop VDI	User/Device	<input type="radio"/> Citrix XenDesktop VDI	Concurrent	<input checked="" type="radio"/> Citrix XenDesktop Platinum	Concurrent	<input type="radio"/> Citrix XenDesktop Platinum	User/Device	<input type="radio"/> Citrix XenDesktop Enterprise	Concurrent	<input type="radio"/> Citrix XenDesktop Enterprise	User/Device
Product	Model														
<input type="radio"/> Citrix XenDesktop VDI	User/Device														
<input type="radio"/> Citrix XenDesktop VDI	Concurrent														
<input checked="" type="radio"/> Citrix XenDesktop Platinum	Concurrent														
<input type="radio"/> Citrix XenDesktop Platinum	User/Device														
<input type="radio"/> Citrix XenDesktop Enterprise	Concurrent														
<input type="radio"/> Citrix XenDesktop Enterprise	User/Device														
<p>5. Click Finish to complete initial setup.</p>	 <p>The screenshot shows the 'Site Setup' window with the 'Summary' tab selected. The summary information is as follows:</p> <table border="1" data-bbox="868 1129 1404 1407"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Site name:</td> <td>Site</td> </tr> <tr> <td>Database server:</td> <td>SQL1.miniflexpod.local</td> </tr> <tr> <td>Database name:</td> <td>CitrixSite</td> </tr> <tr> <td>License server:</td> <td>localhost:27000</td> </tr> </tbody> </table> <p>At the bottom, the 'Citrix Customer Experience Improvement Program' is shown with the 'Yes' option selected.</p>	Field	Value	Site name:	Site	Database server:	SQL1.miniflexpod.local	Database name:	CitrixSite	License server:	localhost:27000				
Field	Value														
Site name:	Site														
Database server:	SQL1.miniflexpod.local														
Database name:	CitrixSite														
License server:	localhost:27000														

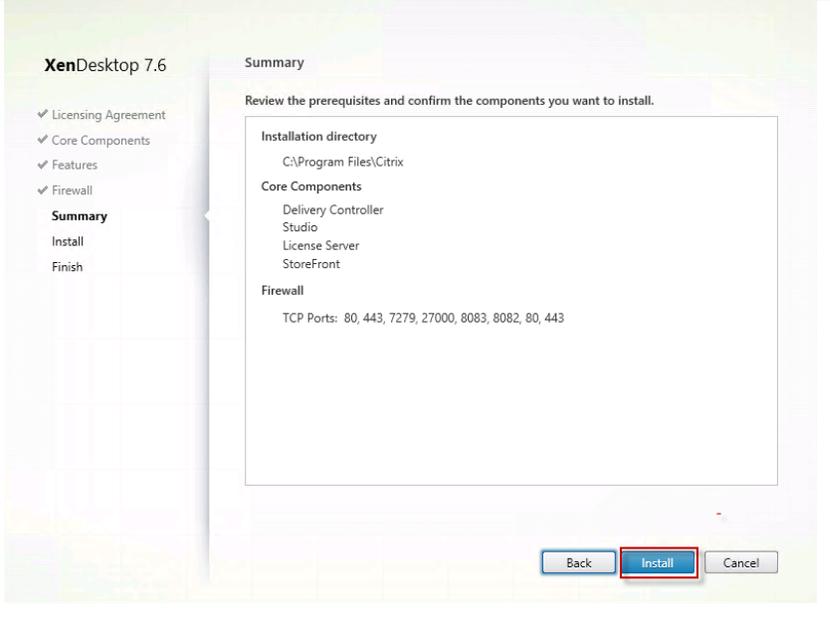
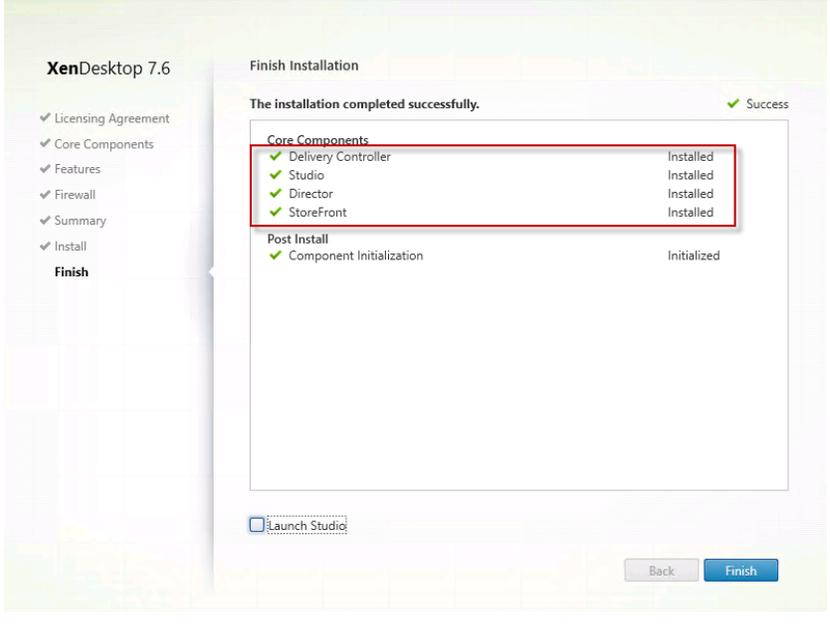
Additional XenApp Controller Configuration

After the first controller is completely configured and the Site is operational, you can add additional controllers. In this CVD, we created two Delivery Controllers.

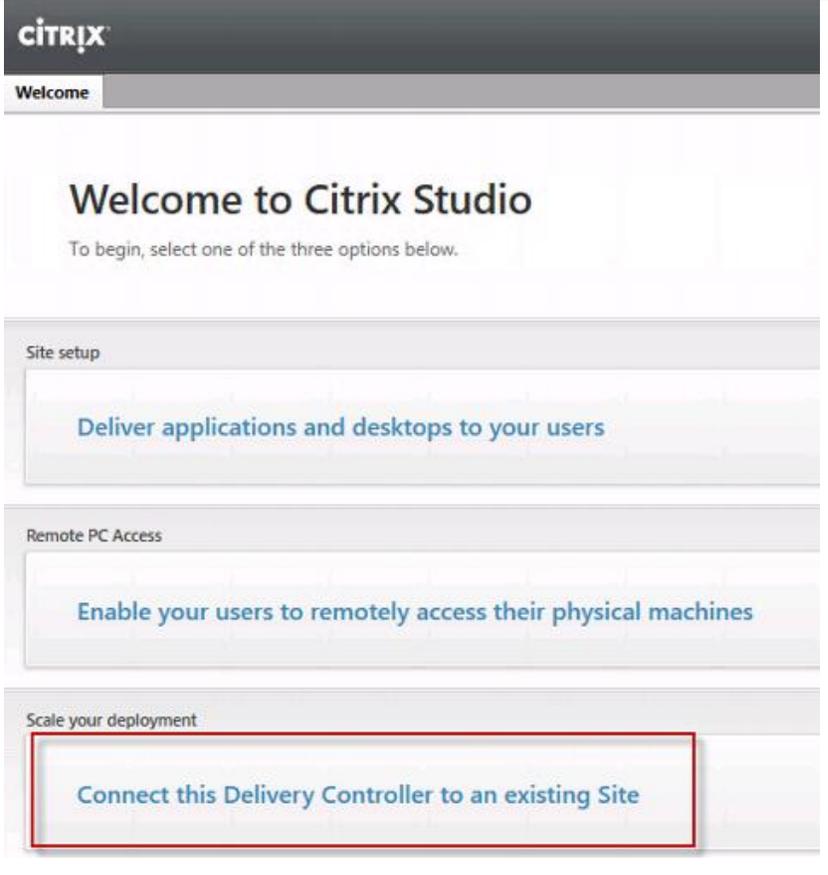
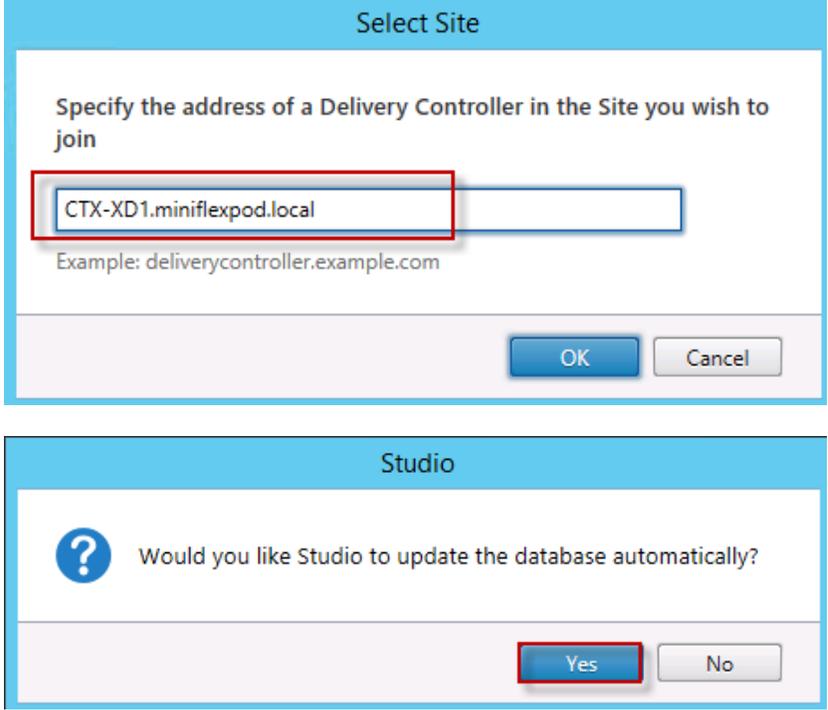
Instructions	Visual
--------------	--------

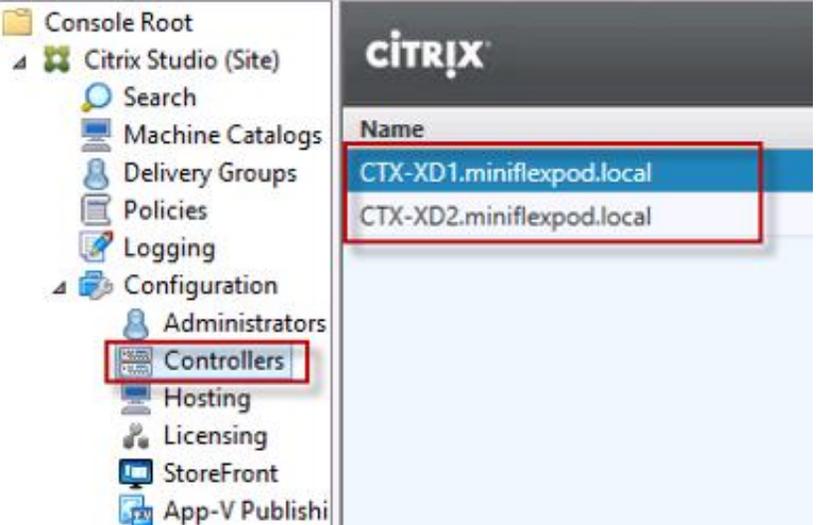
Instructions	Visual
<p>1. To begin the installation of the second Delivery Controller, connect to the second XenApp server and launch the installer from the Citrix XenApp 7.6 ISO.</p> <p>2. Click Start</p>	
<p>3. Select the components to be installed:</p> <ul style="list-style-type: none"> • Delivery Controller • Studio • Director • StoreFront <p>4. Click Next</p>	

Instructions	Visual
--------------	--------

Instructions	Visual										
<p>1. Repeat the same steps used to install the first Delivery Controller.</p> <p>2. Review the Summary configuration.</p> <p>3. Click Install</p>	 <p>The screenshot shows the 'Summary' screen of the XenDesktop 7.6 installation wizard. On the left, a navigation pane lists 'Licensing Agreement', 'Core Components', 'Features', 'Firewall', 'Summary', 'Install', and 'Finish'. The 'Summary' step is selected. The main area displays the following configuration details:</p> <ul style="list-style-type: none"> Installation directory: C:\Program Files\Citrix Core Components: Delivery Controller, Studio, License Server, StoreFront Firewall: TCP Ports: 80, 443, 7279, 27000, 8083, 8082, 80, 443 <p>At the bottom, there are three buttons: 'Back', 'Install' (highlighted with a red box), and 'Cancel'.</p>										
<p>4. Confirm all selected components were successfully installed.</p> <p>5. Verify the Launch Studio checkbox is checked.</p> <p>6. Click Finish</p>	 <p>The screenshot shows the 'Finish Installation' screen of the XenDesktop 7.6 installation wizard. The main area displays a success message: 'The installation completed successfully.' with a green checkmark and the word 'Success'. Below this, a table lists the components and their status:</p> <table border="1" data-bbox="867 1024 1354 1115"> <thead> <tr> <th colspan="2">Core Components</th> </tr> </thead> <tbody> <tr> <td>✓ Delivery Controller</td> <td>Installed</td> </tr> <tr> <td>✓ Studio</td> <td>Installed</td> </tr> <tr> <td>✓ Director</td> <td>Installed</td> </tr> <tr> <td>✓ StoreFront</td> <td>Installed</td> </tr> </tbody> </table> <p>Below the table, under 'Post Install', it shows 'Component Initialization' as 'Initialized'. At the bottom, there is a checkbox for 'Launch Studio' which is checked, and two buttons: 'Back' and 'Finish'.</p>	Core Components		✓ Delivery Controller	Installed	✓ Studio	Installed	✓ Director	Installed	✓ StoreFront	Installed
Core Components											
✓ Delivery Controller	Installed										
✓ Studio	Installed										
✓ Director	Installed										
✓ StoreFront	Installed										

Instructions	Visual
--------------	--------

Instructions	Visual
<p>1. Click the Connect this Delivery Controller to an existing Site button.</p>	
<p>2. Enter the FQDN of the first delivery controller.</p> <p>3. Click OK</p> <p>4. Click Yes to allow the database to be updated with this controller's information automatically.</p>	

Instructions	Visual
<p>1. When complete, verify the Delivery Controller has been added to the list of Controllers.</p>	 <p>The screenshot shows the Citrix Studio console interface. On the left, the 'Console Root' tree is expanded to 'Citrix Studio (Site)', and the 'Controllers' folder is selected and highlighted with a red box. On the right, the 'Name' column of a table lists two delivery controllers: 'CTX-XD1.miniflexpod.local' and 'CTX-XD2.miniflexpod.local', both of which are also highlighted with a red box.</p>

Installing and Configuring Citrix Provisioning Server 7.6

In most implementations, there is a single vDisk providing the standard image for multiple target devices. Thousands of target devices can use a single vDisk shared across multiple Provisioning Services (PVS) servers in the same farm, simplifying virtual desktop management. This section describes the installation and configuration tasks required to create a PVS implementation.

The PVS server can have many stored vDisks, and each vDisk can be several gigabytes in size. Your streaming performance and manageability can be improved using a RAID array, SAN, or NAS. PVS software and hardware requirements are available [at http://support.citrix.com/proddocs/topic/provisioning-7/pvs-install-task1-plan-6-0.html](http://support.citrix.com/proddocs/topic/provisioning-7/pvs-install-task1-plan-6-0.html).

Prerequisites

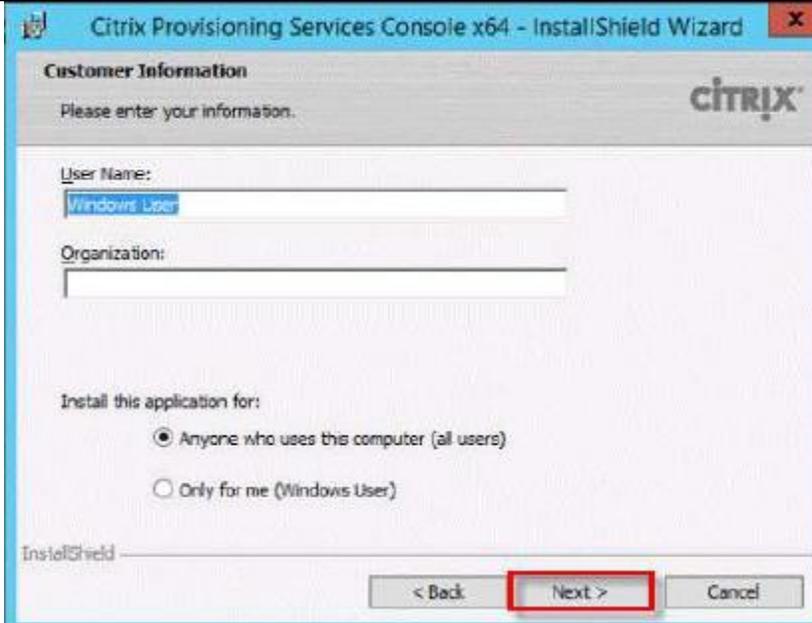
Only one MS SQL database is associated with a farm. You can choose to install the Provisioning Services database software on an existing SQL database, if that machine can communicate with all Provisioning Servers within the farm, or with a new SQL Express database machine, created using the SQL Express software that is free from Microsoft.

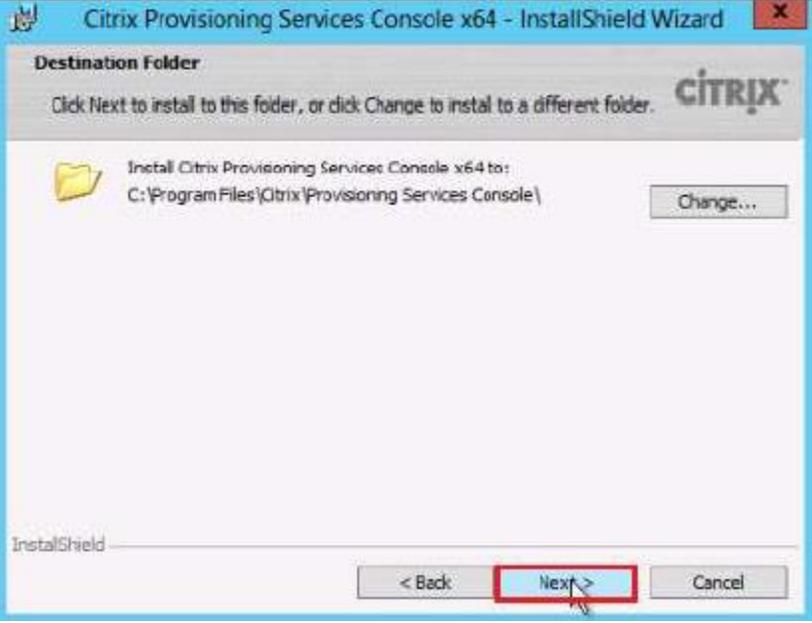
The following MS SQL 2008, MS SQL 2008 R2, MS SQL 2012, MS SQL 2012 R2 and MS SQL 2014 Server (32 or 64-bit editions) databases can be used for the Provisioning Services database: SQL Server Express Edition, SQL Server Workgroup Edition, SQL Server Standard Edition, SQL Server Enterprise Edition. Microsoft SQL were installed separately for this CVD.

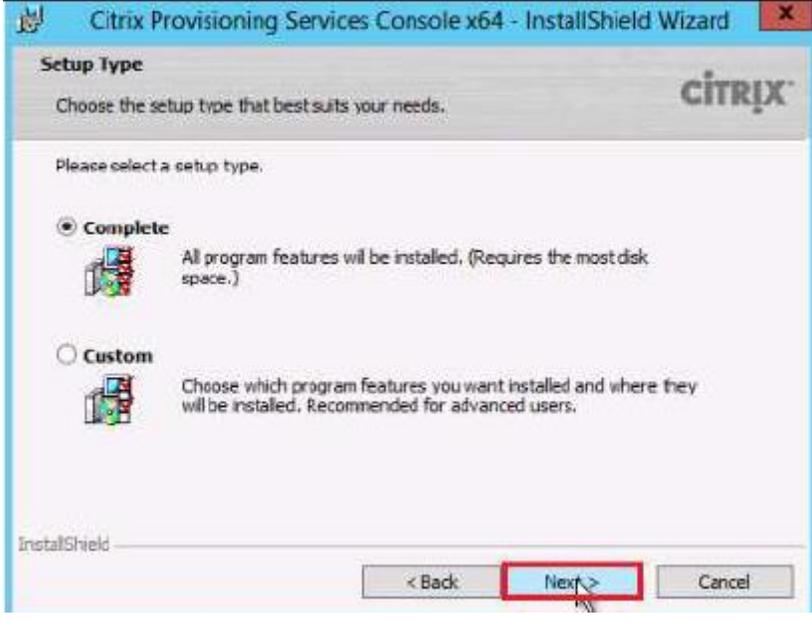
Instructions	Visual
--------------	--------

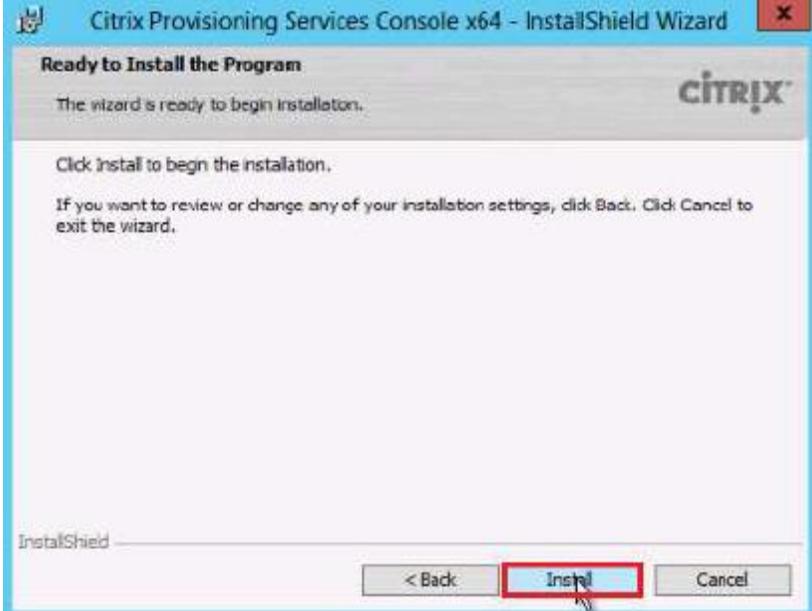
Instructions	Visual
<p>1. Insert the Citrix Provisioning Services 7.6 ISO and let AutoRun launch the installer.</p> <p>2. Click the Console Installation button.</p>	
<p>3. Click Next</p>	

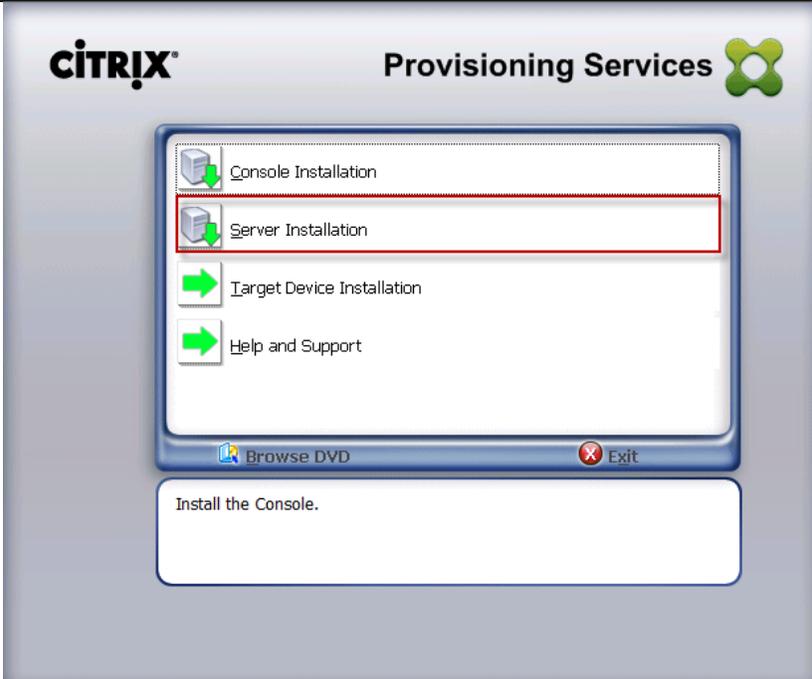
Instructions	Visual
<p>4. Read the Citrix License Agreement.</p> <p>5. If acceptable, select the radio button labeled "I accept the terms in the license agreement."</p> <p>6. Click Next</p>	 <p>The screenshot shows the 'License Agreement' step of the Citrix Provisioning Services Console x64 - InstallShield Wizard. The window title is 'Citrix Provisioning Services Console x64 - InstallShield Wizard'. The main heading is 'License Agreement' with the Citrix logo. Below the heading, it says 'You must view the entire license agreement in order to continue.' A scrollable text area contains the 'CITRIX LICENSE AGREEMENT' text. At the bottom, there are two radio buttons: 'I accept the terms in the license agreement' (which is selected and highlighted with a red box) and 'I do not accept the terms in the license agreement'. To the right of the radio buttons is a 'Print' button. At the very bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

Instructions	Visual
<p>1. Optionally provide User Name and Organization.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Customer Information' step of the Citrix Provisioning Services Console x64 - InstallShield Wizard. The window title is 'Citrix Provisioning Services Console x64 - InstallShield Wizard'. The main heading is 'Customer Information' with the Citrix logo. Below the heading, it says 'Please enter your information.' There are two input fields: 'User Name:' containing 'Windows User' and 'Organization:'. Below these are two radio buttons under the heading 'Install this application for:': 'Anyone who uses this computer (all users)' (selected) and 'Only for me (Windows User)'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

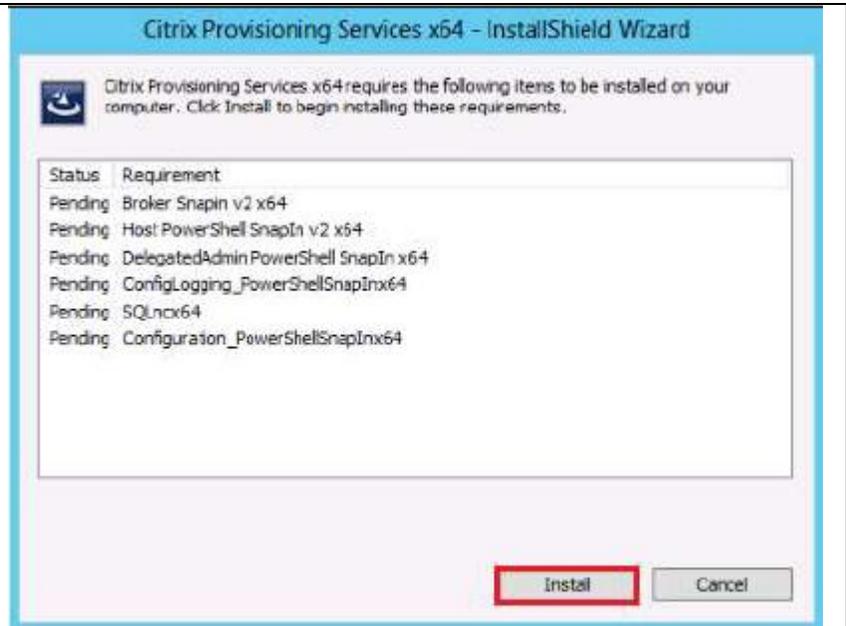
Instructions	Visual
<p>3. Accept the default path.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Destination Folder' step of the Citrix Provisioning Services Console x64 - InstallShield Wizard. The window title is 'Citrix Provisioning Services Console x64 - InstallShield Wizard'. The main heading is 'Destination Folder' with the Citrix logo. Below the heading, it says 'Click Next to install to this folder, or click Change to install to a different folder.' A folder icon is shown next to the text 'Install Citrix Provisioning Services Console x64 to: C:\Program Files\Citrix\Provisioning Services Console'. A 'Change...' button is to the right. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle and has a mouse cursor over it.</p>

Instructions	Visual
<p>1. Leave the Complete radio button selected.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Setup Type' step of the Citrix Provisioning Services Console x64 - InstallShield Wizard. The window title is 'Citrix Provisioning Services Console x64 - InstallShield Wizard'. The main heading is 'Setup Type' with the Citrix logo. Below the heading, it says 'Choose the setup type that best suits your needs.' and 'Please select a setup type.' There are two radio button options: 'Complete' (selected) and 'Custom'. The 'Complete' option has a description: 'All program features will be installed, (Requires the most disk space.)'. The 'Custom' option has a description: 'Choose which program features you want installed and where they will be installed, Recommended for advanced users.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle and has a mouse cursor over it.</p>

Instructions	Visual
<p>3. Click the Install button to start the console installation.</p>	

Instructions	Visual
<p>1. From the main installation screen, select Server Installation.</p> <p>2. The installation wizard will check to resolve dependencies and then begin the PVS server installation process.</p>	

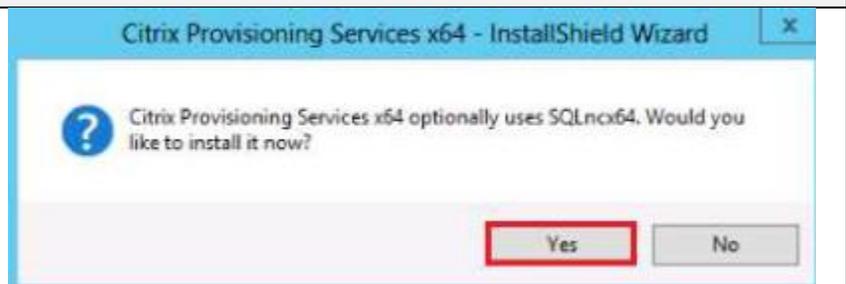
3. Click Install on the prerequisites dialog.



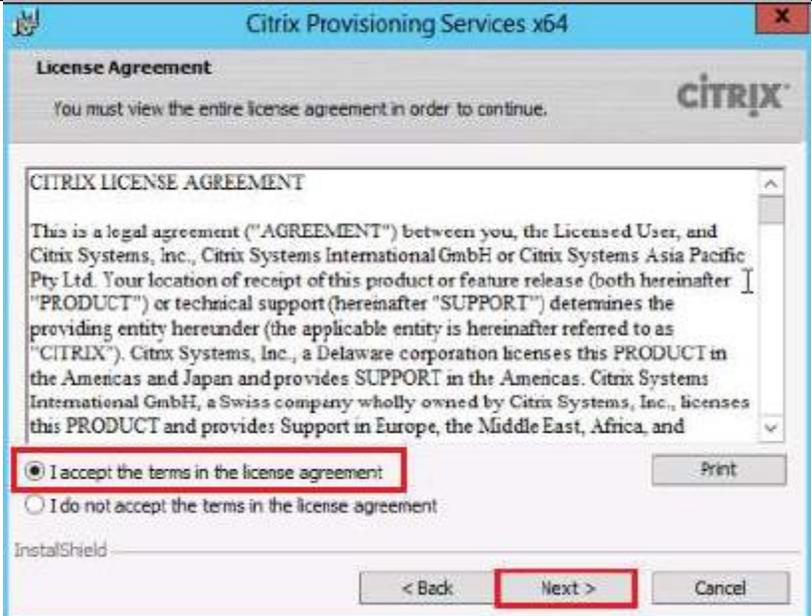
Instructions

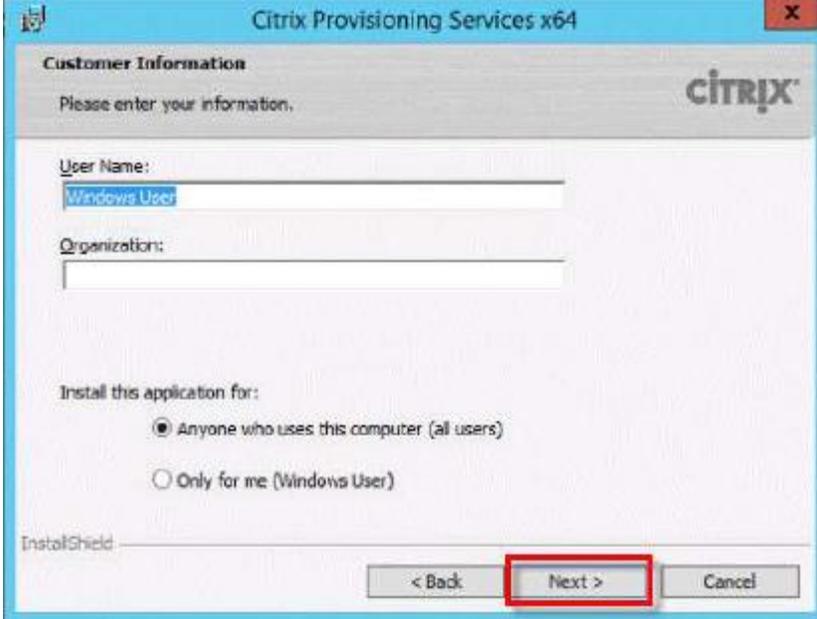
Visual

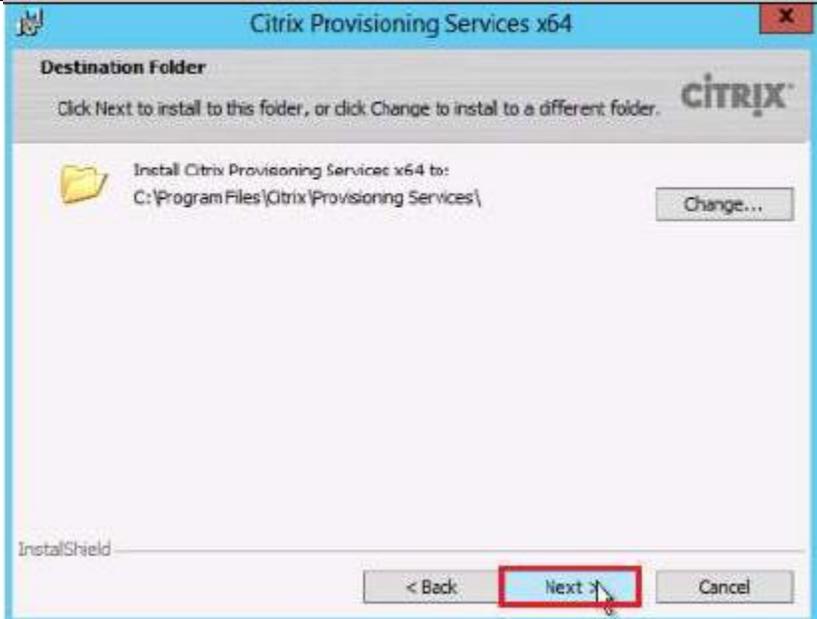
1. Click Yes when prompted to install the SQL Native Client.



<p>Instructions</p>	<p>Visual</p>
<p>2. Click Next when the Installation wizard starts.</p>	

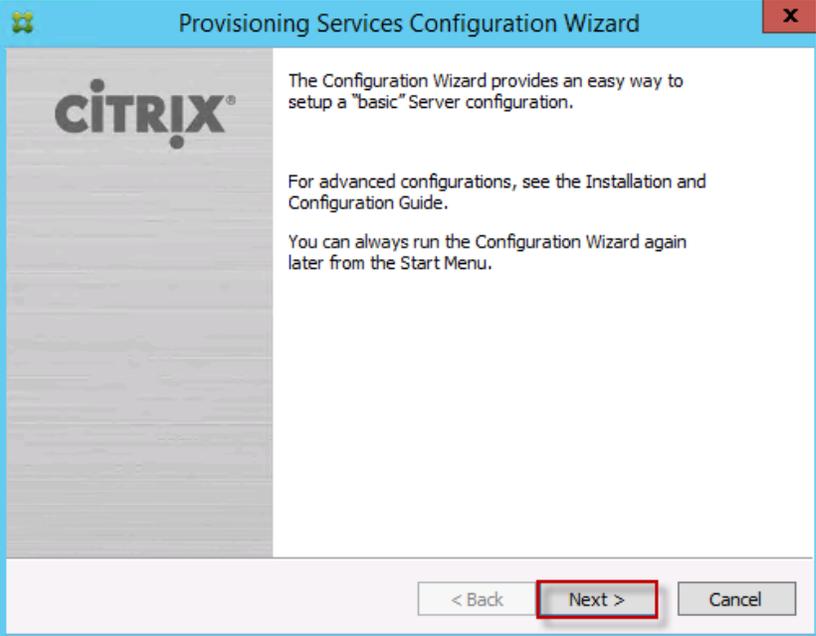
<p>Instructions</p>	<p>Visual</p>
<p>1. Review the license agreement terms.</p> <p>2. If acceptable, select the radio button labeled “I accept the terms in the license agreement.”</p> <p>3. Click Next</p>	

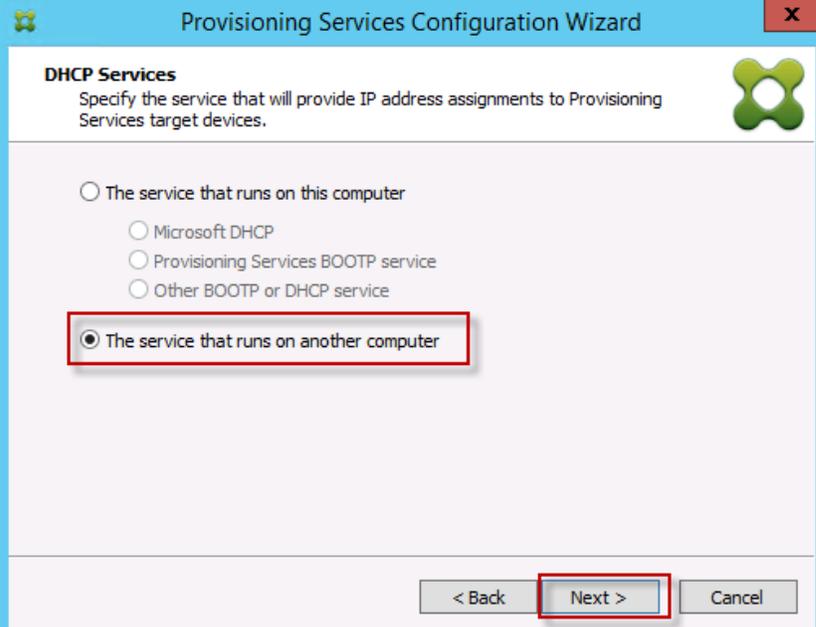
Instructions	Visual
4. Provide User Name, and Organization information. Select who will see the application. 5. Click Next	 <p>The screenshot shows the 'Citrix Provisioning Services x64' dialog box. The title bar is blue with the Citrix logo on the right. Below the title bar is a grey header area with the text 'Customer Information' and 'Please enter your information.' To the right of this header is the Citrix logo. The main area contains two text input fields: 'User Name:' with 'Windows User' entered, and 'Organization:' which is empty. Below these fields is a section titled 'Install this application for:' with two radio button options: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me (Windows User)'. At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.</p>

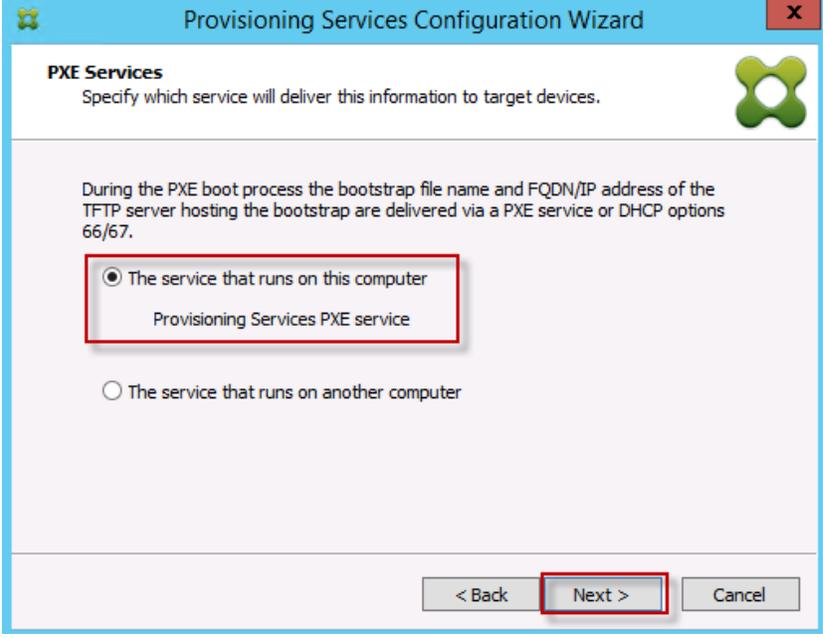
Instructions	Visual
1. Accept the default installation location. 2. Click Next	 <p>The screenshot shows the 'Citrix Provisioning Services x64' dialog box. The title bar is blue with the Citrix logo on the right. Below the title bar is a grey header area with the text 'Destination Folder' and 'Click Next to install to this folder, or click Change to install to a different folder.' To the right of this header is the Citrix logo. The main area contains a folder icon and the text 'Install Citrix Provisioning Services x64 to: C:\Program Files\Citrix\Provisioning Services\'. To the right of this text is a 'Change...' button. At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.</p>

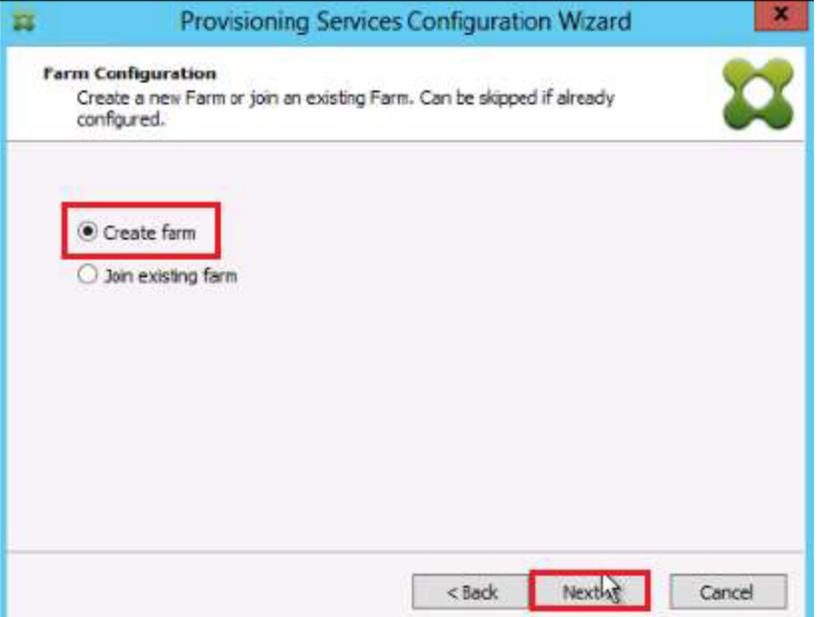
Instructions	Visual
<p>3. Click Install to begin the installation.</p>	

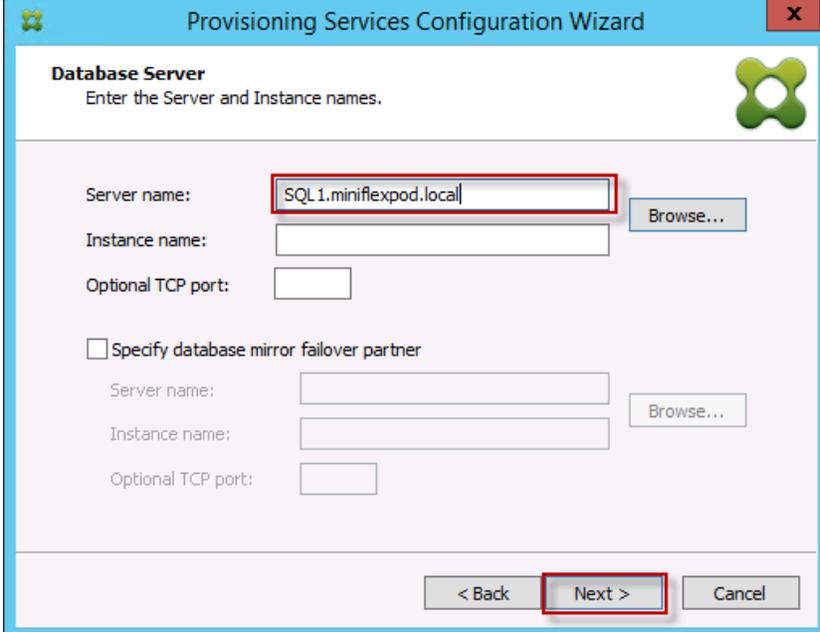
Instructions	Visual
<p>1. Click Finish when the install is complete.</p>	

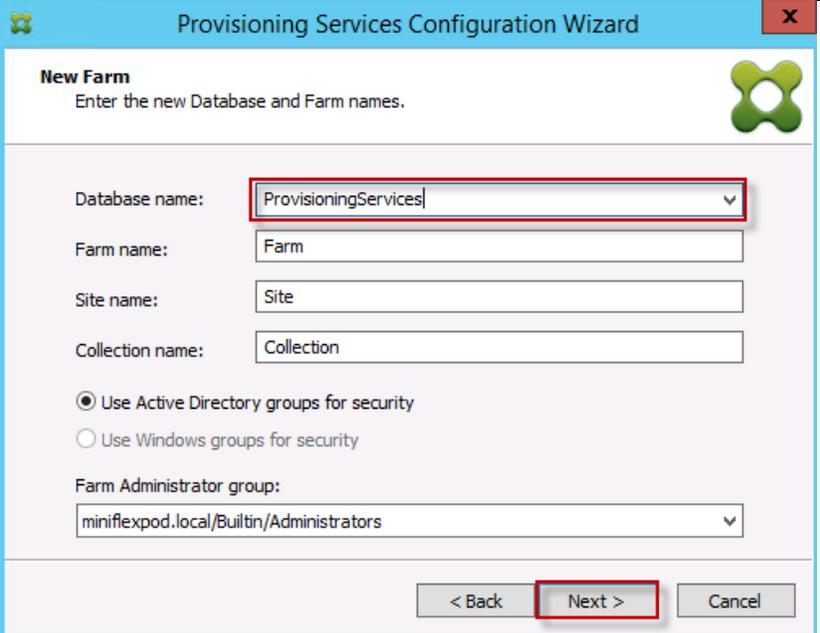
Instructions	Visual
<p>2. The PVS Configuration Wizard starts automatically.</p> <p>3. Click Next</p>	

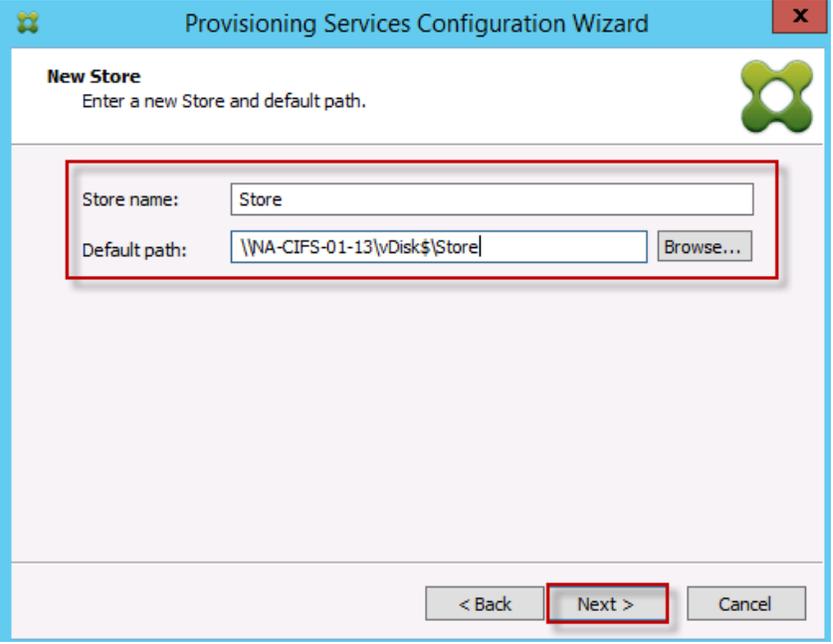
Instructions	Visual
<p>1. Since the PVS server is not the DHCP server for the environment, select the radio button labeled, “The service that runs on another computer.”</p> <p>2. Click Next</p>	

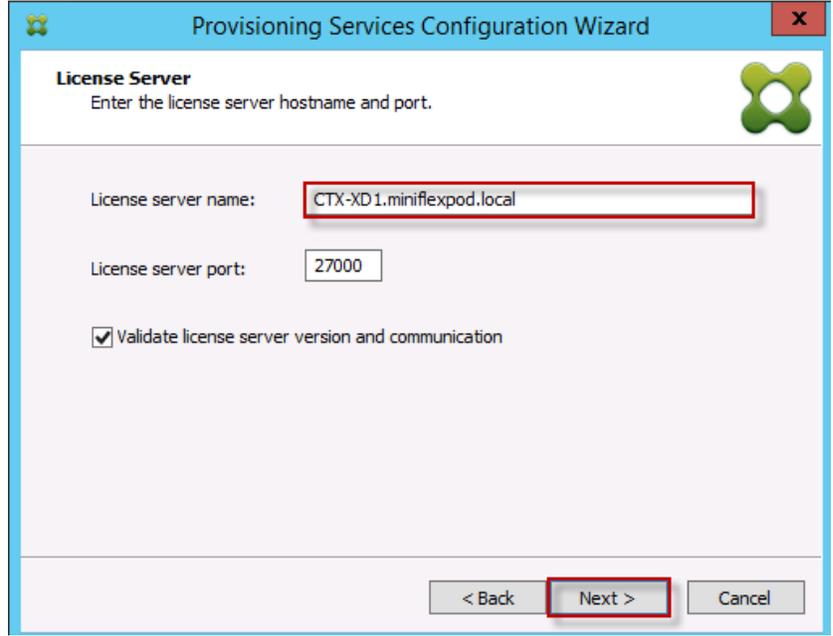
Instructions	Visual
<p>3. Since this server will be a PXE server, select the radio button labeled, “The service that runs on this computer.”</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the section is titled 'PXE Services' with the instruction 'Specify which service will deliver this information to target devices.' A sub-instruction states: 'During the PXE boot process the bootstrap file name and FQDN/IP address of the TFTP server hosting the bootstrap are delivered via a PXE service or DHCP options 66/67.' There are two radio button options: 'The service that runs on this computer' (which is selected and highlighted with a red box) and 'The service that runs on another computer'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

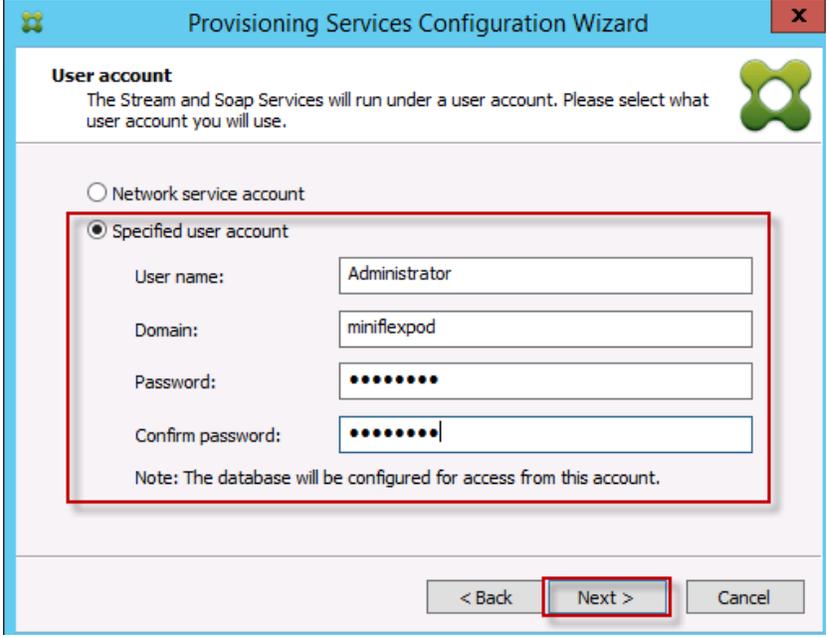
Instructions	Visual
<p>1. Since this is the first server in the farm, select the radio button labeled, “Create farm”.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the section is titled 'Farm Configuration' with the instruction 'Create a new Farm or join an existing Farm. Can be skipped if already configured.' There are two radio button options: 'Create farm' (which is selected and highlighted with a red box) and 'Join existing farm'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

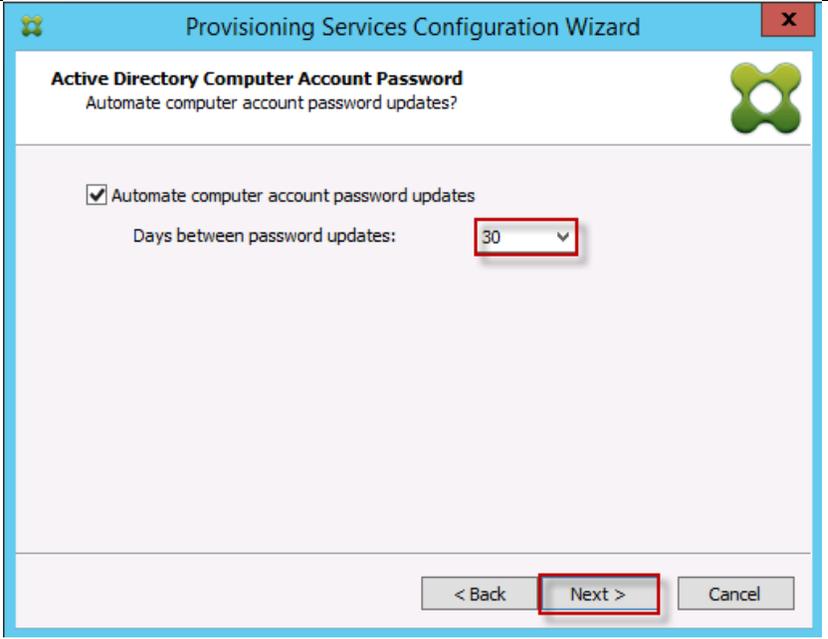
Instructions	Visual
<p>3. Enter the FQDN of the SQL server.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Database Server' configuration window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title, it says 'Database Server' and 'Enter the Server and Instance names.' There are two sets of input fields. The first set includes 'Server name' (containing 'SQL1.miniflexpod.local'), 'Instance name', and 'Optional TCP port'. The second set is for a 'Specify database mirror failover partner' and includes 'Server name', 'Instance name', and 'Optional TCP port'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.</p>

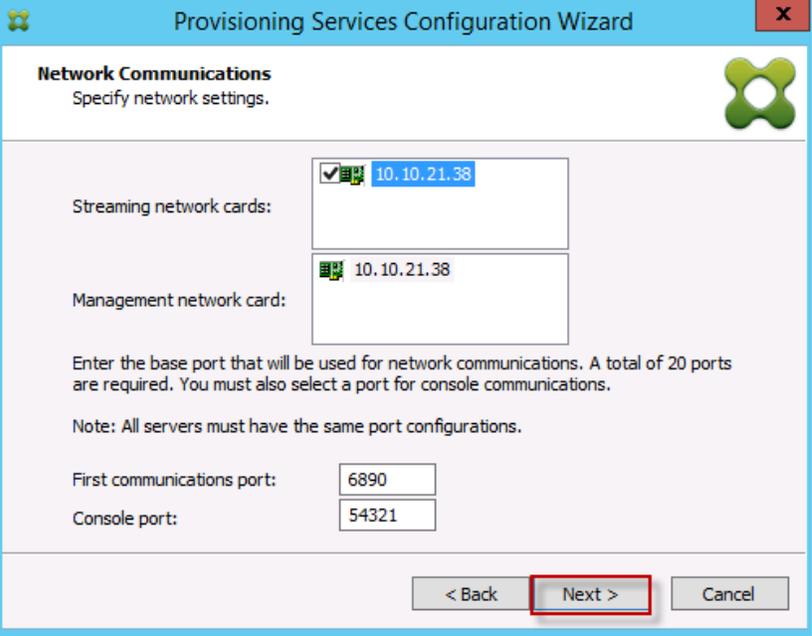
Instructions	Visual
<p>1. Provide a vDisk Store name and the storage path to the NetApp vDisk share.</p> <hr/> <p> Create the share using NetApp's native support for SMB3.</p> <hr/> <p>2. Click Next</p>	 <p>The screenshot shows the 'New Farm' configuration window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title, it says 'New Farm' and 'Enter the new Database and Farm names.' There are four input fields: 'Database name' (a dropdown menu showing 'ProvisioningServices'), 'Farm name' (containing 'Farm'), 'Site name' (containing 'Site'), and 'Collection name' (containing 'Collection'). Below these are two radio buttons: 'Use Active Directory groups for security' (selected) and 'Use Windows groups for security'. At the bottom, there is a 'Farm Administrator group' dropdown menu showing 'miniflexpod.local/Builtin/Administrators'. At the very bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.</p>

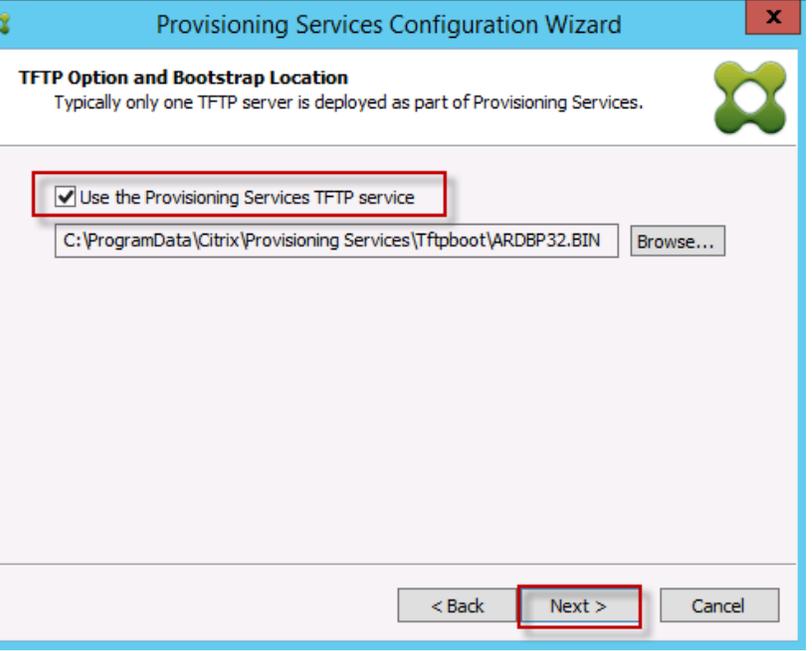
Instructions	Visual
<p>3. Provide a vDisk Store name and the storage path to the NetApp vDisk share.</p> <hr/> <p> Create the share using NetApp's native support for SMB3.</p> <hr/> <p>4. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the window title is 'New Store' and the instruction is 'Enter a new Store and default path.' There are two input fields: 'Store name:' with the value 'Store' and 'Default path:' with the value '\\NA-CIFS-01-13\vdisk\$\Store'. A 'Browse...' button is next to the default path field. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.</p>

Instructions	Visual
<p>1. Provide the FQDN of the license server.</p> <p>2. Optionally, provide a port number if changed on the license server.</p> <p>3. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the window title is 'License Server' and the instruction is 'Enter the license server hostname and port.' There are two input fields: 'License server name:' with the value 'CTX-XD1.miniflexpod.local' and 'License server port:' with the value '27000'. Below these fields is a checkbox labeled 'Validate license server version and communication' which is checked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.</p>

Instructions	Visual
<p>4. If an Active Directory service account is not already setup for the PVS servers, create that account prior to clicking Next on this dialog.</p> <p>5. Select the Specified user account radio button.</p> <p>6. Complete the User name, Domain, Password, and Confirm password fields, using the PVS account information created earlier.</p> <p>7. Click Next</p>	 <p>The screenshot shows the 'User account' step of the Provisioning Services Configuration Wizard. It prompts the user to select an account type: 'Network service account' (unselected) or 'Specified user account' (selected). Under 'Specified user account', there are four input fields: 'User name' (Administrator), 'Domain' (miniflexpod), 'Password' (masked with dots), and 'Confirm password' (masked with dots). A note at the bottom states: 'Note: The database will be configured for access from this account.' At the bottom right, the '< Back' and 'Next >' buttons are visible, with 'Next >' highlighted by a red box.</p>

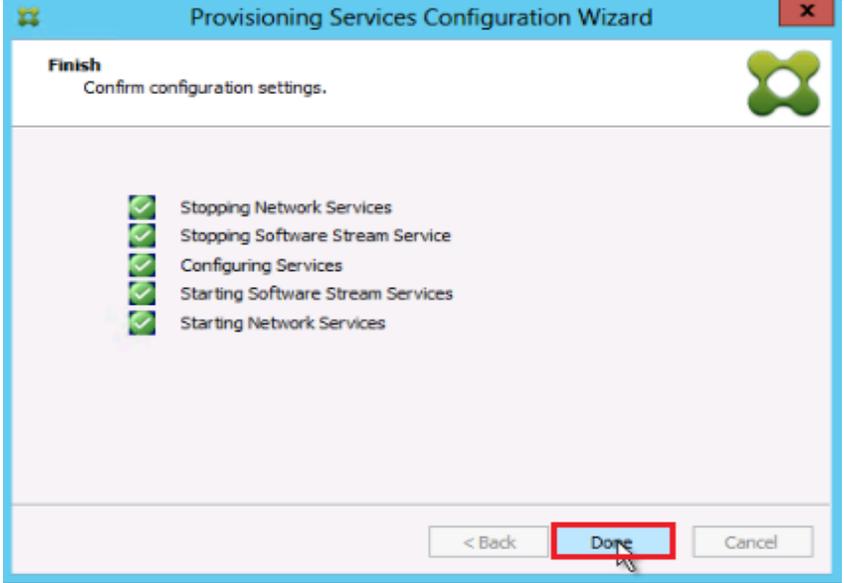
Instructions	Visual
<p>1. Set the Days between password updates to 30.</p> <hr/> <p> This will vary per environment. "30 days" for the configuration was appropriate for testing purposes.</p> <hr/> <p>2. Click Next</p>	 <p>The screenshot shows the 'Active Directory Computer Account Password' step of the Provisioning Services Configuration Wizard. It asks to 'Automate computer account password updates?'. The checkbox is checked. Below it, there is a dropdown menu for 'Days between password updates' which is currently set to '30'. At the bottom right, the '< Back' and 'Next >' buttons are visible, with 'Next >' highlighted by a red box.</p>

Instructions	Visual
<p>3. Keep the defaults for the network cards.</p> <p>4. Click Next</p>	 <p>Provisioning Services Configuration Wizard</p> <p>Network Communications Specify network settings.</p> <p>Streaming network cards: <input checked="" type="checkbox"/> 10.10.21.38</p> <p>Management network card: <input type="checkbox"/> 10.10.21.38</p> <p>Enter the base port that will be used for network communications. A total of 20 ports are required. You must also select a port for console communications.</p> <p>Note: All servers must have the same port configurations.</p> <p>First communications port: <input type="text" value="6890"/></p> <p>Console port: <input type="text" value="54321"/></p> <p>< Back Next > Cancel</p>

Instructions	Visual
<p>1. Select Use the Provisioning Services TFTP service checkbox.</p> <p>2. Click Next</p>	 <p>Provisioning Services Configuration Wizard</p> <p>TFTP Option and Bootstrap Location Typically only one TFTP server is deployed as part of Provisioning Services.</p> <p><input checked="" type="checkbox"/> Use the Provisioning Services TFTP service</p> <p>C:\ProgramData\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN <input type="button" value="Browse..."/></p> <p>< Back Next > Cancel</p>

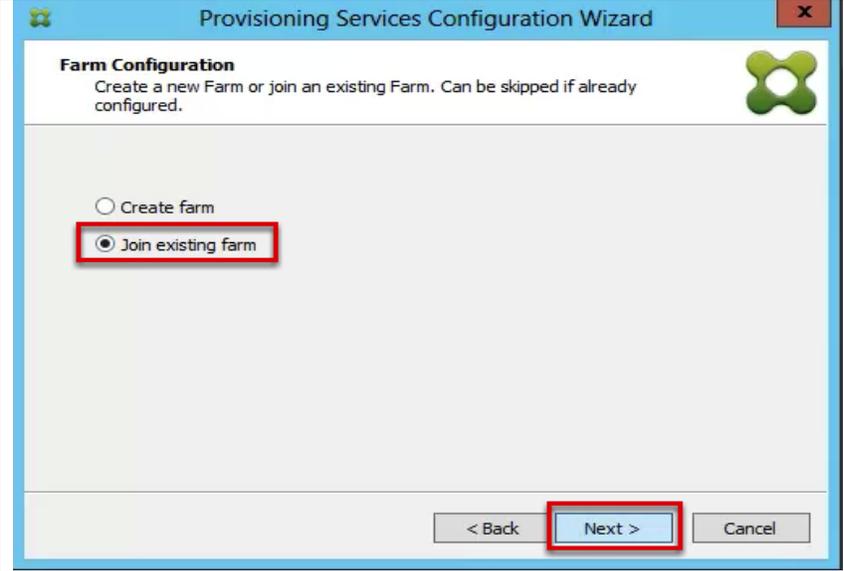
<p>Instructions</p>	<p>Visual</p>
<p>3. Make sure that the IP Addresses for all PVS servers are listed in the Stream Servers Boot List</p> <p>4. Click Next</p>	

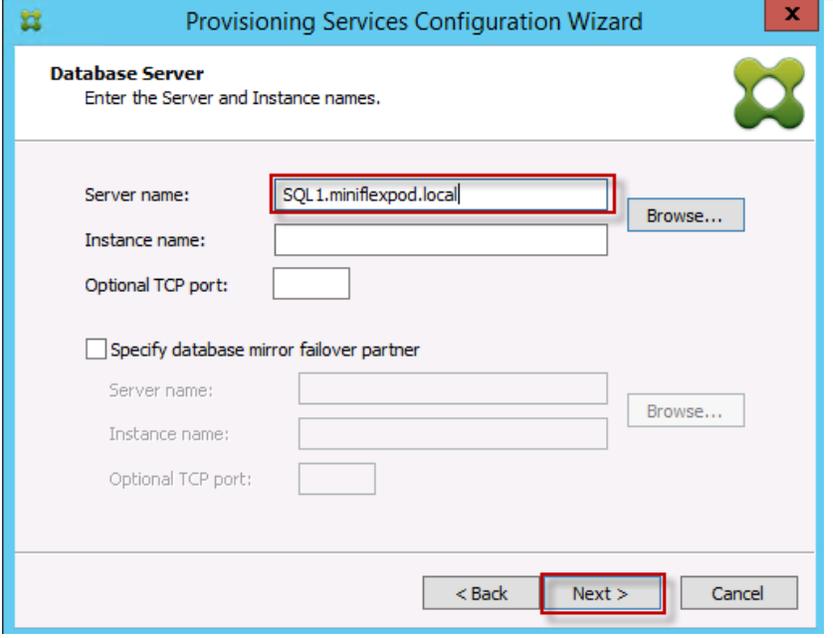
<p>Instructions</p>	<p>Visual</p>
<p>1. Click Finish to start installation.</p>	

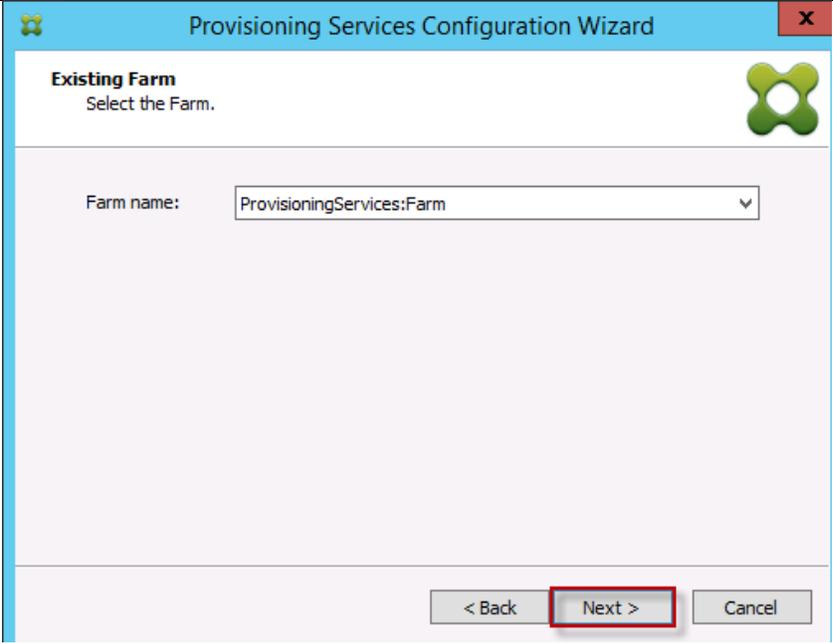
Instructions	Visual
<p>2. When the installation is completed, click the Done button.</p>	

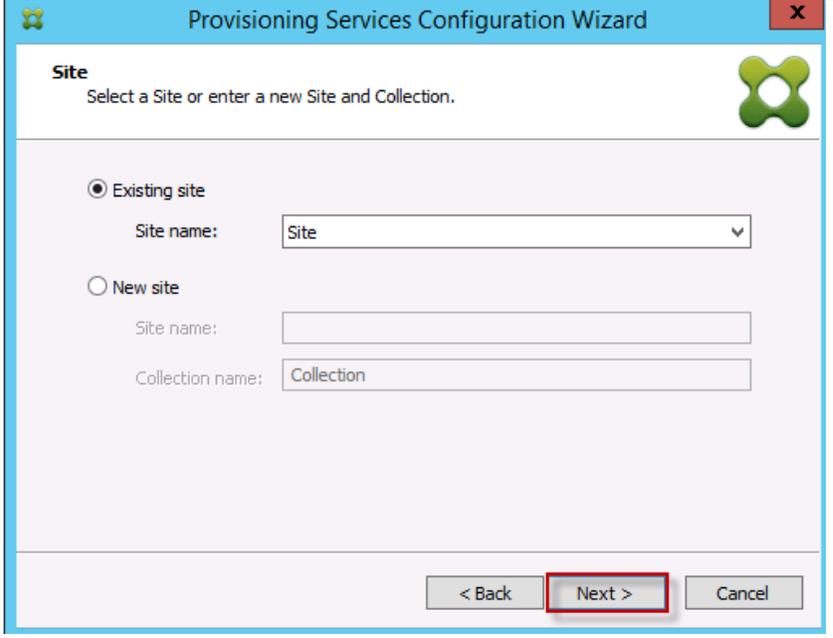
Install Additional PVS Servers

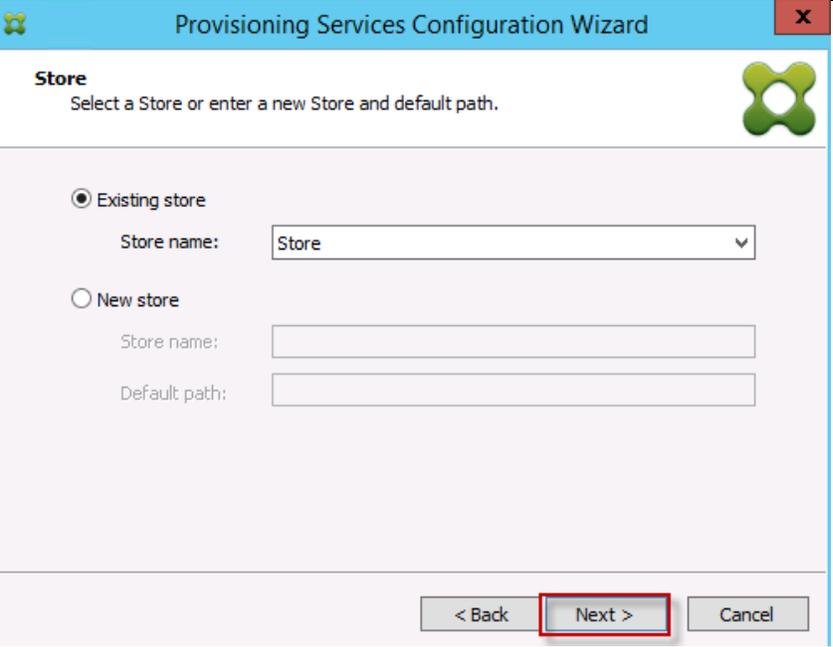
Complete the same installation steps on the additional PVS servers up to the configuration step where it asks to Create or Join a farm. In this CVD, we repeated the procedure to add the second PVS servers

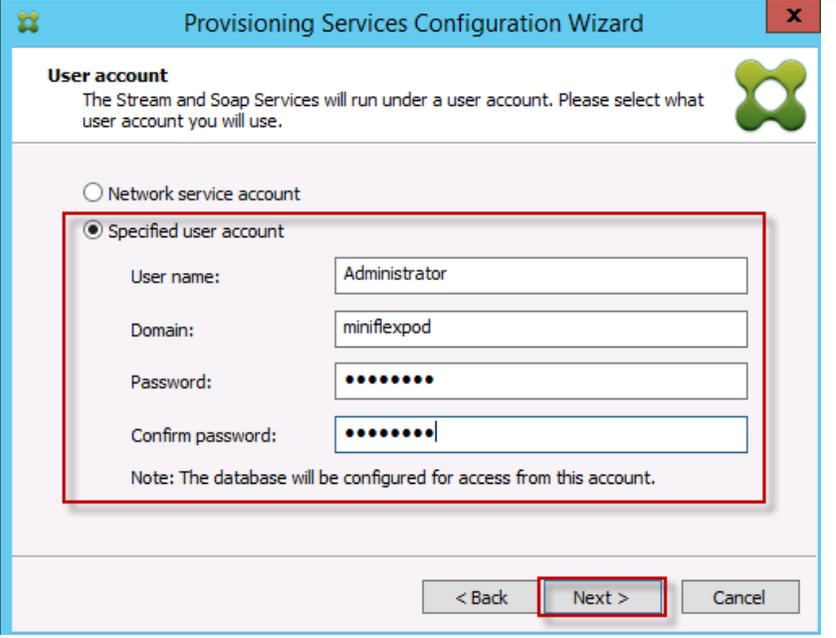
Instructions	Visual
<p>1. On the Farm Configuration dialog, select “Join existing farm.”</p> <p>2. Click Next</p>	

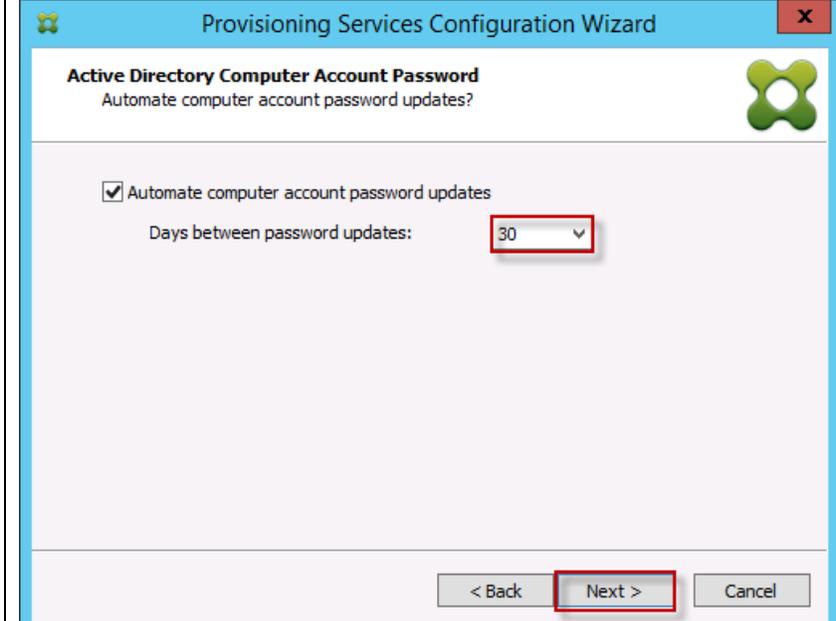
Instructions	Visual
<p>3. Provide the FQDN of the SQL Server.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Database Server' step of the 'Provisioning Services Configuration Wizard'. The title bar reads 'Provisioning Services Configuration Wizard' with a close button (X) on the right. Below the title bar, the text 'Database Server' is followed by 'Enter the Server and Instance names.' and a green logo. The form contains the following fields: 'Server name:' with the value 'SQL1.miniflexpod.local' (highlighted with a red box), 'Instance name:', and 'Optional TCP port:'. To the right of the 'Server name' field is a 'Browse...' button. Below these fields is a checkbox labeled 'Specify database mirror failover partner'. Underneath this checkbox are three more fields: 'Server name:', 'Instance name:', and 'Optional TCP port:', each with a 'Browse...' button to its right. At the bottom of the wizard, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

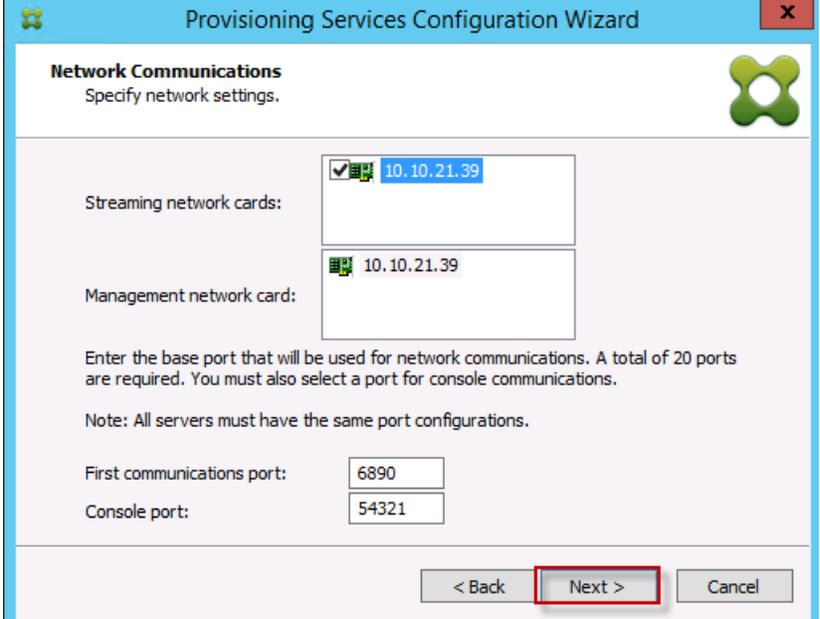
Instructions	Visual
<p>1. Accept the Farm Name.</p> <p>2. Click Next.</p>	 <p>The screenshot shows the 'Existing Farm' step of the 'Provisioning Services Configuration Wizard'. The title bar reads 'Provisioning Services Configuration Wizard' with a close button (X) on the right. Below the title bar, the text 'Existing Farm' is followed by 'Select the Farm.' and a green logo. The form contains a single field: 'Farm name:' with a dropdown menu showing 'ProvisioningServices:Farm'. At the bottom of the wizard, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

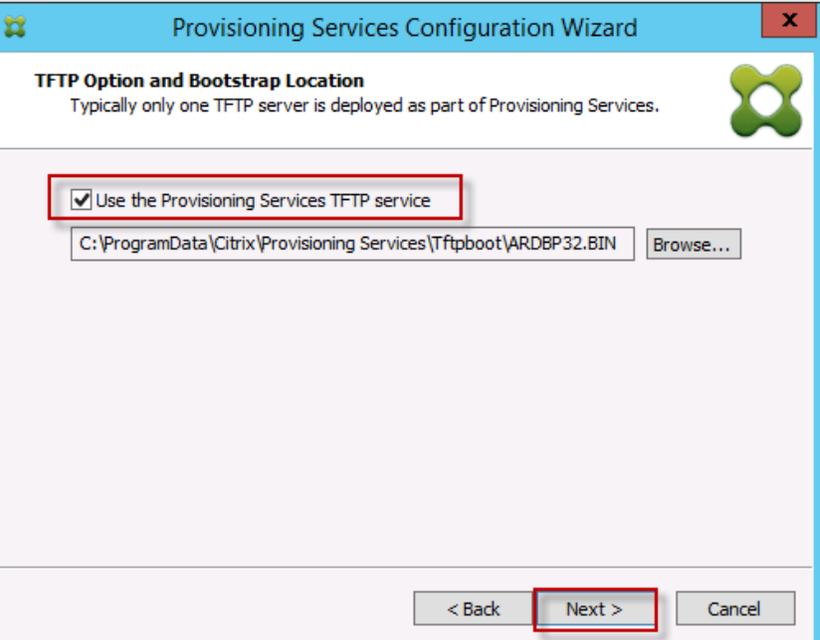
Instructions	Visual
<p>3. Accept the Existing Site.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar is blue with a green icon on the left and a red 'X' on the right. The main content area is white with a blue header that says 'Site' and 'Select a Site or enter a new Site and Collection.' Below this, there are two radio button options: 'Existing site' (which is selected) and 'New site'. Under 'Existing site', there is a 'Site name:' label followed by a dropdown menu showing 'Site'. Under 'New site', there are two text input fields: 'Site name:' and 'Collection name:' with the text 'Collection' entered in the second field. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangular border.</p>

Instructions	Visual
<p>1. Accept the existing vDisk store.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar is blue with a green icon on the left and a red 'X' on the right. The main content area is white with a blue header that says 'Store' and 'Select a Store or enter a new Store and default path.' Below this, there are two radio button options: 'Existing store' (which is selected) and 'New store'. Under 'Existing store', there is a 'Store name:' label followed by a dropdown menu showing 'Store'. Under 'New store', there are two text input fields: 'Store name:' and 'Default path:'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangular border.</p>

Instructions	Visual
<p>3. Provide the PVS service account information.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the section is titled 'User account' with a sub-header: 'The Stream and Soap Services will run under a user account. Please select what user account you will use.' There are two radio button options: 'Network service account' (unselected) and 'Specified user account' (selected). The 'Specified user account' section is enclosed in a red box and contains four input fields: 'User name' with the text 'Administrator', 'Domain' with 'miniflexpod', 'Password' with masked characters, and 'Confirm password' with masked characters. Below these fields is a note: 'Note: The database will be configured for access from this account.' At the bottom of the window, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

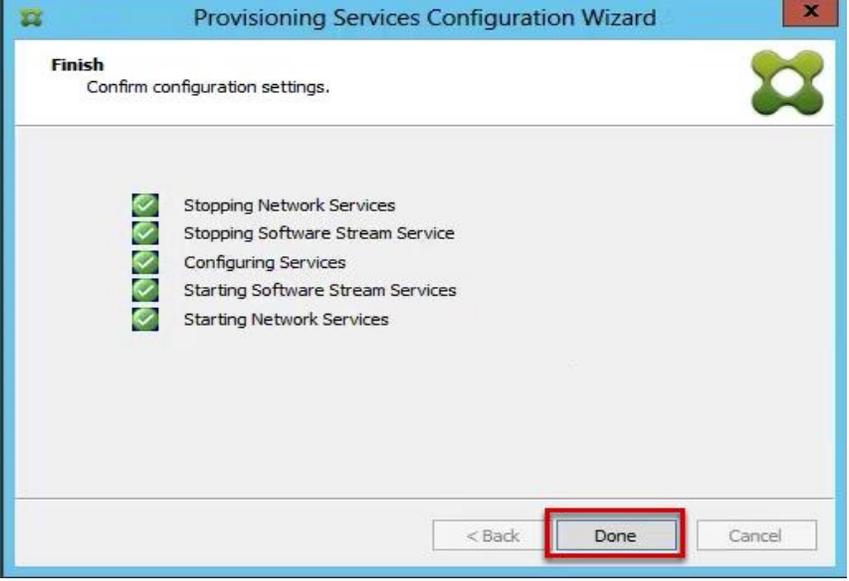
Instructions	Visual
<p>1. Set the Days between password updates to 30.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Provisioning Services Configuration Wizard' window. The title bar reads 'Provisioning Services Configuration Wizard'. Below the title bar, the section is titled 'Active Directory Computer Account Password' with a sub-header: 'Automate computer account password updates?'. There is a checked checkbox labeled 'Automate computer account password updates'. Below this, there is a label 'Days between password updates:' followed by a dropdown menu showing the value '30'. The dropdown menu is highlighted with a red box. At the bottom of the window, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.</p>

Instructions	Visual
<p>3. Accept the network card settings.</p> <p>4. Click Next</p>	 <p>Provisioning Services Configuration Wizard</p> <p>Network Communications Specify network settings.</p> <p>Streaming network cards: <input checked="" type="checkbox"/> 10.10.21.39</p> <p>Management network card: 10.10.21.39</p> <p>Enter the base port that will be used for network communications. A total of 20 ports are required. You must also select a port for console communications.</p> <p>Note: All servers must have the same port configurations.</p> <p>First communications port: 6890</p> <p>Console port: 54321</p> <p>< Back Next > Cancel</p>

Instructions	Visual
<p>1. Select Use the Provisioning Services TFTP service checkbox.</p> <p>2. Click Next</p>	 <p>Provisioning Services Configuration Wizard</p> <p>TFTP Option and Bootstrap Location Typically only one TFTP server is deployed as part of Provisioning Services.</p> <p><input checked="" type="checkbox"/> Use the Provisioning Services TFTP service</p> <p>C:\ProgramData\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN <input type="button" value="Browse..."/></p> <p>< Back Next > Cancel</p>

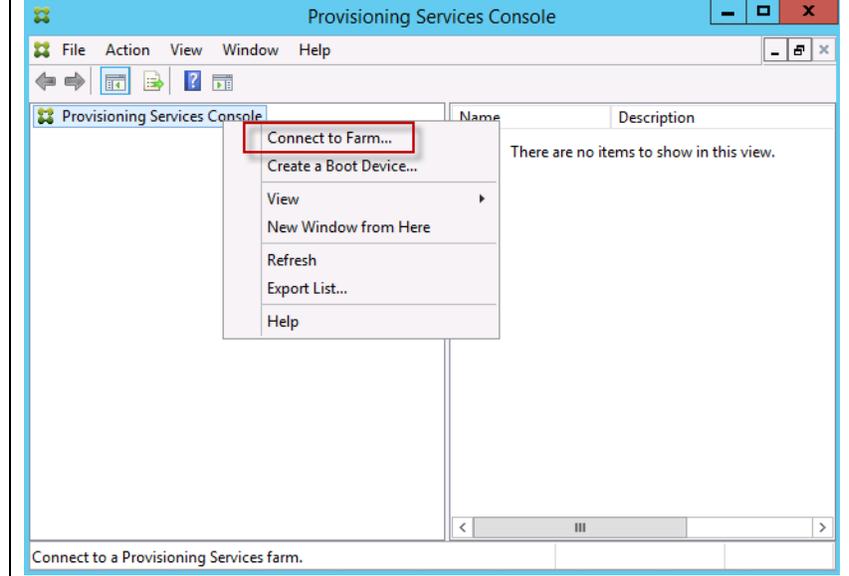
<p>Instructions</p>	<p>Visual</p>
<p>3. Make sure that the IP Addresses for all PVS servers are listed in the Stream Servers Boot List</p> <p>4. Click Next</p>	

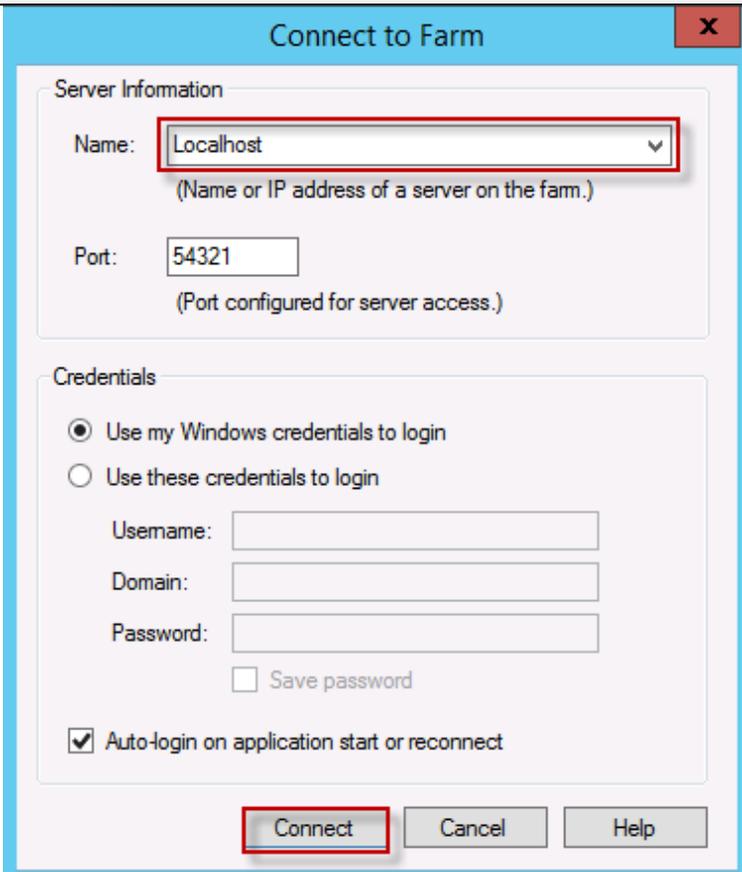
<p>Instructions</p>	<p>Visual</p>
<p>1. Click Finish to start the installation process.</p>	

<p>Instructions</p>	<p>Visual</p>
<p>2. Click Done when the installation finishes</p>	

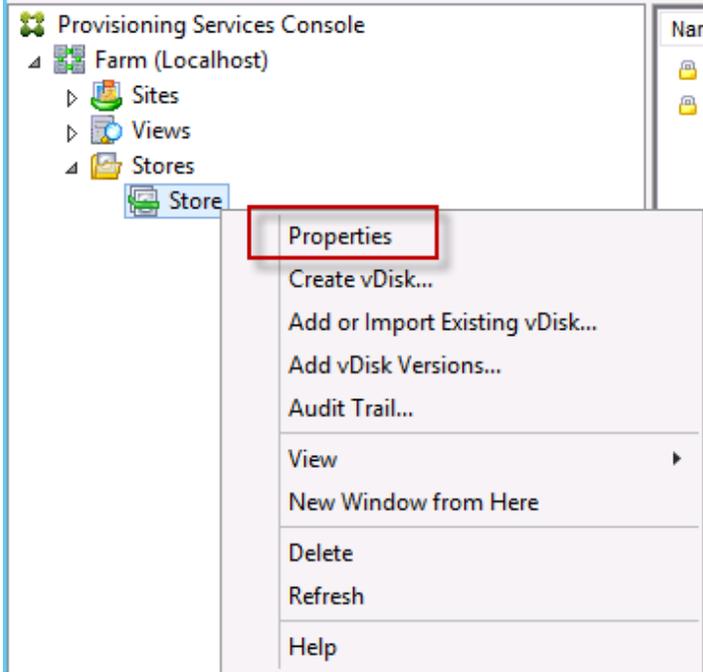
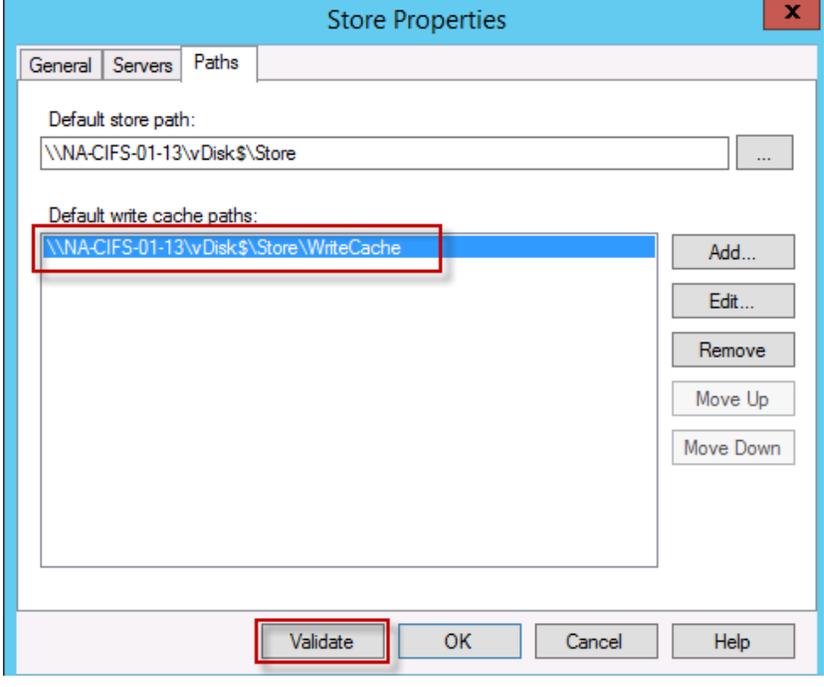
Optionally, you can install the Provisioning Services console on the second PVS server following the procedure in section Installing Provisioning Services.

After completing the steps to install the second PVS server, launch the Provisioning Services Console to verify that the PVS Servers and Stores are configured and that DHCP boot options are defined.

<p>Instructions</p>	<p>Visual</p>
<p>1. Launch Provisioning Services Console and select Connect to Farm</p>	

<p>Instructions</p>	<p>Visual</p>
<p>2. Enter localhost for the PVS1 server</p> <p>3. Click Connect</p>	 <p>The screenshot shows a dialog box titled "Connect to Farm" with a close button (X) in the top right corner. It is divided into two sections: "Server Information" and "Credentials".</p> <p>Server Information:</p> <ul style="list-style-type: none"> Name: A dropdown menu showing "Localhost" is highlighted with a red box. Below it is the text "(Name or IP address of a server on the farm.)". Port: A text box containing "54321". Below it is the text "(Port configured for server access.)". <p>Credentials:</p> <ul style="list-style-type: none"> Two radio buttons are present: "Use my Windows credentials to login" (which is selected) and "Use these credentials to login". Below the radio buttons are three text boxes labeled "Username:", "Domain:", and "Password:". A checkbox labeled "Save password" is located below the "Password:" field. A checked checkbox labeled "Auto-login on application start or reconnect" is at the bottom of the credentials section. <p>At the bottom of the dialog box, there are three buttons: "Connect" (highlighted with a red box), "Cancel", and "Help".</p>

<p>Instructions</p>	<p>Visual</p>
---------------------	---------------

Instructions	Visual
<p>1. Select Store Properties from the drop-down menu</p>	 <p>The screenshot shows the Provisioning Services Console interface. The tree view on the left is expanded to 'Stores' > 'Store'. A context menu is open over the 'Store' folder, with the 'Properties' option highlighted by a red rectangular box. Other menu items include 'Create vDisk...', 'Add or Import Existing vDisk...', 'Add vDisk Versions...', 'Audit Trail...', 'View', 'New Window from Here', 'Delete', 'Refresh', and 'Help'.</p>
<p>2. In the Store Properties dialog, add the Default store path to the list of Default write cache paths.</p> <p>3. Click Validate. If the validation is successful, click OK to continue.</p>	 <p>The screenshot shows the 'Store Properties' dialog box with the 'Paths' tab selected. The 'Default store path' field contains '\\NA-CIFS-01-13\wDisk\$\Store'. Below it, the 'Default write cache paths' list contains one entry: '\\NA-CIFS-01-13\wDisk\$\Store\WriteCache', which is highlighted with a red rectangular box. To the right of the list are buttons for 'Add...', 'Edit...', 'Remove', 'Move Up', and 'Move Down'. At the bottom of the dialog, the 'Validate' button is highlighted with a red rectangular box, along with 'OK', 'Cancel', and 'Help' buttons.</p>

Create the Provisioning Services Master Image

In this section we will describe the steps to create the master image to be used in this solution. Because of the unique nature of having a shared group of local disks, we need to approach the imaging process in three different steps. First apply the Boot Policy created earlier that boots from CD/DVD first, then local Hard Disk. This will allow us to install Windows Server 2012 R2 locally like you would any machine. Second, we would

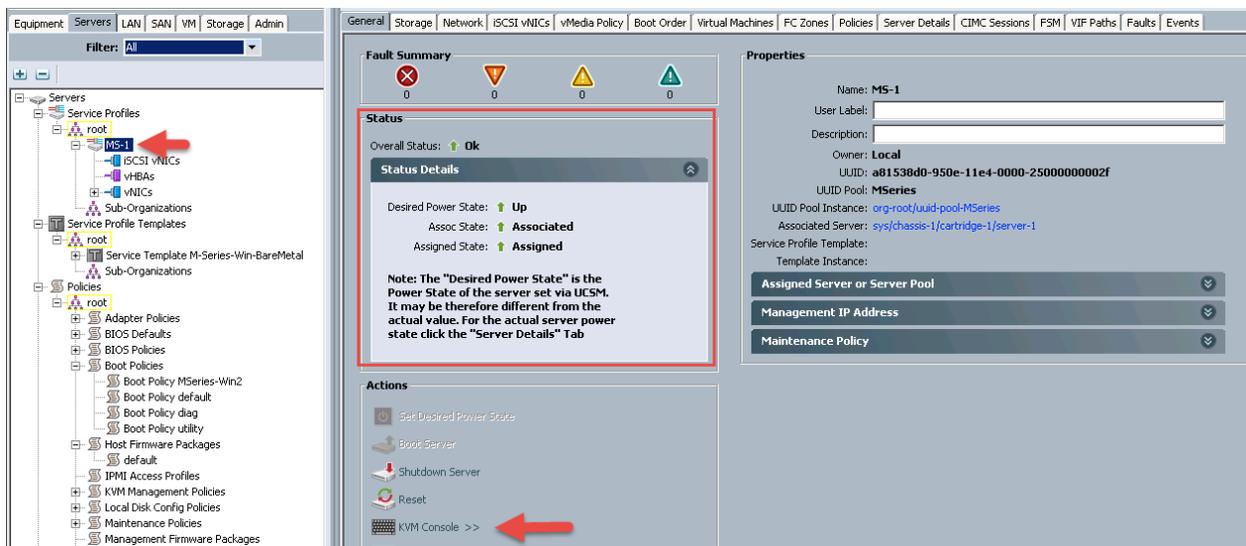
apply the Boot Policy that defines booting from PXE first, then local hard disk. This allows a PXE connection to the Citrix Provisioning Server to complete the imaging process. Last, after we have successfully taken the master image, we would apply the Boot Policy that is boot from PXE only.

The following Boot Policies were created for this solution:

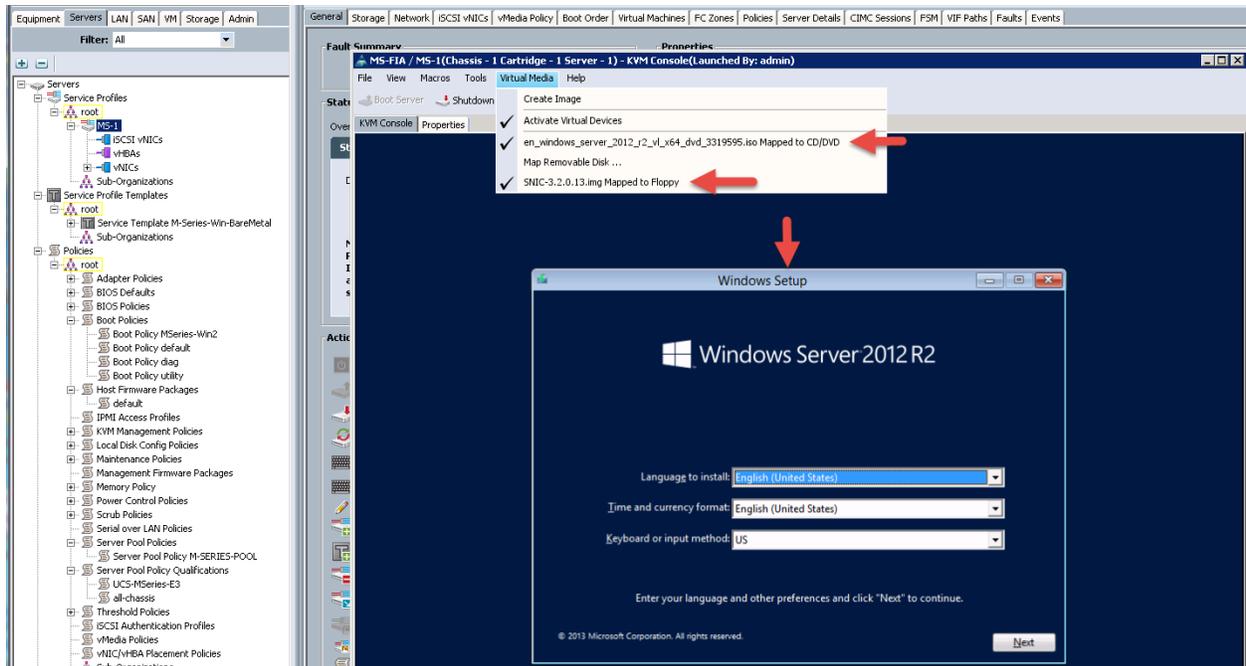
1. MSeries-Win2: Boot order is CD/DVD then Local Hard Disk. The purpose here is to install the first instance of Windows 2012 R2 Server to prepare for imaging.
2. CD-PXE-HDD: Is the boot policy created for the second step that will allow the cartridge server to PXE boot from PVS the load the master image from the local disk which will be copied to a Citrix PVS vDisk. This policy is only necessary for the actual copying of the local disk to the PVS server. It will be changed when imaging completes.
3. PXE-Boot: This is the final boot policy that will need to be applied for the cartridge servers to boot from the PVS servers. This is the last boot policy that will need to be applied in this solution.

To create the provisioning services master image, complete the following steps:

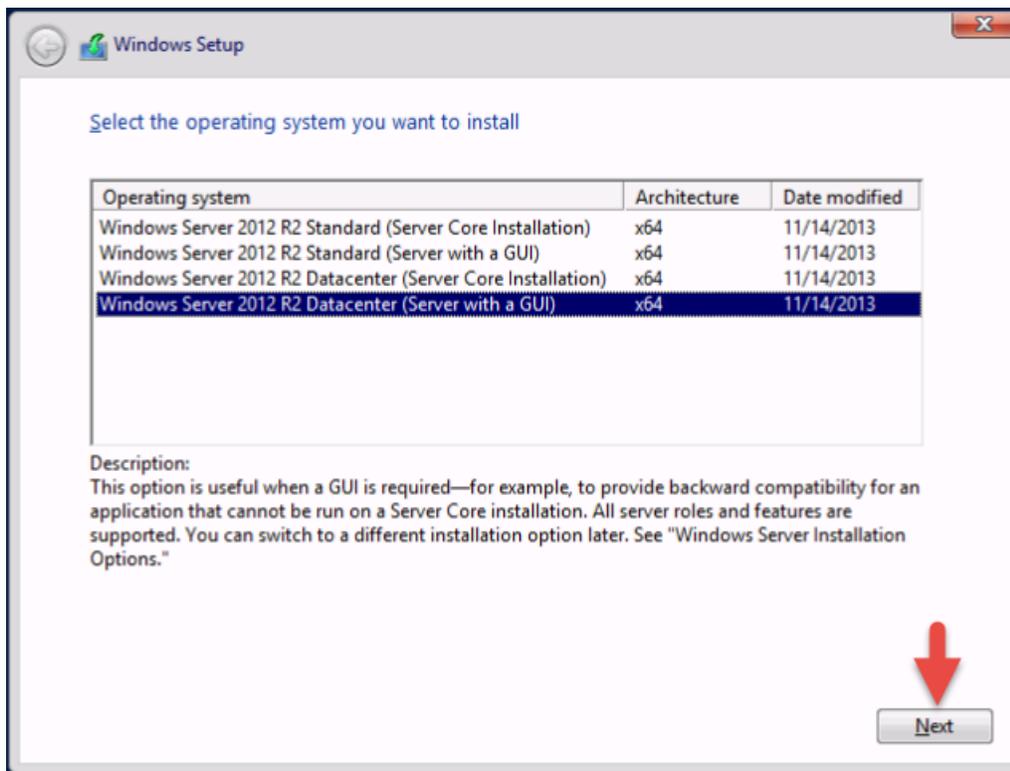
1. Apply the Service Profile Template created earlier to one server in the chassis and start the KVM.



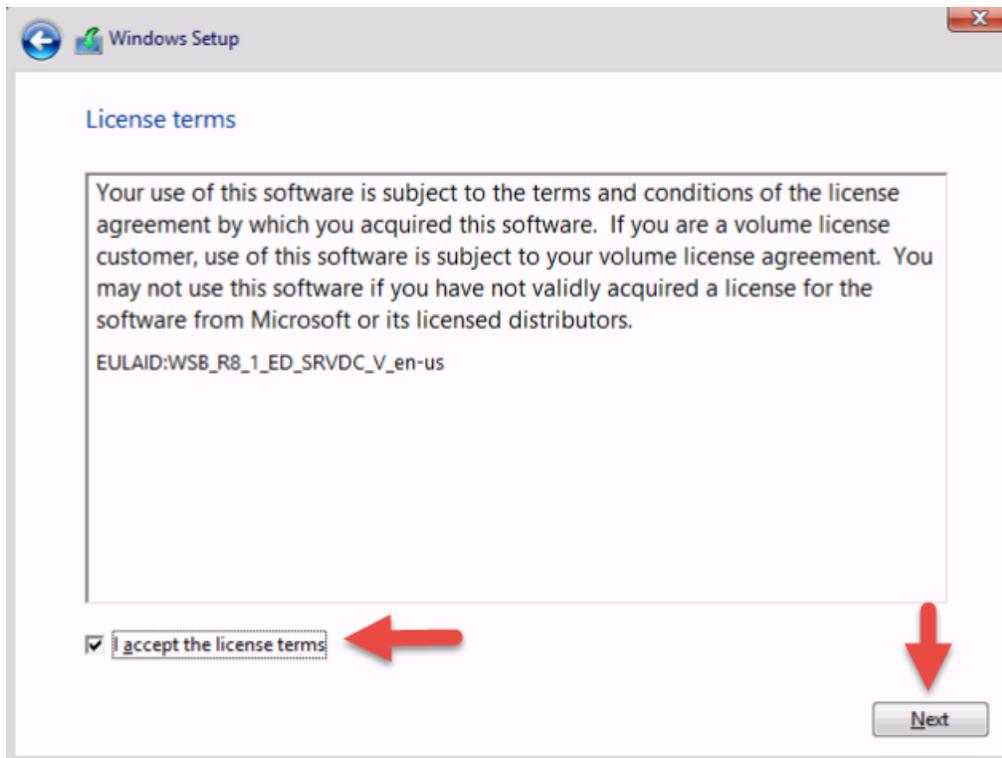
2. Map the Windows 2012 R2 ISO to the CD-ROM and the SNIC driver image to the Floppy Disk, then boot the server.



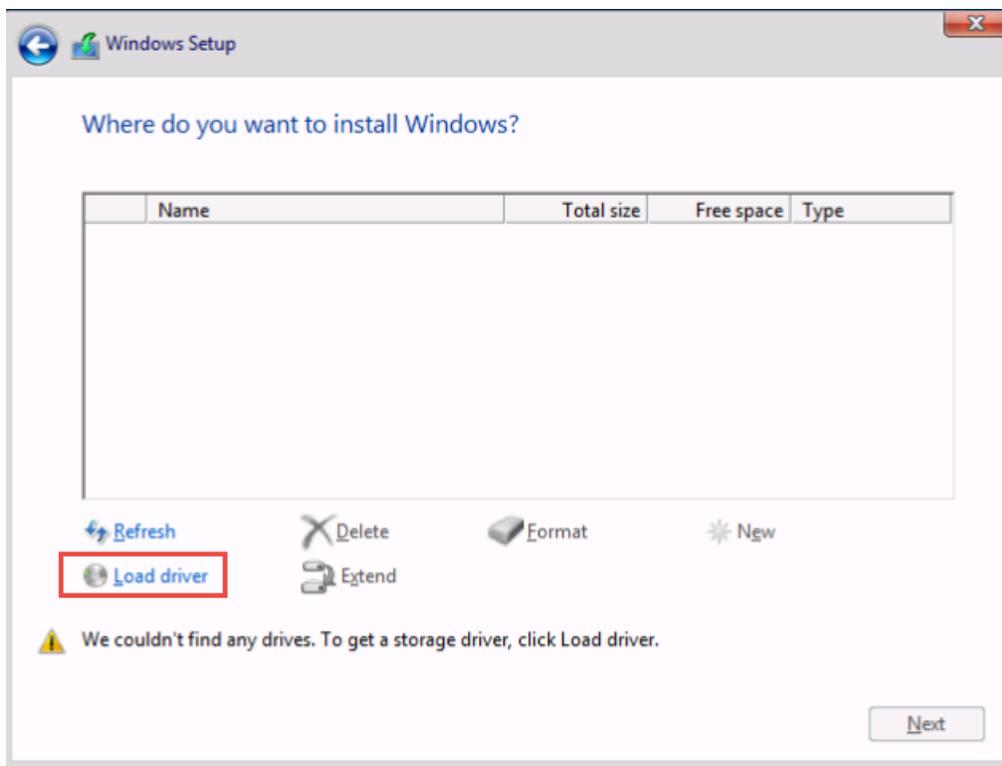
3. Proceed to install Windows Server 2012 R2.



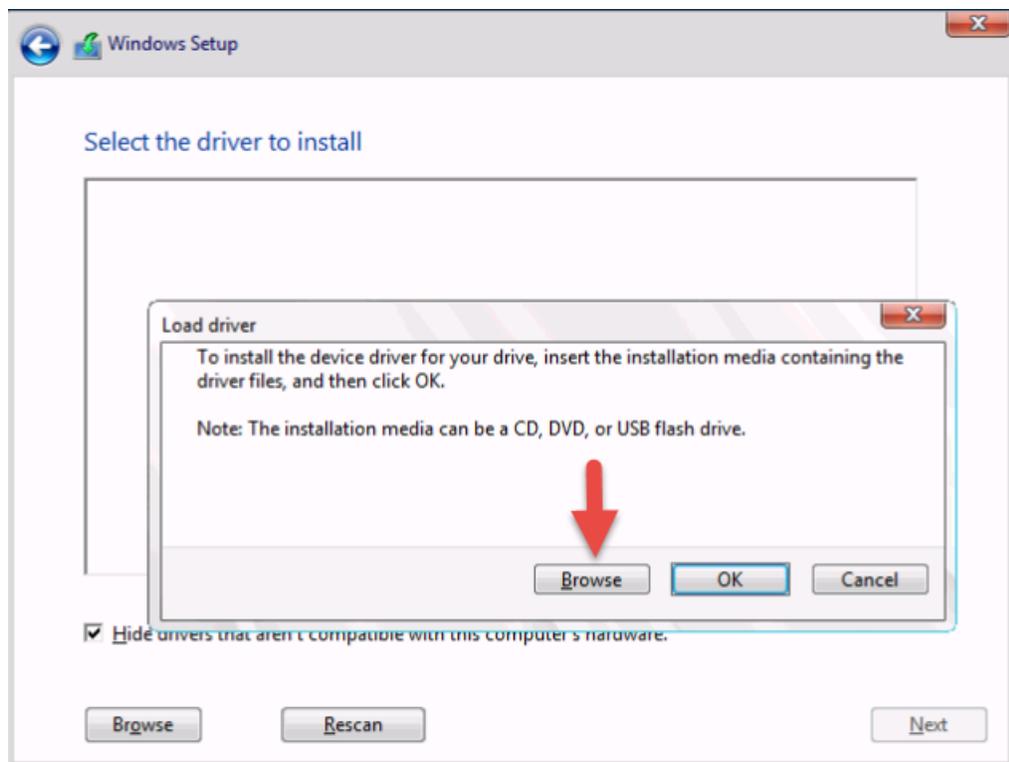
4. Accept the License Agreement.



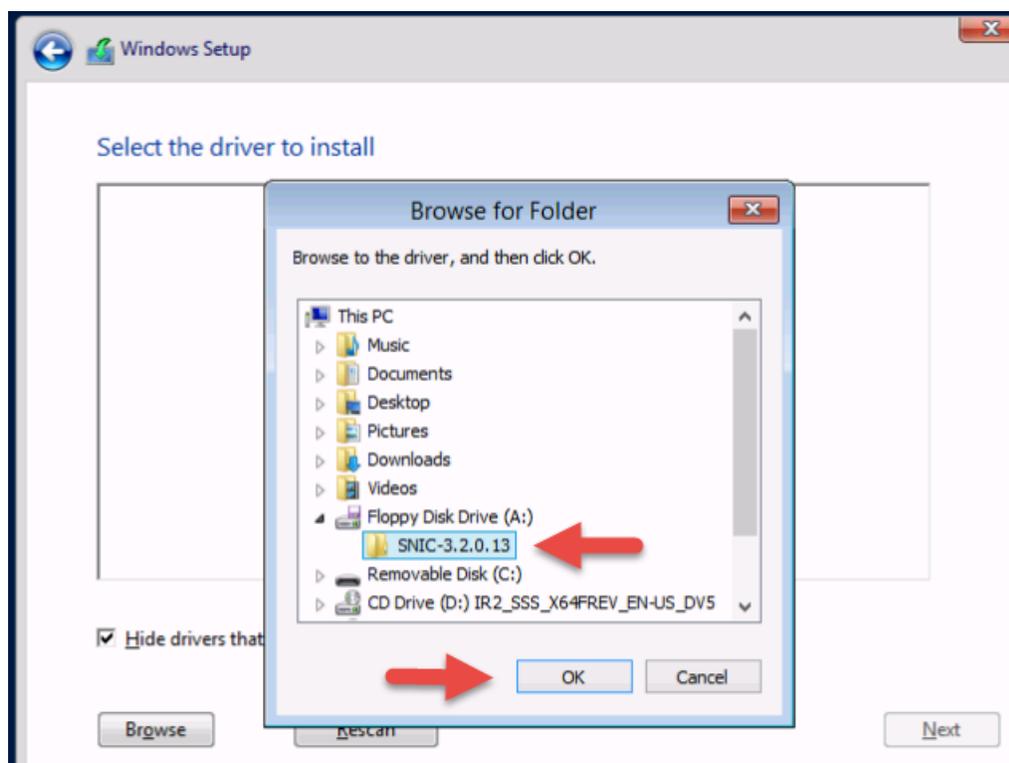
5. When prompted by the Windows install wizard to load additional drivers, select the 'Load Driver' button.



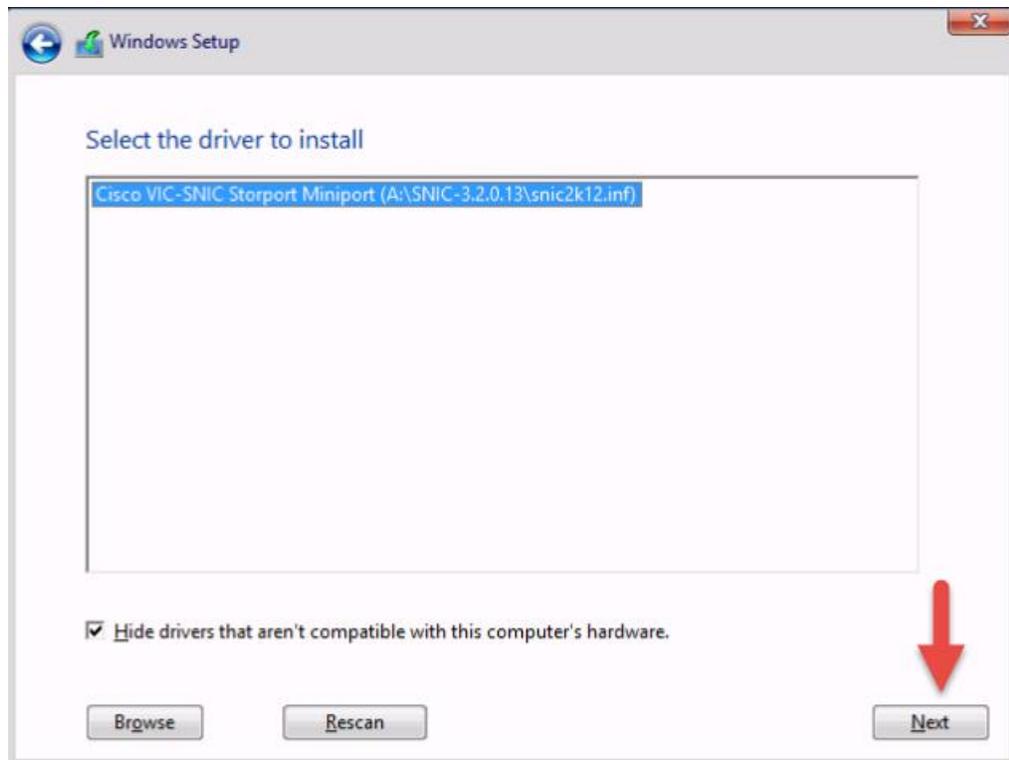
6. Click Browse.



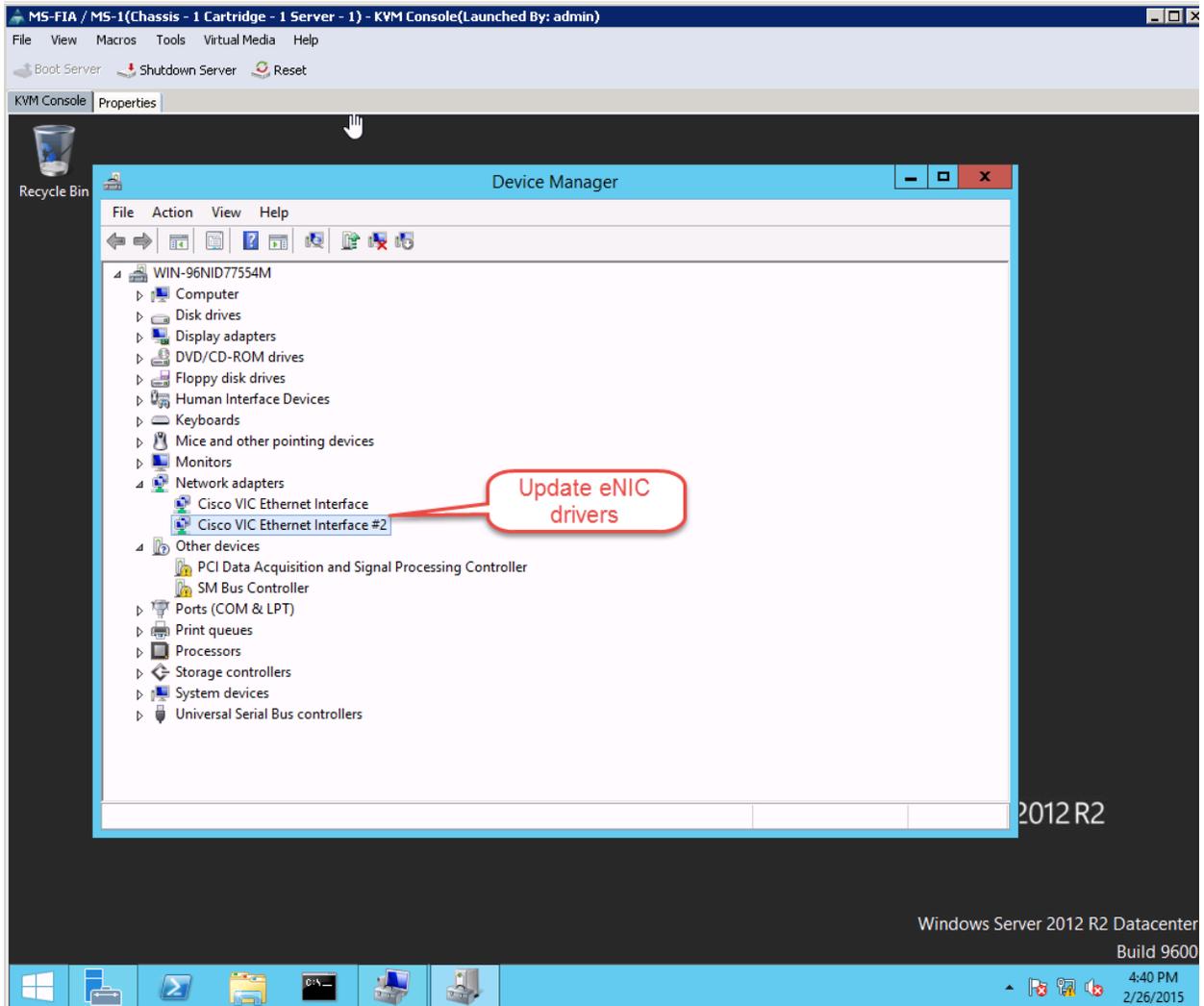
7. Expand the floppy drive and select the SNIC driver, then click OK.



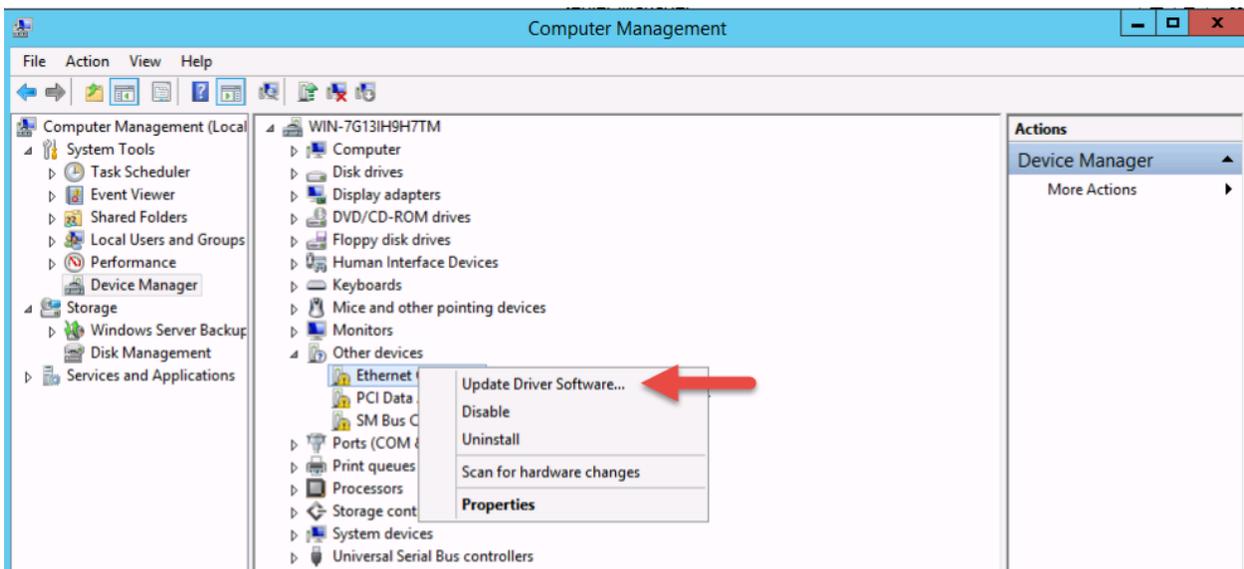
8. Click Next.



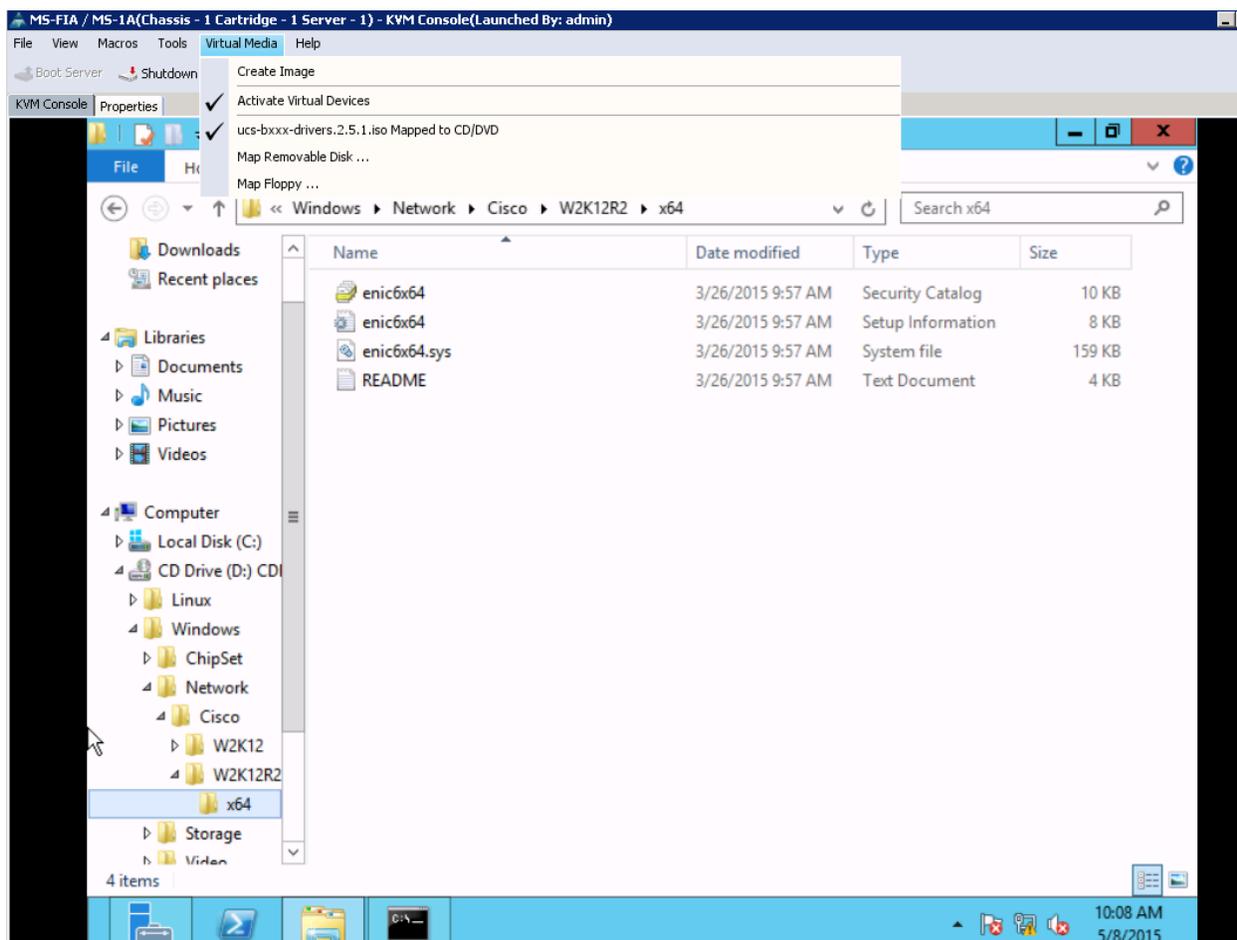
9. Click Next to finish the installation.
10. Mount the ucs-bxxx-drivers.2.5.1.iso on the KVM for the server.
11. When logged into Windows Desktop, open Device Manager, browse to the CD/DVD drive to update the Cisco eNIC drivers using the ucs-bxxx-drivers.2.5.1.iso mounted previously.



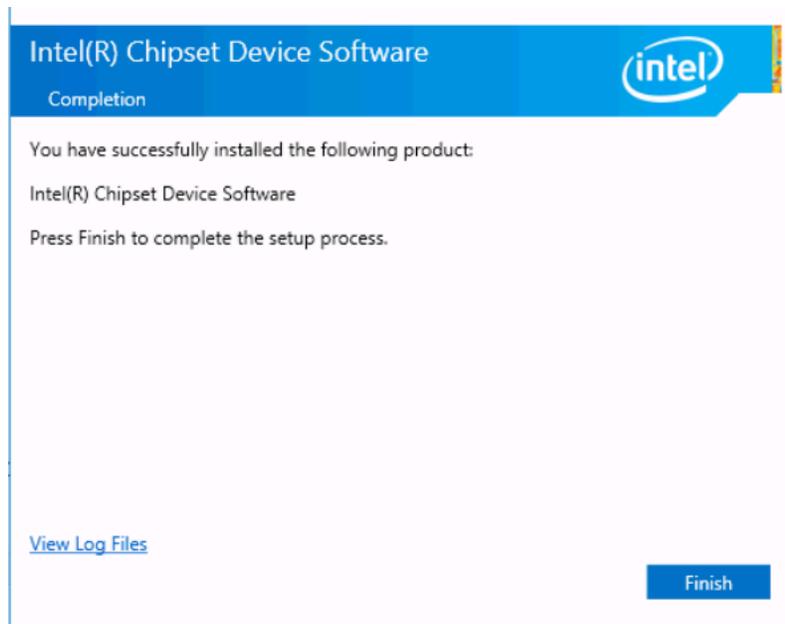
12. Update the driver software.



13. Choose Browse. Browse to \Windows\Network\Cisco\W2K12R2\x64 folder as the location of the updated driver.



14. Complete the NIC software update.
15. Click Finish. There should be no unknown devices in the Device Manager.
16. Choose Custom Install, then choose Load Driver on the Where do you want to install Windows dialog.
17. Allow the wizard to run and the completion notice will display.



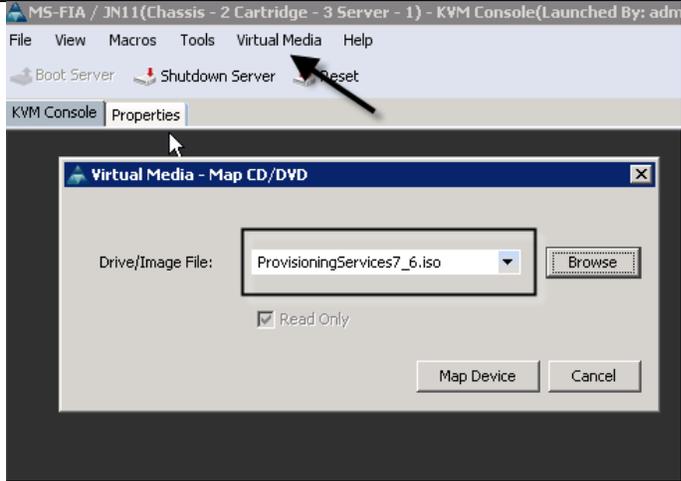
18. Apply Windows Updates as prescribed by your organization.
19. Join the server to the domain.
20. Install the Remote Desktop Services Host Session Role (detailed instructions here).
21. Microsoft Office 2010 SP1 or higher. (Office 2010 SP2 was used in this study).
22. In this study we installed the Login VSI 4.1.4 target machine software.
23. Install the Citrix Provisioning Services Target Device Software for imaging and streaming the master image. (Detailed in table and screen shots below)
24. Create a DHCP scope for the streamed servers and add options 66 and 67 to the scope options to point to the IP address of the PVS Servers (recommended to be load balanced with Citrix NetScaler in production environments) and the ardbp32.bin file respectively.
25. In the Citrix PVS Console, a device collection needs to be made to import the bare metal M-Series Cartridge servers.
26. Create a device in the collection with a name and the mac address of your bare metal install cartridge. Set the boot from Hard Disk. Save the machine.
27. Convert the bare metal server to a PVS vDisk using PVS 7.6. At the point where you are prompted to re-start with boot order, Network, HDD, shut the machine down gracefully. Change your SP to utilize the CD-PXE-HDD boot policy created earlier.
28. When the CD-PXE-HDD boot policy is applied, Citrix PVS imaging wizard will be able to pxe boot to the PVS server then copy the image to the vDisk to complete the imaging process.

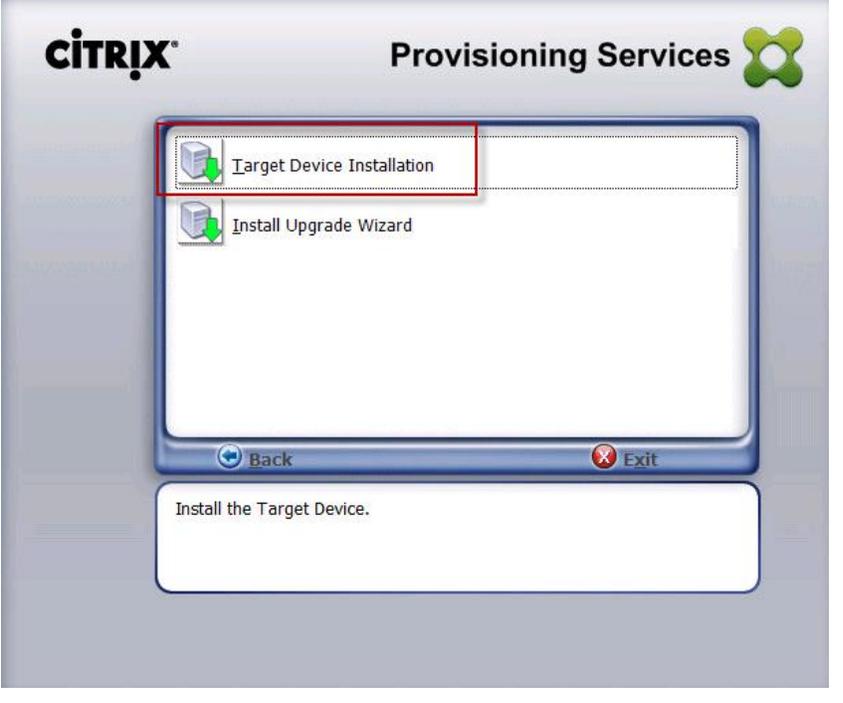
29. When imaging is complete, apply the PXE only boot policy to begin streaming from PVS to the bare metal cartridges.

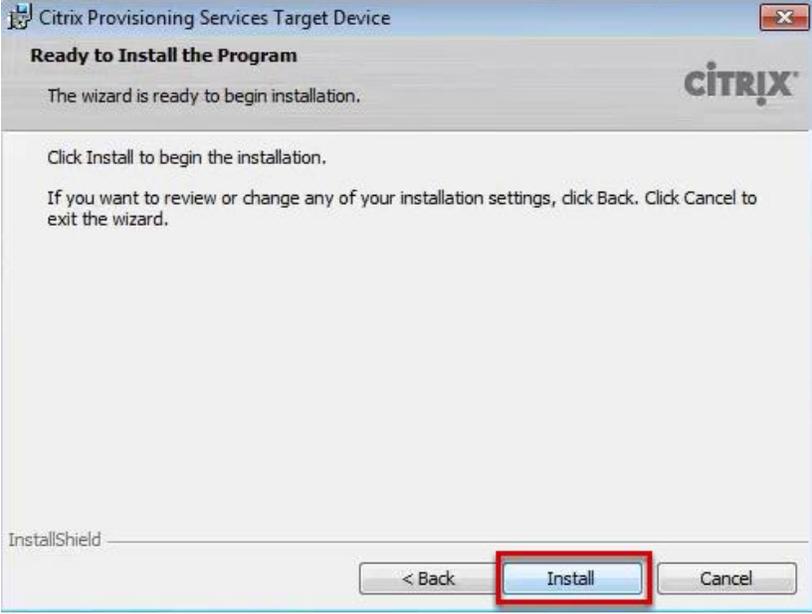
Install the PVS Target Device Software

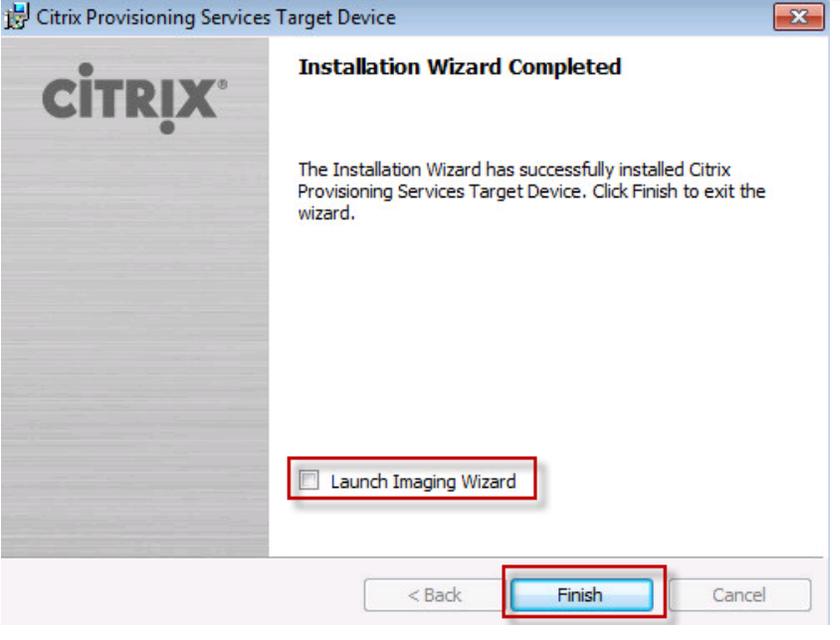
The Master Target Device refers to the target device from which a hard disk image is built and stored on a vDisk. Provisioning Services then streams the contents of the vDisk created to other target devices. This procedure installs the PVS Target Device software that is used to build the RDS and VDI golden images.

 The instructions below outline the installation procedure to configure a vDisk for VDI desktops. When you have completed these installation steps, repeat the procedure to configure a vDisk for RDS.

Instructions	Visual
<ol style="list-style-type: none"> 1. On the Master Target Device mount the PVS 7.6 iso in the KVM to begin the install. 2. Click Map Device to install. 	

Instructions	Visual
<p>4. Launch the PVS installer from the Provisioning Services 7.6 ISO.</p> <p>5. Click the Target Device Installation button</p>	 <p>The screenshot shows the Citrix Provisioning Services installer main menu. The title bar reads 'CITRIX Provisioning Services'. The main window contains a list of options: 'Console Installation', 'Server Installation', 'Target Device Installation', and 'Help and Support'. Each option is preceded by a server icon with a green arrow. The 'Target Device Installation' option is highlighted with a red rectangular box. At the bottom of the window, there are buttons for 'Browse DVD' and 'Exit'. Below the main window, a status bar displays the text 'Install the Console.'</p>
<p>1. Click the Target Device Installation button.</p> <p>The installation wizard will check to resolve dependencies and then begin the PVS target device installation process</p>	 <p>The screenshot shows the Citrix Provisioning Services installer wizard at a subsequent step. The title bar reads 'CITRIX Provisioning Services'. The main window contains a list of options: 'Target Device Installation' and 'Install Upgrade Wizard'. Each option is preceded by a server icon with a green arrow. The 'Target Device Installation' option is highlighted with a red rectangular box. At the bottom of the window, there are buttons for 'Back' and 'Exit'. Below the main window, a status bar displays the text 'Install the Target Device.'</p>

Instructions	Visual
<p>The wizard's Welcome page appears.</p> <p>2. Click Next.</p>	
<p>1. Confirm the installation settings and click Install.</p>	

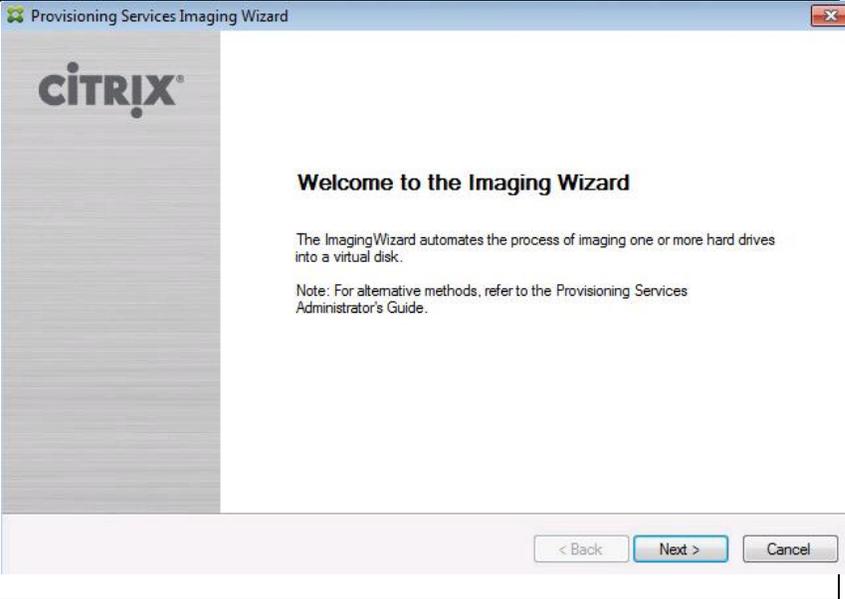
Instructions	Visual
<p>A confirmation screen appears indicating that the installation completed successfully.</p> <ol style="list-style-type: none"> Unlick the checkbox to launch the Imaging Wizard and click Finish. Reboot the machine 	

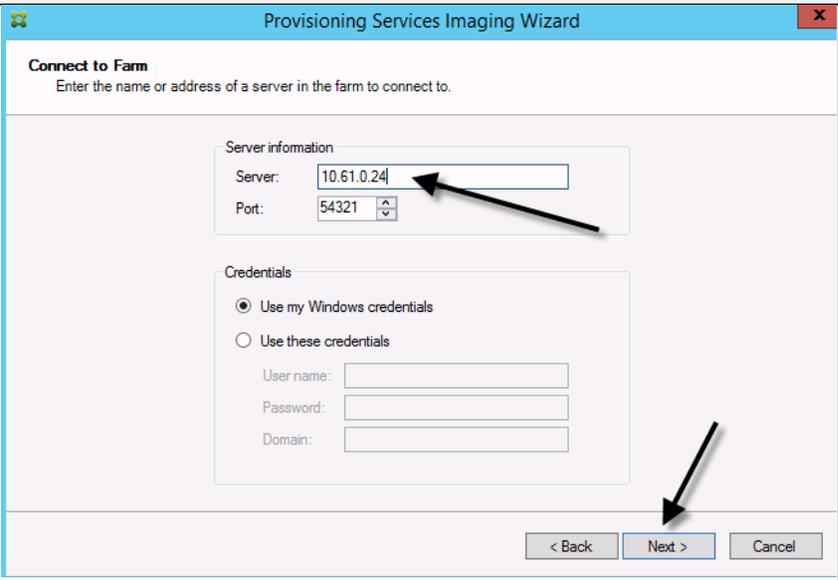
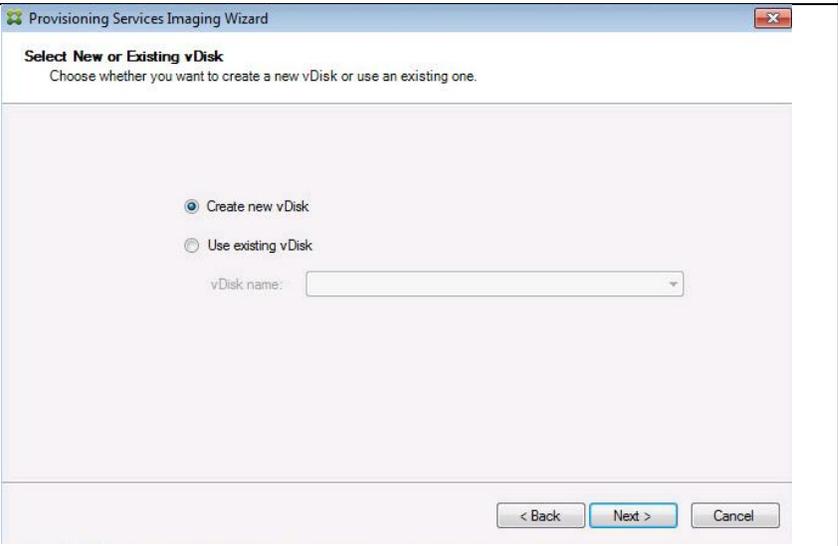
Creating PVS vDisks

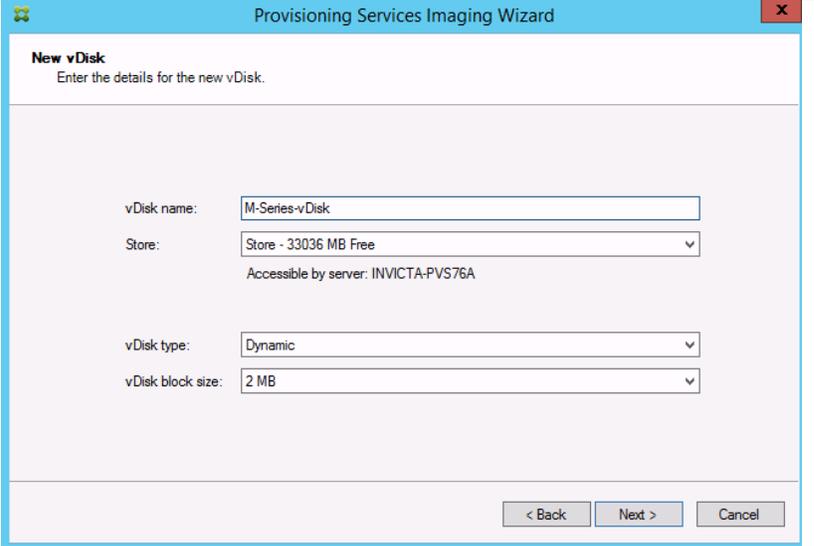
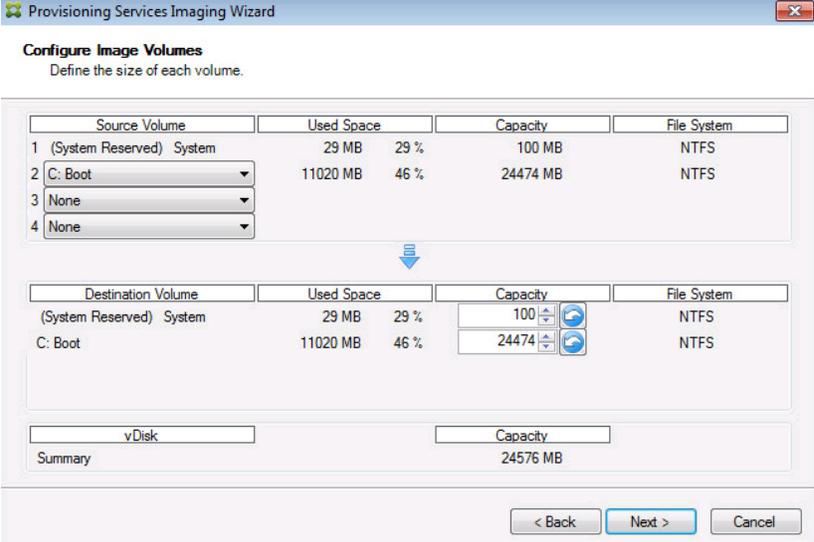
The PVS Imaging Wizard automatically creates a base vDisk image from the master target device. To create the PVS vDisks, complete the following steps.

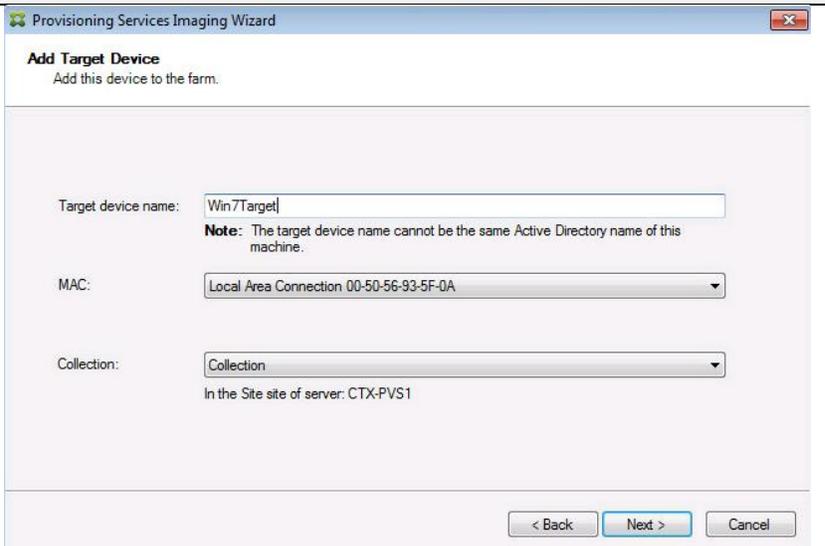
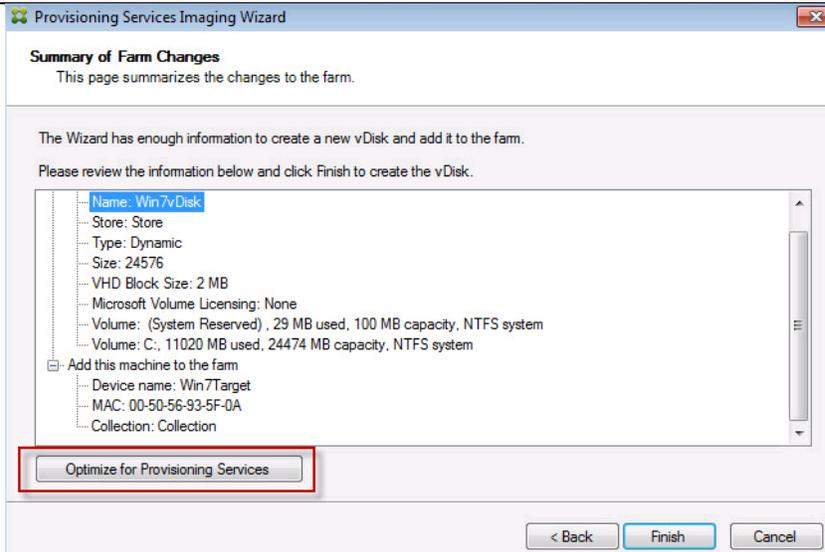


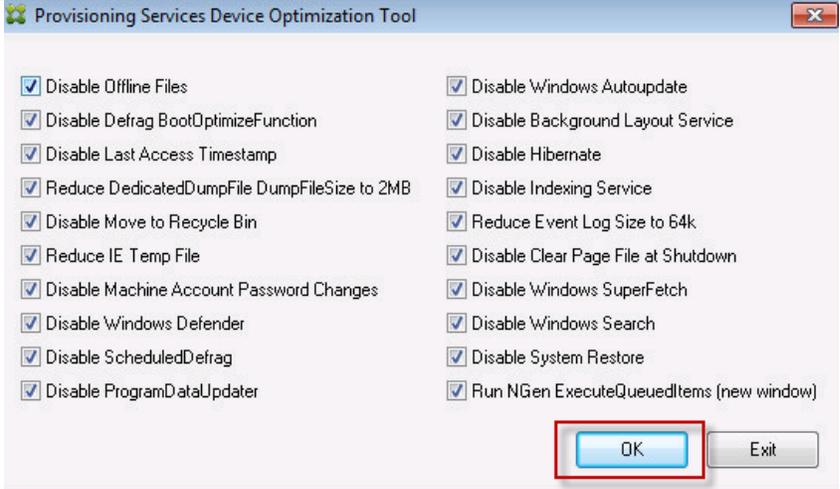
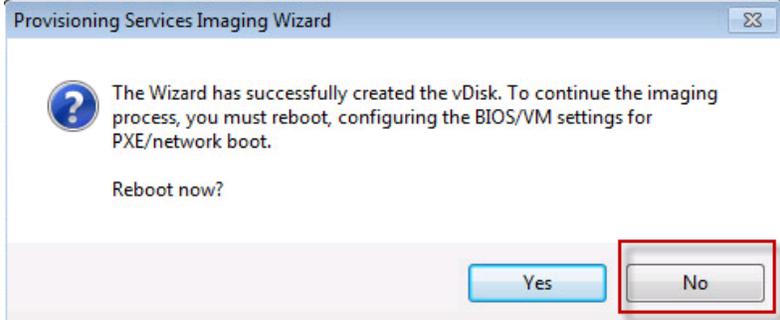
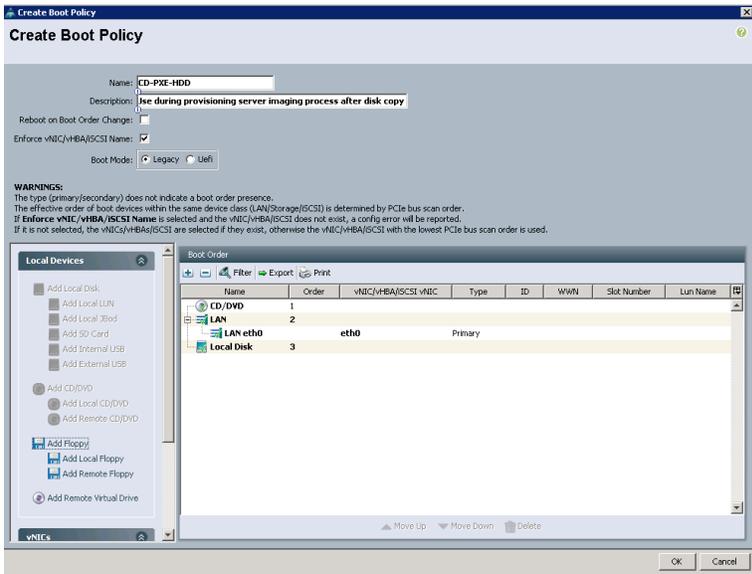
The following instructions describe the process of creating a vDisk for VDI desktops. When you have completed these steps, repeat the procedure to build a vDisk for RDS.

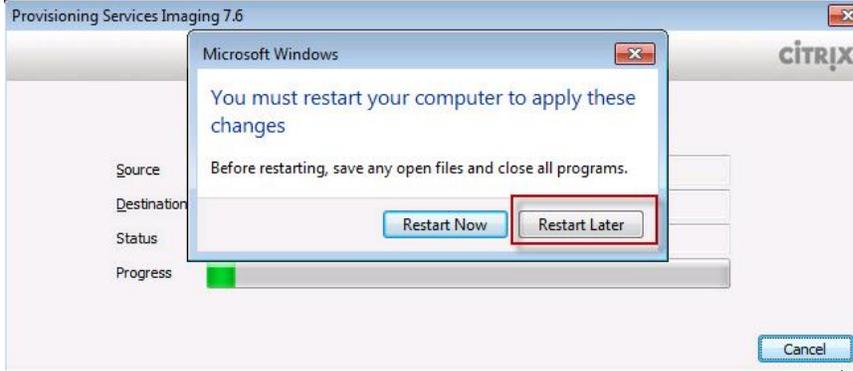
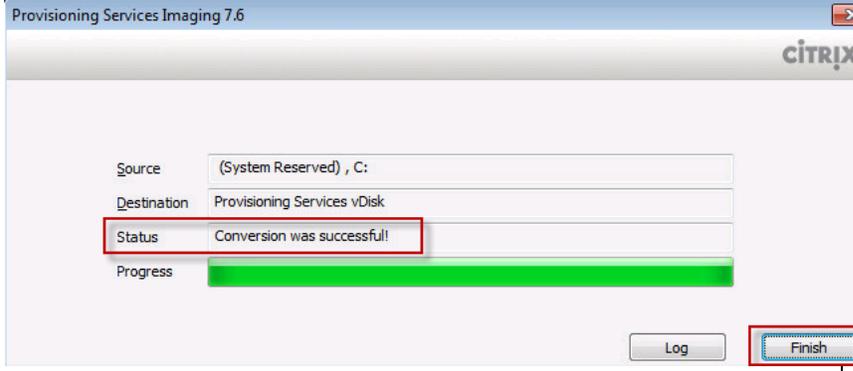
Instructions	Visual
<ol style="list-style-type: none"> The PVS Imaging Wizard's Welcome page appears. Click Next 	

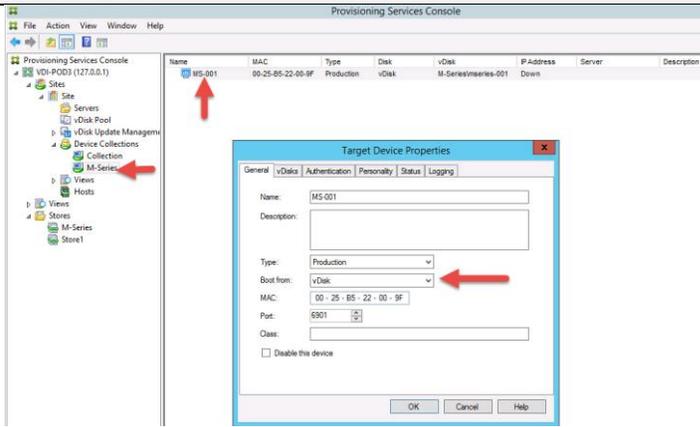
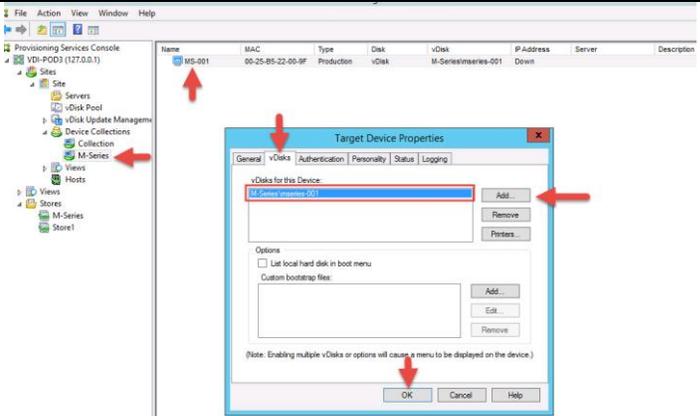
Instructions	Visual
<p>3. The Connect to Farm page appears. Enter the name or IP address of a Provisioning Server within the farm to connect to and the port to use to make that connection.</p> <p>4. Use the Windows credentials (default) or enter different credentials.</p> <p>5. Click Next.</p>	
<p>1. Select Create new vDisk.</p> <p>2. Click Next.</p>	

Instructions	Visual
	
<p>1. Define volume sizes on the Configure Image Volumes page.</p> <p>2. Click Next.</p>	

Instructions	Visual
<p>3. The Add Target Device page appears.</p> <p>4. Select the Target Device Name, the MAC address associated with one of the NICs that was selected when the target device software was installed on the master target device, and the Collection to which you are adding the device.</p> <p>5. Click Next.</p>	
<p>A Summary of Farm Changes appears.</p> <p>1. Select Optimize for Provisioning Services</p>	

<p>Instructions</p>	<p>Visual</p>																																								
<p>2. The PVS Optimization Tool appears. Select the appropriate optimizations and click OK.</p> <p>3. Review the configuration and click Finish</p>	 <p>Provisioning Services Device Optimization Tool</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Disable Offline Files <input checked="" type="checkbox"/> Disable Defrag BootOptimizeFunction <input checked="" type="checkbox"/> Disable Last Access Timestamp <input checked="" type="checkbox"/> Reduce DedicatedDumpFile DumpFileSize to 2MB <input checked="" type="checkbox"/> Disable Move to Recycle Bin <input checked="" type="checkbox"/> Reduce IE Temp File <input checked="" type="checkbox"/> Disable Machine Account Password Changes <input checked="" type="checkbox"/> Disable Windows Defender <input checked="" type="checkbox"/> Disable ScheduledDefrag <input checked="" type="checkbox"/> Disable ProgramDataUpdater <input checked="" type="checkbox"/> Disable Windows Autoupdate <input checked="" type="checkbox"/> Disable Background Layout Service <input checked="" type="checkbox"/> Disable Hibernate <input checked="" type="checkbox"/> Disable Indexing Service <input checked="" type="checkbox"/> Reduce Event Log Size to 64k <input checked="" type="checkbox"/> Disable Clear Page File at Shutdown <input checked="" type="checkbox"/> Disable Windows SuperFetch <input checked="" type="checkbox"/> Disable Windows Search <input checked="" type="checkbox"/> Disable System Restore <input checked="" type="checkbox"/> Run NGen ExecuteQueuedItems (new window) <p>OK Exit</p>																																								
<p>The vDisk creation process begins. A dialog appears when the creation process is complete.</p> <p>1. At the reboot now prompt select No and manually shutdown the machine.</p>	 <p>Provisioning Services Imaging Wizard</p> <p>The Wizard has successfully created the vDisk. To continue the imaging process, you must reboot, configuring the BIOS/VM settings for PXE/network boot.</p> <p>Reboot now?</p> <p>Yes No</p>																																								
<p>2. At this point, change the Boot Policy created earlier to the CD-PXE-HDD boot order. The master image will now stream only and a secondary local hard disk will be added and formatted for local write cache.</p>	 <p>Create Boot Policy</p> <p>Name: CD-PXE-HDD</p> <p>Description: see during provisioning server imaging process after disk copy</p> <p>Reboot on Boot Order Change: <input type="checkbox"/></p> <p>Enforce vNIC/vHBA/iSCSI Name: <input checked="" type="checkbox"/></p> <p>Boot Mode: Legacy UEFI</p> <p>WARNINGS: The type (primary/secondary) does not indicate a boot order presence. The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/iSCSI Name is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported. If it is not selected, the vNIC/vHBA/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.</p> <p>Local Devices</p> <ul style="list-style-type: none"> Add Local Disk Add Local LUN Add Local iBoot Add SD Card Add Internal USB Add External USB Add CD/DVD Add Local CD/DVD Add Remote CD/DVD Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive <p>Boot Order</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Order</th> <th>vNIC/vHBA/iSCSI vNIC</th> <th>Type</th> <th>ID</th> <th>WWN</th> <th>Slot Number</th> <th>Lun Name</th> </tr> </thead> <tbody> <tr> <td>CD/DVD</td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>LAN</td> <td>2</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>LAN eth0</td> <td></td> <td>eth0</td> <td>Primary</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Local Disk</td> <td>3</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>OK Cancel</p>	Name	Order	vNIC/vHBA/iSCSI vNIC	Type	ID	WWN	Slot Number	Lun Name	CD/DVD	1							LAN	2							LAN eth0		eth0	Primary					Local Disk	3						
Name	Order	vNIC/vHBA/iSCSI vNIC	Type	ID	WWN	Slot Number	Lun Name																																		
CD/DVD	1																																								
LAN	2																																								
LAN eth0		eth0	Primary																																						
Local Disk	3																																								

<p>Instructions</p>	<p>Visual</p>												
<p>After restarting, log into the VDI or RDS master target. The PVS Imaging conversion process begins, converting C: to the PVS vDisk.</p> <p>1. If prompted to Restart select Restart Later</p>													
<p>A message is displayed when the conversion is complete</p> <p>2. Click Finish</p> <p>The machine can be turned off.</p>													
<p>3. From the UCS Manager, change the boot policy to the PXE-Boot profile created earlier.</p>	 <table border="1" data-bbox="987 1318 1333 1381"> <thead> <tr> <th>Name</th> <th>Order</th> <th>vNIC/vHB</th> </tr> </thead> <tbody> <tr> <td>CD/DVD</td> <td>1</td> <td></td> </tr> <tr> <td>LAN</td> <td>2</td> <td></td> </tr> <tr> <td>LAN eth0</td> <td></td> <td>eth0</td> </tr> </tbody> </table>	Name	Order	vNIC/vHB	CD/DVD	1		LAN	2		LAN eth0		eth0
Name	Order	vNIC/vHB											
CD/DVD	1												
LAN	2												
LAN eth0		eth0											

Instructions	Visual
<p>4. Return to the PVS console, in the properties of the VM, change the Boot from: field to vDisk on the General tab.</p>	
<p>5. Add the newly created vDisk on the vDisks tab and click OK.</p>	
<p>6. Boot the machine from the vDisk and verify there are no errors. Leave the vDisk in 'Private Mode' so changes will be saved. Next step is to install the XenDesktop 7.6 VDA.</p>	

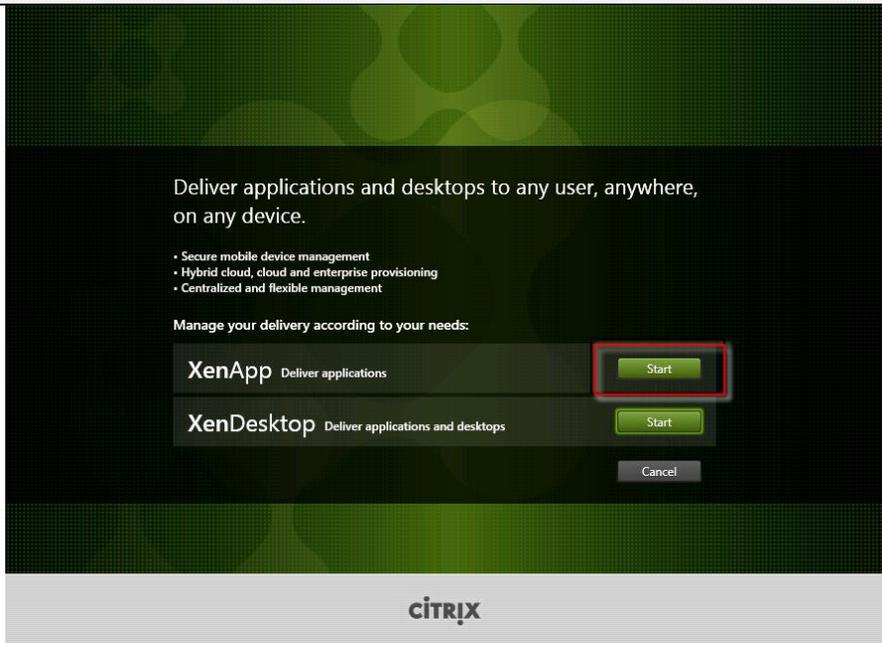
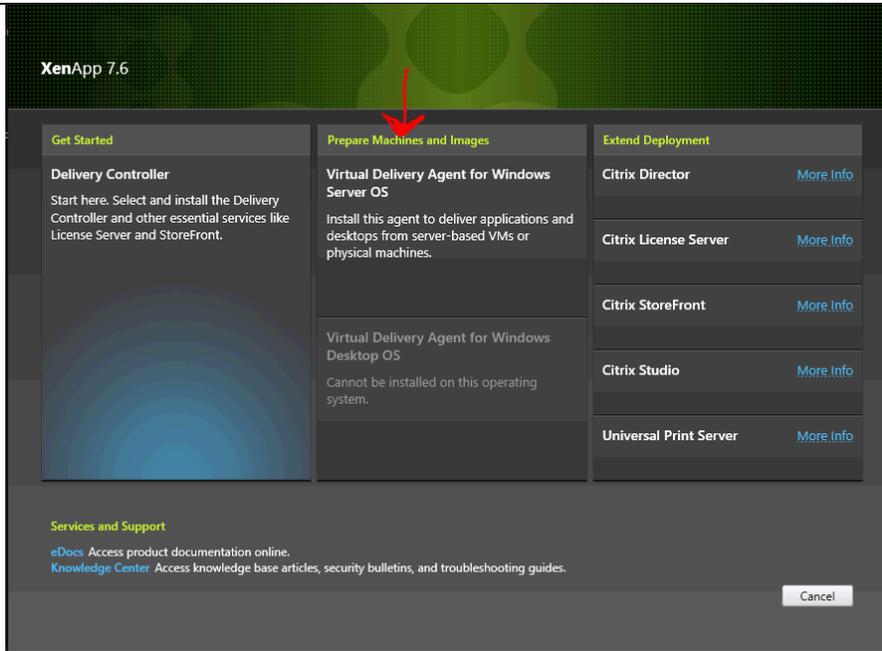
Install the XenApp Virtual Desktop Agent to the Master vDisk Image

The Citrix XenApp Virtual Delivery Agent (VDA) is installed on the master vDisk image of the Windows 2012 R2 server. The VDA enables connections to server hosted desktops and apps. The following procedure was used to install VDAs for the HSD environment.

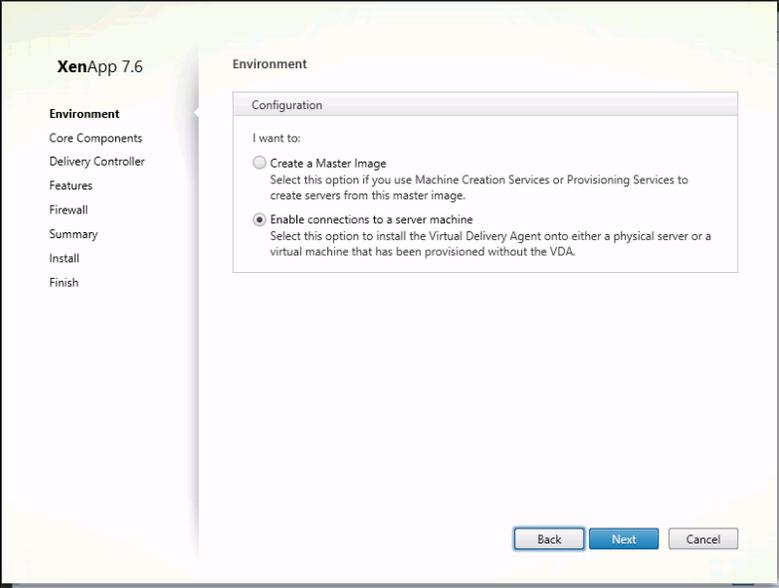
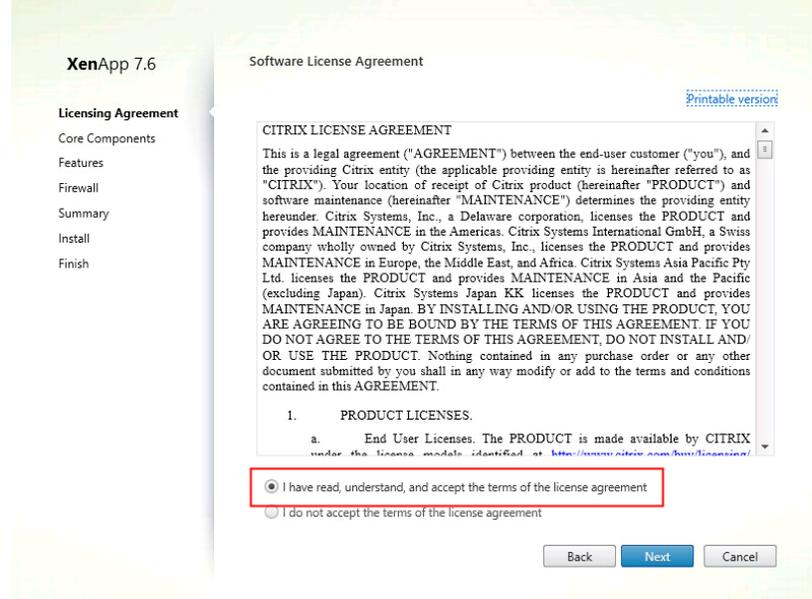
By default, when you install the Virtual Delivery Agent, Citrix User Profile Management is installed silently on master images.



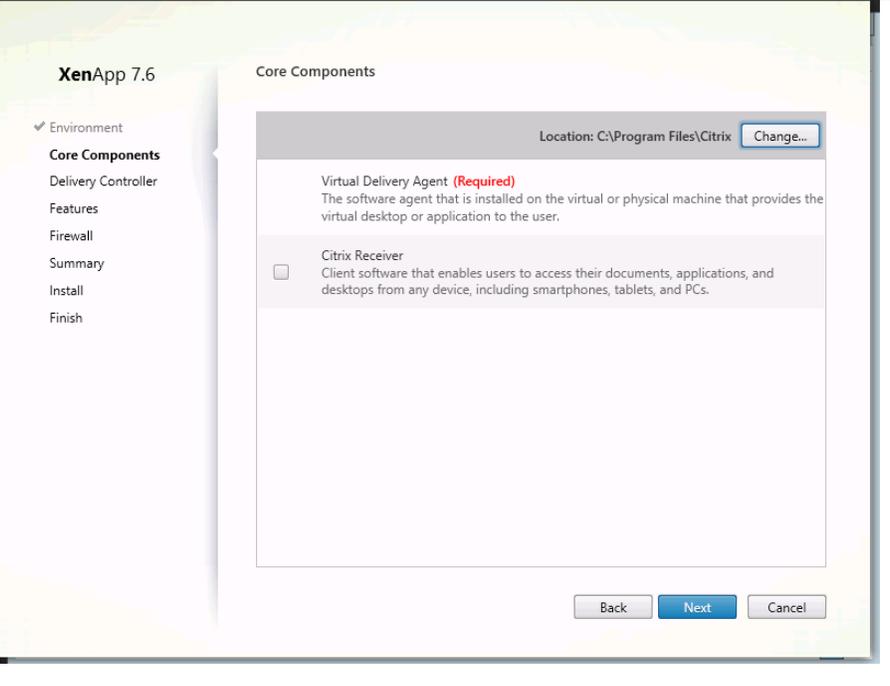
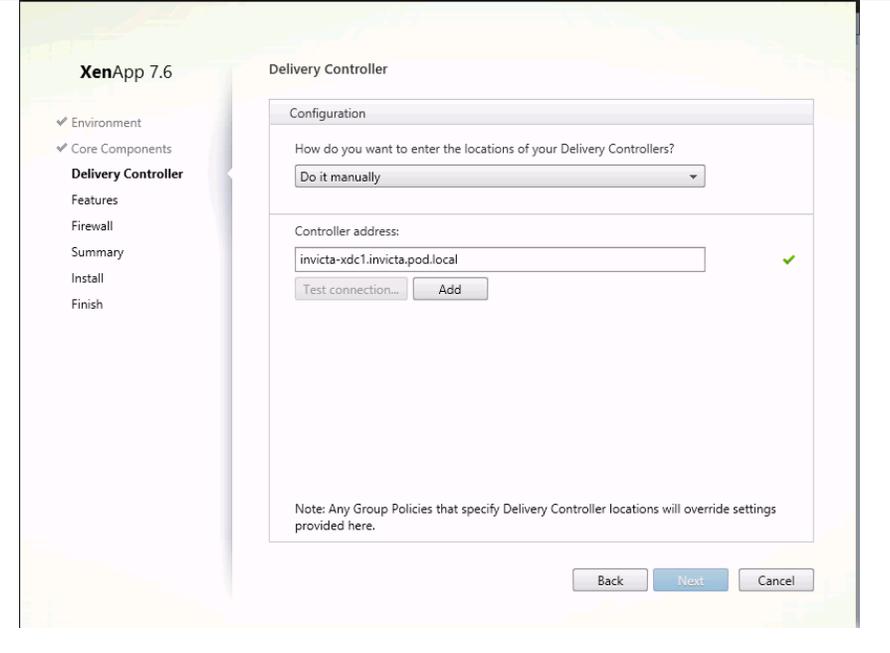
Using profile management as a profile solution is optional but was used for this CVD, and is described in a later section.

Instructions	Visual
<p>1. Launch the XenApp installer from the XenApp 7.6 ISO.</p> <p>2. Click Start on the Welcome Screen.</p>	 <p>The image shows the XenApp Welcome Screen. At the top, it says "Deliver applications and desktops to any user, anywhere, on any device." Below this are three bullet points: "Secure mobile device management", "Hybrid cloud, cloud and enterprise provisioning", and "Centralized and flexible management". Underneath, it says "Manage your delivery according to your needs:". There are two main sections: "XenApp Deliver applications" and "XenDesktop Deliver applications and desktops". Each section has a green "Start" button. The "Start" button for XenApp is highlighted with a red rectangle. At the bottom, there is a "Cancel" button and the Citrix logo.</p>
<p>3. To install the VDA for the Hosted VDI Desktops, select Virtual Delivery Agent for Windows Desktop OS. (After the VDA is installed for Hosted VDI Desktops, repeat the procedure to install the VDA for Hosted Shared Desktops. In this case, select Virtual Delivery Agent for Windows Server OS and follow the same basic steps.)</p>	 <p>The image shows the XenApp 7.6 installation wizard. The title bar says "XenApp 7.6". There are three main sections: "Get Started", "Prepare Machines and Images", and "Extend Deployment". Under "Get Started", there is a "Delivery Controller" section with a description. Under "Prepare Machines and Images", there are two options: "Virtual Delivery Agent for Windows Server OS" and "Virtual Delivery Agent for Windows Desktop OS". A red arrow points to the "Virtual Delivery Agent for Windows Server OS" option. The "Extend Deployment" section lists several components: Citrix Director, Citrix License Server, Citrix StoreFront, Citrix Studio, and Universal Print Server, each with a "More Info" link. At the bottom, there is a "Services and Support" section with links to "eDocs" and "Knowledge Center". A "Cancel" button is at the bottom right.</p>

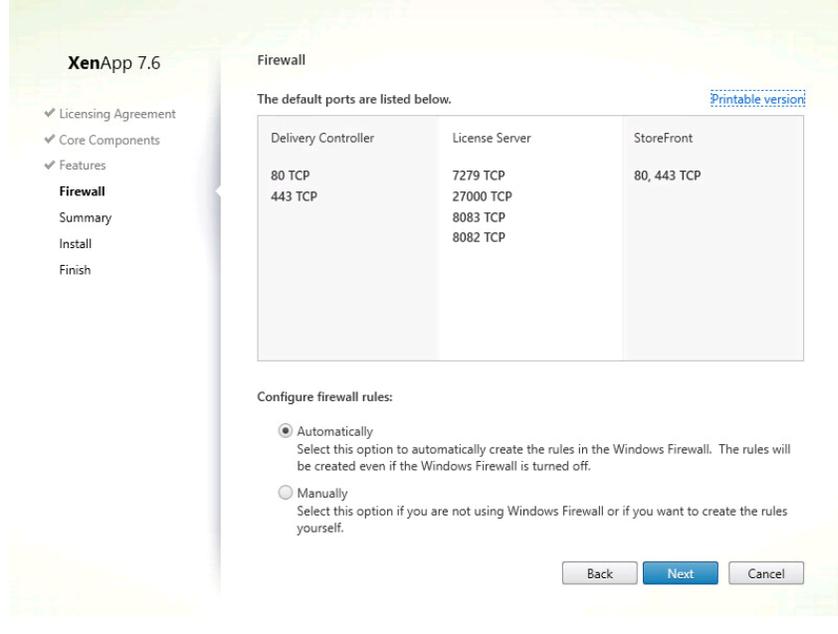
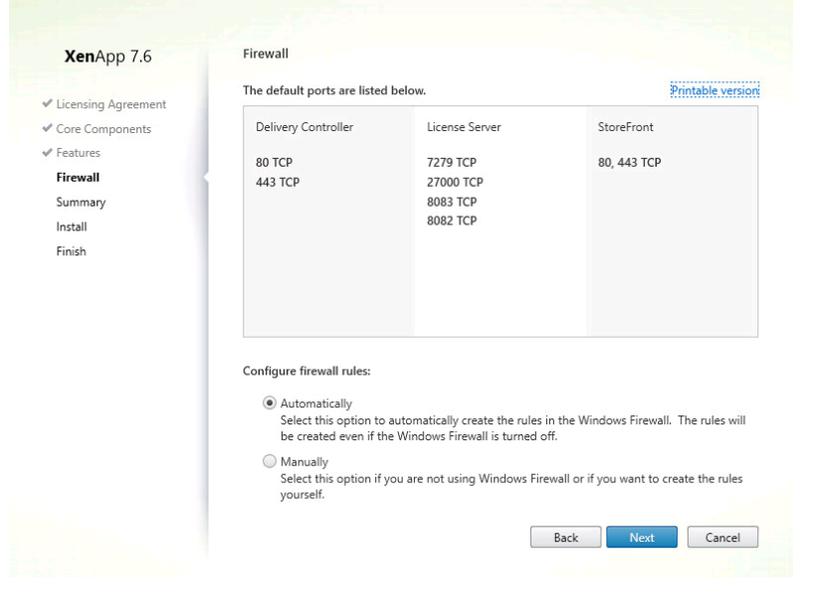
Instructions	Visual
--------------	--------

Instructions	Visual
<p>1. Select “Enable connections to a server machine”.</p> <p>2. Click Next</p>	
<p>3. For the Licensing Agreement, acknowledge.</p> <p>4. Click Next</p>	

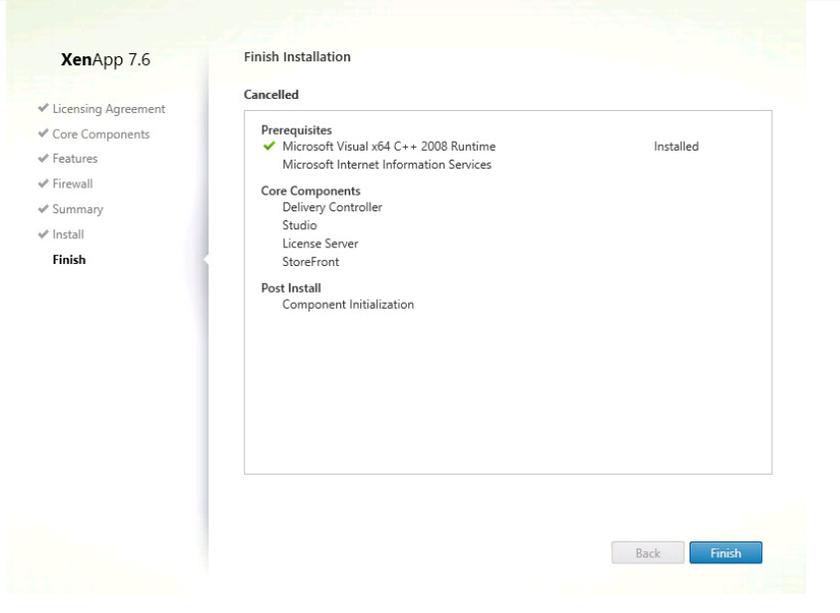
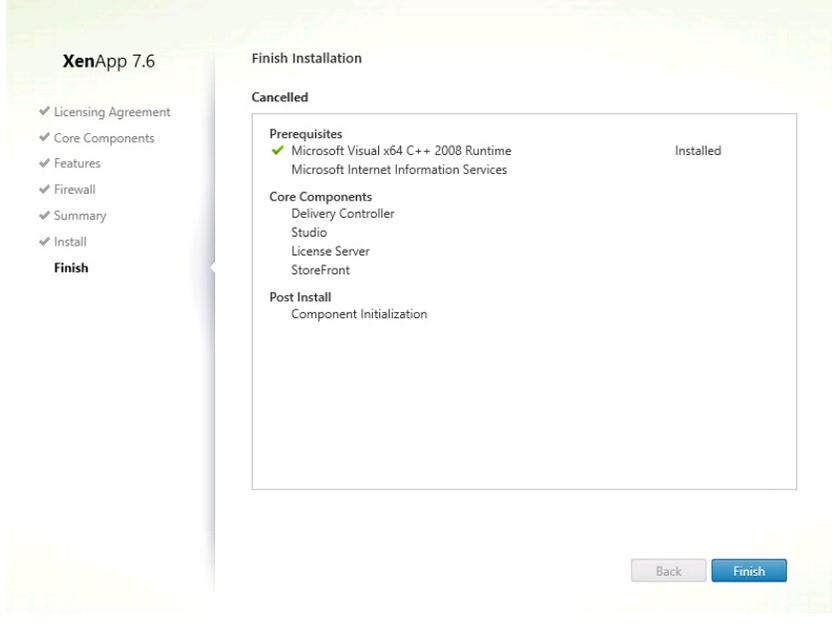
Instructions	Visual
--------------	--------

<p>Instructions</p>	<p>Visual</p>
<p>1. Deselect Citrix Receiver.</p> <p>2. Click Next</p>	 <p>The screenshot shows the 'Core Components' window in the XenApp 7.6 installation wizard. On the left sidebar, 'Core Components' is selected. The main area shows a list of components: 'Virtual Delivery Agent (Required)' which is checked, and 'Citrix Receiver' which is unchecked. The location for the components is 'C:\Program Files\Citrix'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.</p>
<p>3. Select “Do it manually” and specify the FQDN of the Delivery Controllers.</p> <p>4. Click Next</p>	 <p>The screenshot shows the 'Delivery Controller' configuration window. The 'Configuration' section has a dropdown menu set to 'Do it manually'. Below it, the 'Controller address' field contains 'invicta-xdc1.invicta.pod.local' with a green checkmark to its right. There are 'Test connection...' and 'Add' buttons. A note at the bottom states: 'Note: Any Group Policies that specify Delivery Controller locations will override settings provided here.' At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.</p>

<p>Instructions</p>	<p>Visual</p>
---------------------	---------------

Instructions	Visual						
<p>1. Accept the default features.</p> <p>2. Click Next.</p>	 <p>XenApp 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components ✓ Features Firewall Summary Install Finish <p>Firewall</p> <p>The default ports are listed below. Printable version</p> <table border="1"> <thead> <tr> <th>Delivery Controller</th> <th>License Server</th> <th>StoreFront</th> </tr> </thead> <tbody> <tr> <td>80 TCP 443 TCP</td> <td>7279 TCP 27000 TCP 8083 TCP 8082 TCP</td> <td>80, 443 TCP</td> </tr> </tbody> </table> <p>Configure firewall rules:</p> <p><input checked="" type="radio"/> Automatically Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.</p> <p><input type="radio"/> Manually Select this option if you are not using Windows Firewall or if you want to create the rules yourself.</p> <p>Back Next Cancel</p>	Delivery Controller	License Server	StoreFront	80 TCP 443 TCP	7279 TCP 27000 TCP 8083 TCP 8082 TCP	80, 443 TCP
Delivery Controller	License Server	StoreFront					
80 TCP 443 TCP	7279 TCP 27000 TCP 8083 TCP 8082 TCP	80, 443 TCP					
<p>3. Allow the firewall rules to be configured Automatically.</p> <p>4. Click Next</p>	 <p>XenApp 7.6</p> <ul style="list-style-type: none"> ✓ Licensing Agreement ✓ Core Components ✓ Features Firewall Summary Install Finish <p>Firewall</p> <p>The default ports are listed below. Printable version</p> <table border="1"> <thead> <tr> <th>Delivery Controller</th> <th>License Server</th> <th>StoreFront</th> </tr> </thead> <tbody> <tr> <td>80 TCP 443 TCP</td> <td>7279 TCP 27000 TCP 8083 TCP 8082 TCP</td> <td>80, 443 TCP</td> </tr> </tbody> </table> <p>Configure firewall rules:</p> <p><input checked="" type="radio"/> Automatically Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.</p> <p><input type="radio"/> Manually Select this option if you are not using Windows Firewall or if you want to create the rules yourself.</p> <p>Back Next Cancel</p>	Delivery Controller	License Server	StoreFront	80 TCP 443 TCP	7279 TCP 27000 TCP 8083 TCP 8082 TCP	80, 443 TCP
Delivery Controller	License Server	StoreFront					
80 TCP 443 TCP	7279 TCP 27000 TCP 8083 TCP 8082 TCP	80, 443 TCP					

Instructions	Visual
--------------	--------

Instructions	Visual
<p>1. Verify the Summary and click Install.</p>	 <p>The screenshot shows the XenApp 7.6 installation wizard. On the left, a navigation pane lists steps: Licensing Agreement, Core Components, Features, Firewall, Summary, Install, and Finish. The 'Finish' step is selected and highlighted in blue. The main area shows the 'Finish Installation' screen with a 'Cancelled' status. A list of prerequisites is shown as 'Installed', including Microsoft Visual x64 C++ 2008 Runtime and Microsoft Internet Information Services. Below this, 'Core Components' (Delivery Controller, Studio, License Server, StoreFront) and 'Post Install' (Component Initialization) are listed. At the bottom right, there are 'Back' and 'Finish' buttons.</p>
<p>2. Check “Restart Machine”.</p> <p>3. Click Finish and the machine will reboot automatically.</p>	 <p>This screenshot is identical to the one above, showing the XenApp 7.6 installation wizard at the 'Finish' step. The 'Finish' button is highlighted in blue, indicating it is the next step to be taken.</p>

Configure Local Hard Disks for PVS Write Cache with Script

When using Citrix Provisioning Services to stream to Bare Metal machines, there has always been a challenge with the configuration of the secondary hard disk for the purpose of local write cache. In this solution we are provisioning Windows operating system to bare metal cartridge servers and using local hard disks to redirect write cache to as well.

In a traditional deployment, the steps to configure a local hard disk cache on a bare metal deployment would include putting the PVD vDisk into private mode, mounting and formatting the local server disk and then placing the vDisk into standard mode and connecting multiple machines to that single image.

While manually formatting and mounting a local hard disk for a handful of machines might be acceptable on a small scale, for a large enterprise, automating this process is required.

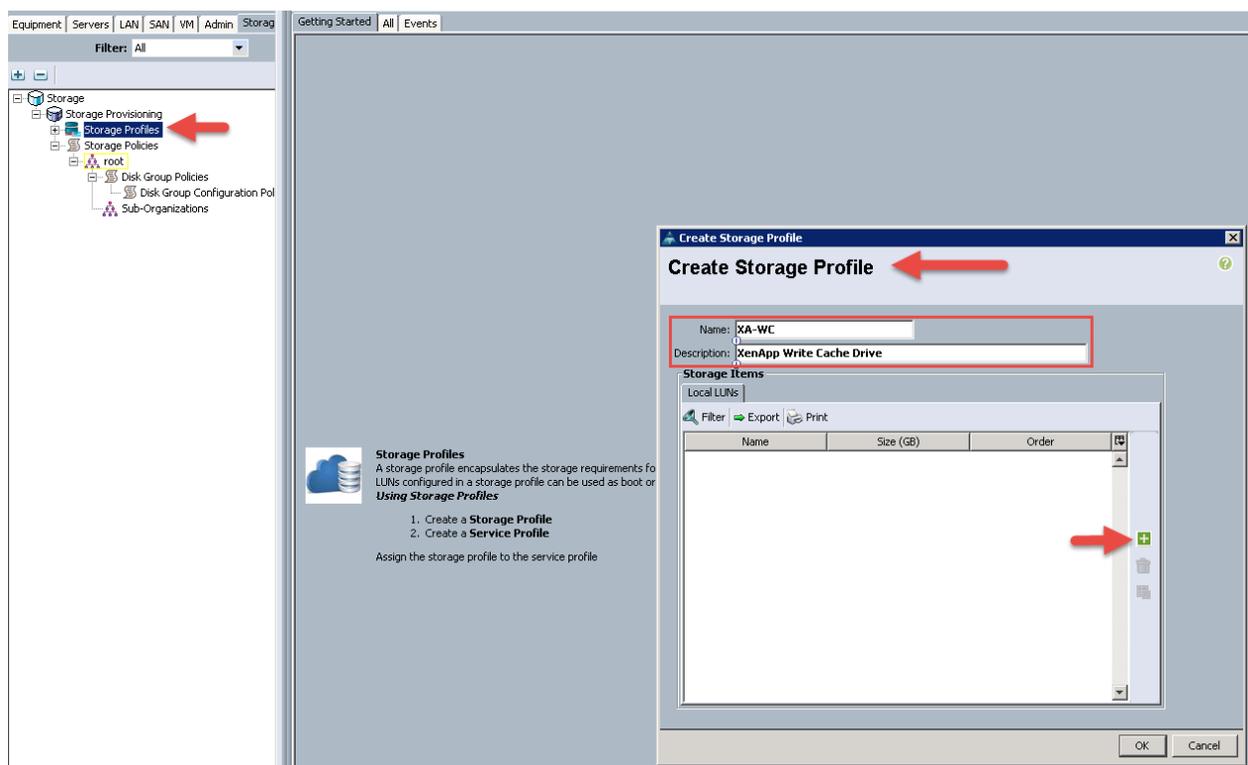
There have long been scripts to automate the initial mounting and formatting of the local hard disk for bare metal deployments. We did however find a unique challenge during this process that is related to the UCS M-Series midplane shared architecture.

Typically when you create the master image and attach the first local hard disk and format it, a registry entry is created at HKLM\System\CurrentControlSet\Control\DeviceClass\{Device ID}\{SCSI Target ID #}. In traditional deployments, a single entry in the master image registry would be sufficient for hundreds of unique machines connecting to that single registry entry because the SCSI Target ID number is always the same.

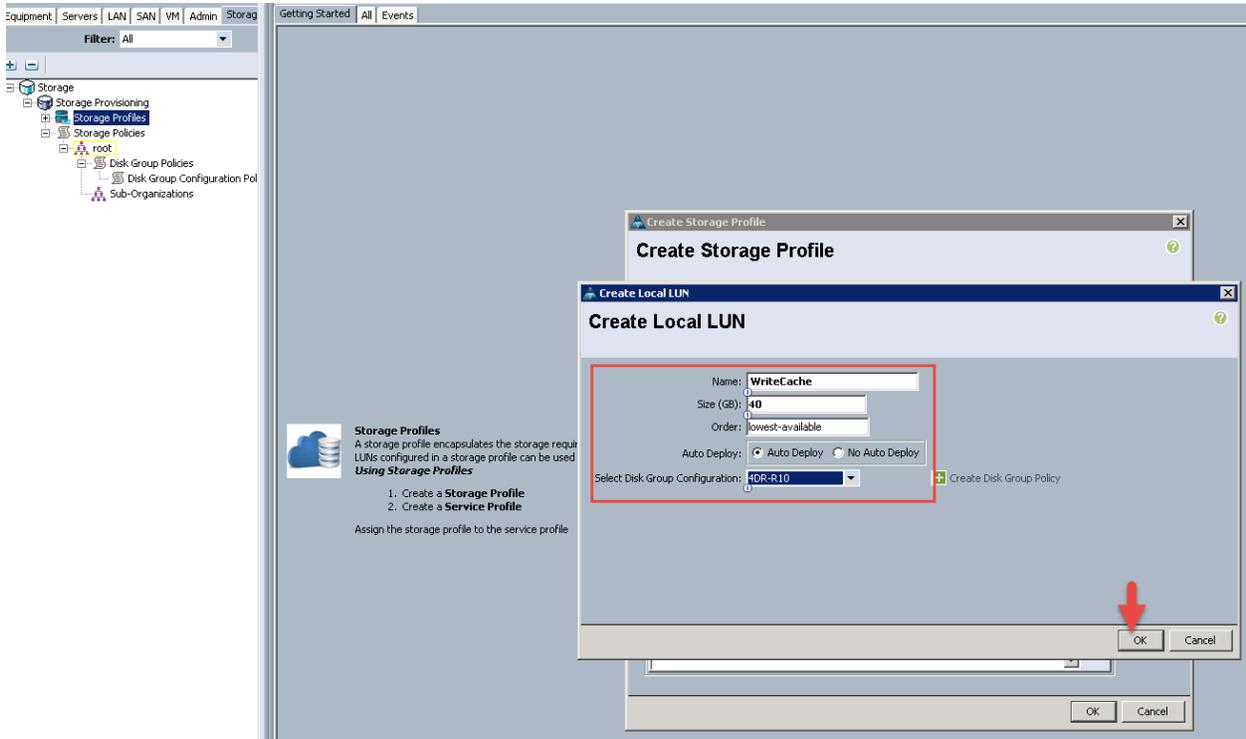
However, since the Cisco UCS M-Series Cartridge servers all share a SCSI controller, the SCSI target ID for the write cache drive on each server is different. For that reason, a unique registry entry is needed for every machine to be able to successfully mount and use its local write cache hard disk. What we identified is for **each machine's registry entry to increment by 1's and then alphabetically.**

To implement multiple chassis of 16 servers each in an automated fashion, complete the following steps:

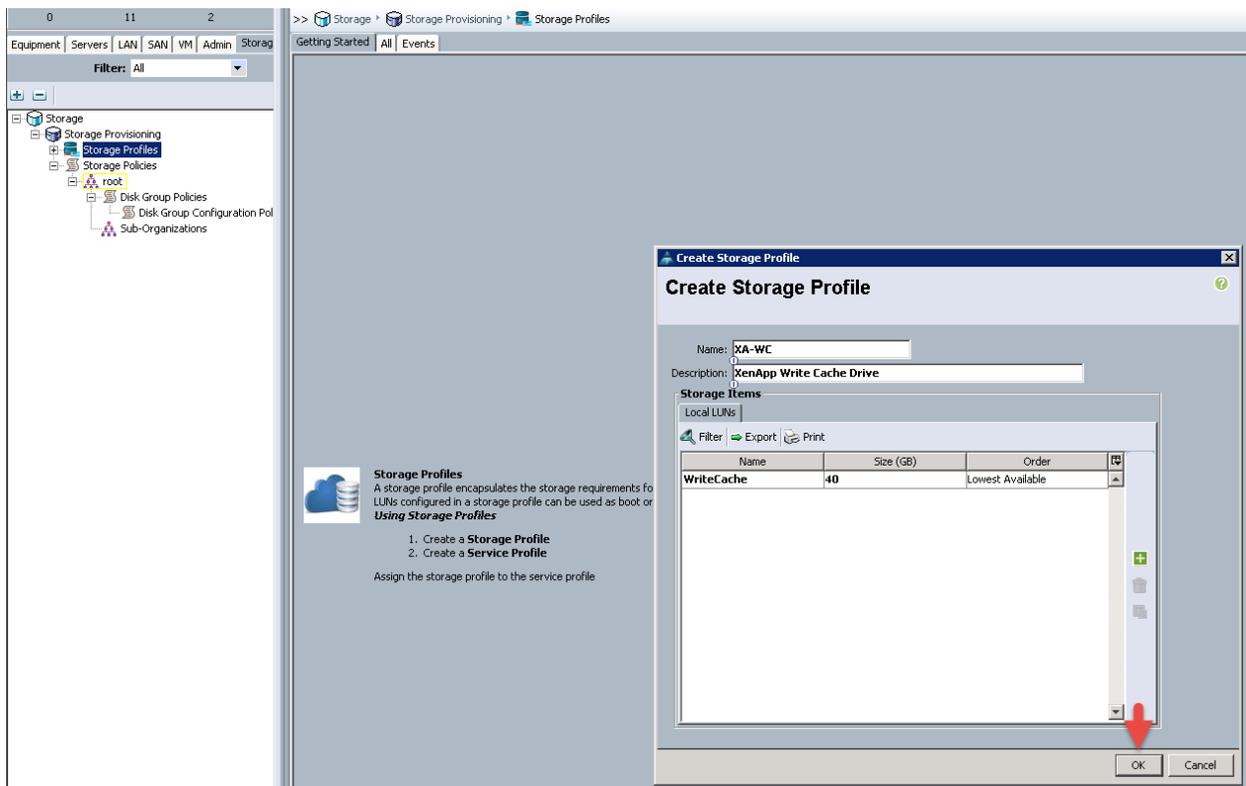
1. Create a new Storage Profile in UCSM on the Storage tab, Storage Profiles node called XA-WC as follows.



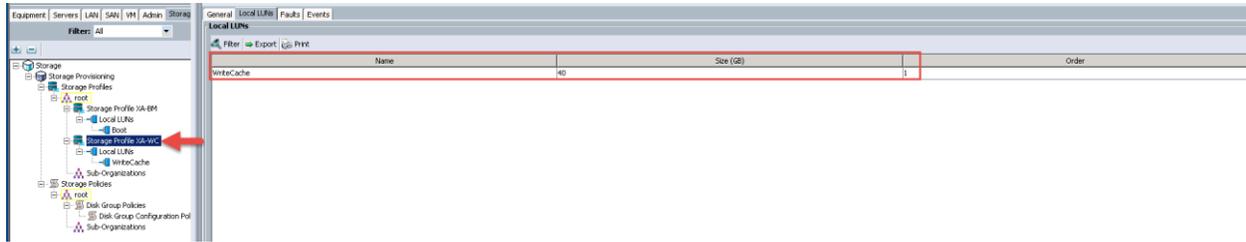
2. When you click the "+" control, name the LUN WriteCache, use 40GB for the size (2x RAM + over-head), choose the 4DR-R10 Disk Group created earlier, then click OK.



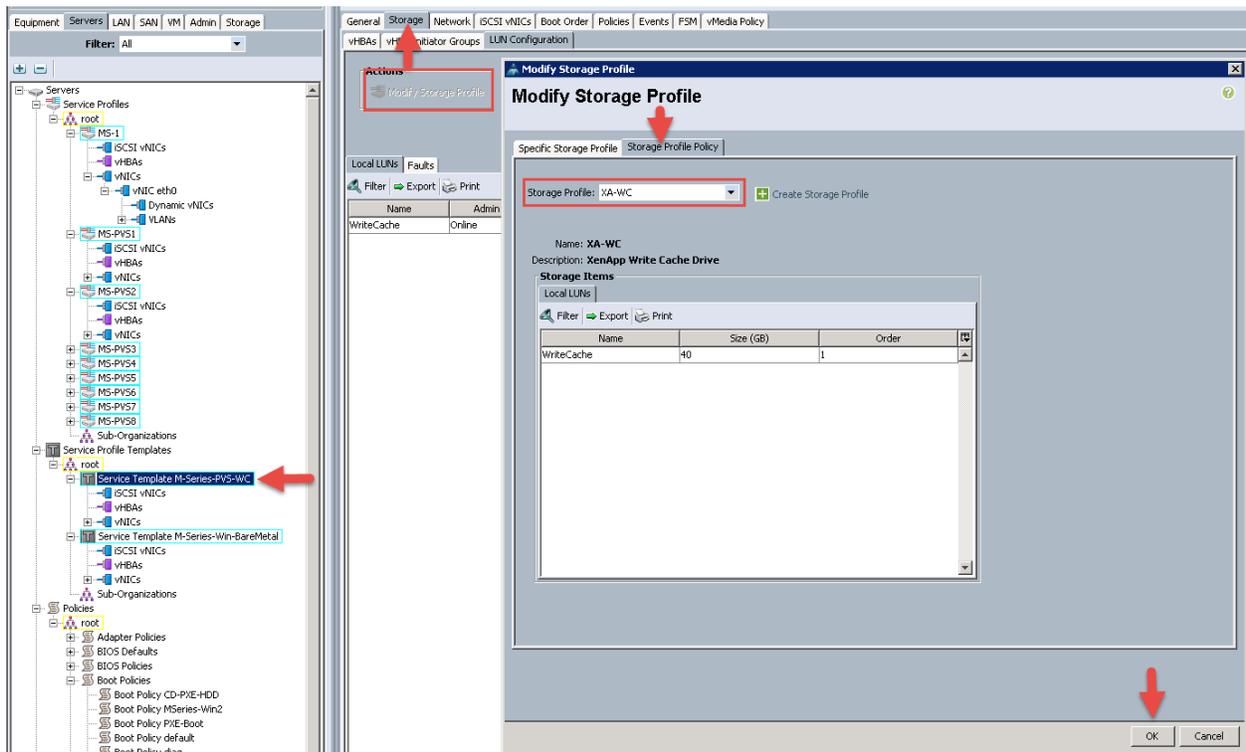
3. Click OK to save the Storage Profile.



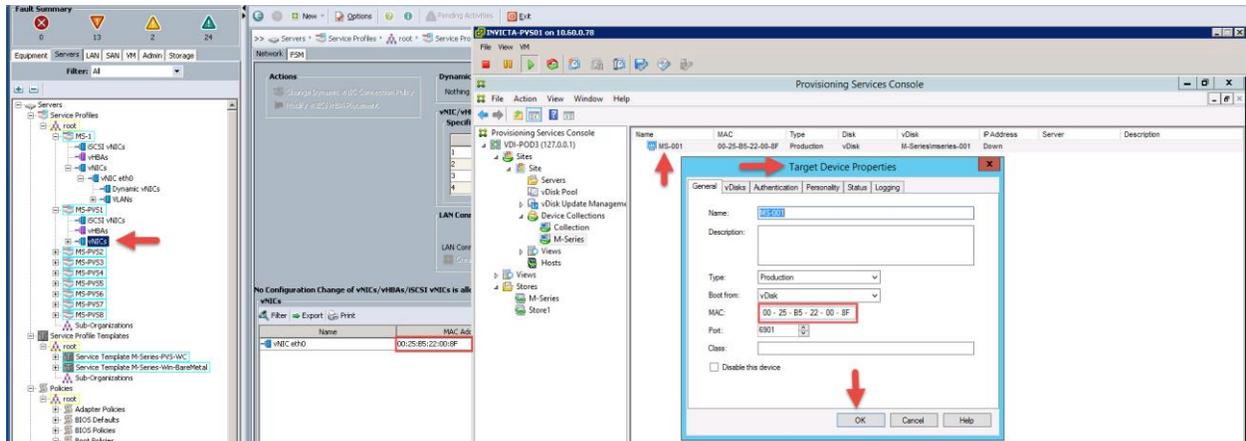
The policy will look like the screen shot below:



4. Clone your SP Template M-Series-Win-BareMetal and name the new template M-Series-PVS-WC in the same Org (Root in our case).
5. Modify the Storage Policy on the Storage tab and select the Storage Profile XA-WC on the Storage Profile Policy tab.

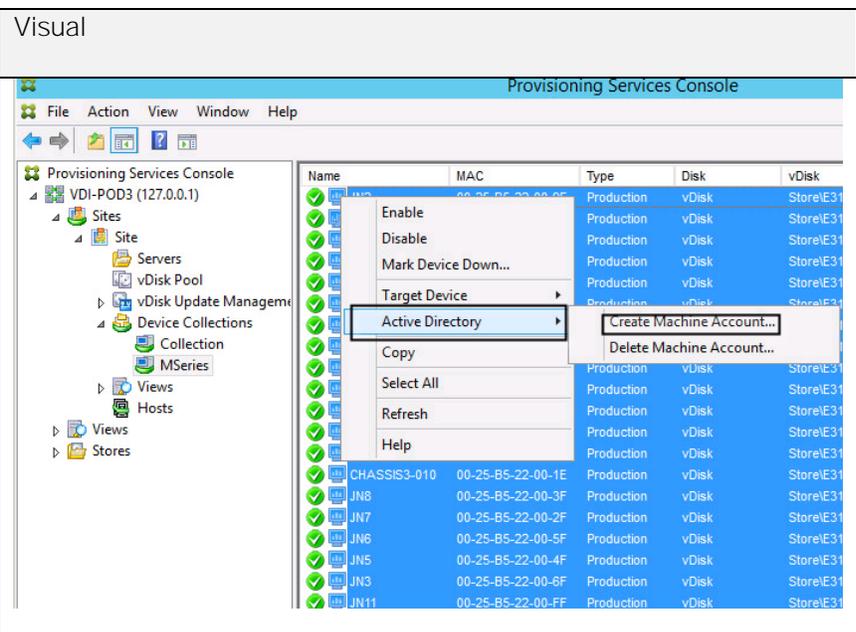


6. Create the number of Service Profiles you need for you deployment, two per M-Series cartridge. We recommend including an indication in the naming that PVS is involved. (Used MS-PVS as the prefix generating MS-PVS1, MS-PVS2, etc.)
7. Disassociate the MS-1 bare metal service profile from Cartridge 1, Server 1 and associate the same server with the MS-PVS1 Service Profile you just created. Associate the remaining Servers to their profiles to create the storage for each.
8. Update the Mac address in the PVS console for the mseries-001 machine Properties to the new MAC address in the MS-PVS1 Service Profile.



Instructions

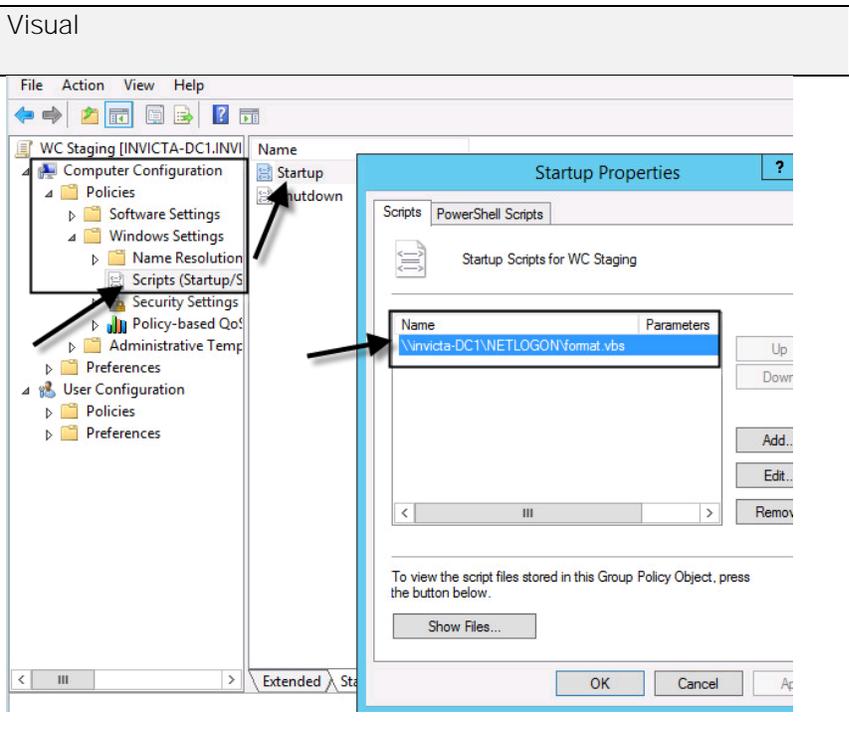
1. When create the collection machines in PVS, right-click the machines, click Active Directory and Create Machine Account. Browse to the OU that the RDS machine will reside in. (in this study it was the Login VSI Computers OU)



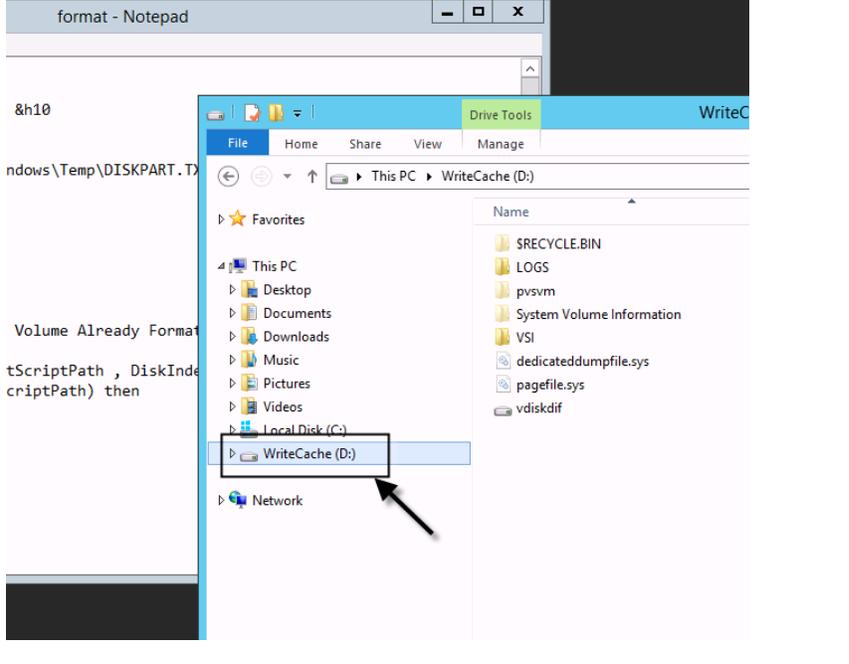
Instructions

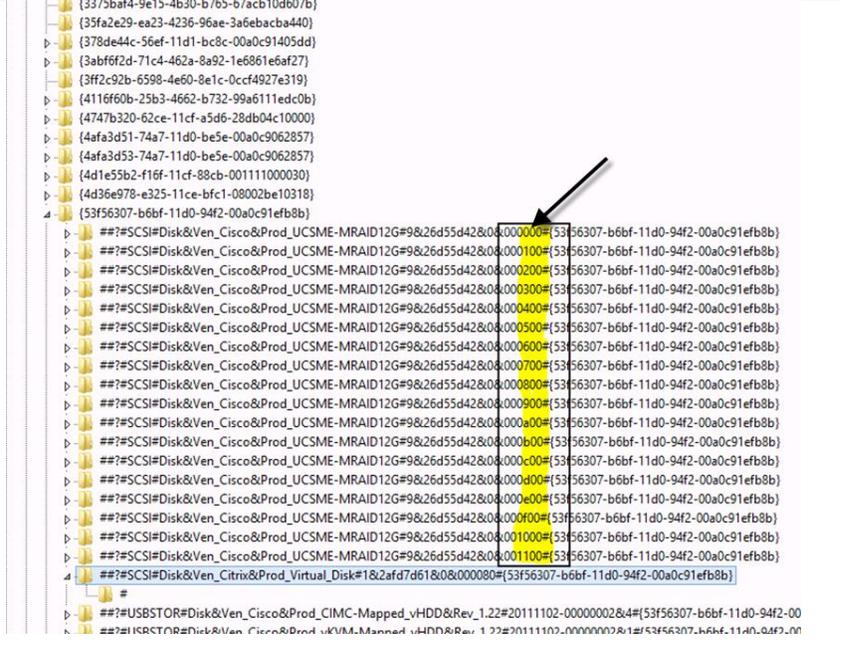
2. In the OU that the XenApp machines reside in, create a GPO and add a Startup script under Computer Configuration.

*The format.vbs is in the Appendix of this document.



3. Now that the script is in place and the provisioned machines have local disks attached to them via the Service profile creation, upon boot the disks will be mounted, formatted with NTFS and labeled as 'WriteCache'.

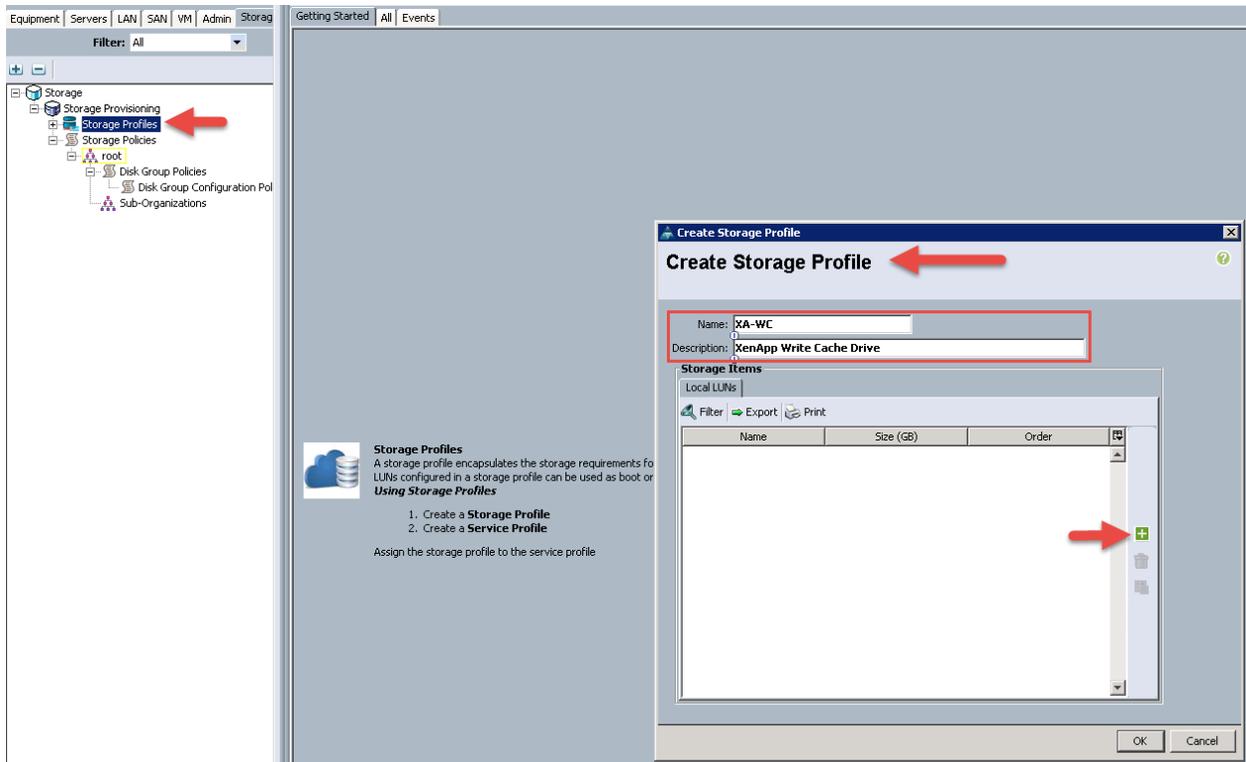


Instructions	Visual
<p>Next, manually create and import a registry entry for all 16 servers in the chassis. These 16 registry entries will work for scaling out to multiple chassis. We tested connecting multiple chassis connecting to the one master image.</p>	 <p>The screenshot shows a registry tree with the following entries (some truncated for brevity):</p> <ul style="list-style-type: none"> (3375baf4-9e15-4b30-b765-67acb10d607b) (35fa2e29- ea23-4236-96ae-3a6ebacba440) (378de44c-56ef-11d1-bc8c-00a0c91405dd) (3abff62d-71c4-462a-9a92-1e6861e6af27) (3ff2c92b-6598-4e60-8e1c-0ccf4927e319) (4116f60b-25b3-4662-b732-99a6111edc0b) (4747b320-62ce-11cf-a5d6-28db04c10000) (4afa3d51-74a7-11d0-be5e-00a0c9062857) (4afa3d53-74a7-11d0-be5e-00a0c9062857) (4d1e55b2-f16f-11cf-88cb-001111000030) (4d36e978-e325-11ce-bfc1-08002be10318) (53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000100#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000200#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000300#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000400#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000500#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000600#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000700#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000800#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000900#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000a00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000b00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000c00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000d00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000e00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0000f00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0010000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&0011000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#SCSI#Disk&Ven_Citrix&Prod_Virtual_Disk#1&2afd7d61&0&0000000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#USBSTOR#Disk&Ven_Cisco&Prod_CIMC-Mapped_vHDD&Rev_1.22#20111102-00000002&4#(53f56307-b6bf-11d0-94f2-00a0c91efb8b) ##?#ISCRSTOR#Disk&Ven_Cisco&Prod_vVMM-Mapped_vHDD&Rev_1.22#20111102-00000002&1#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)

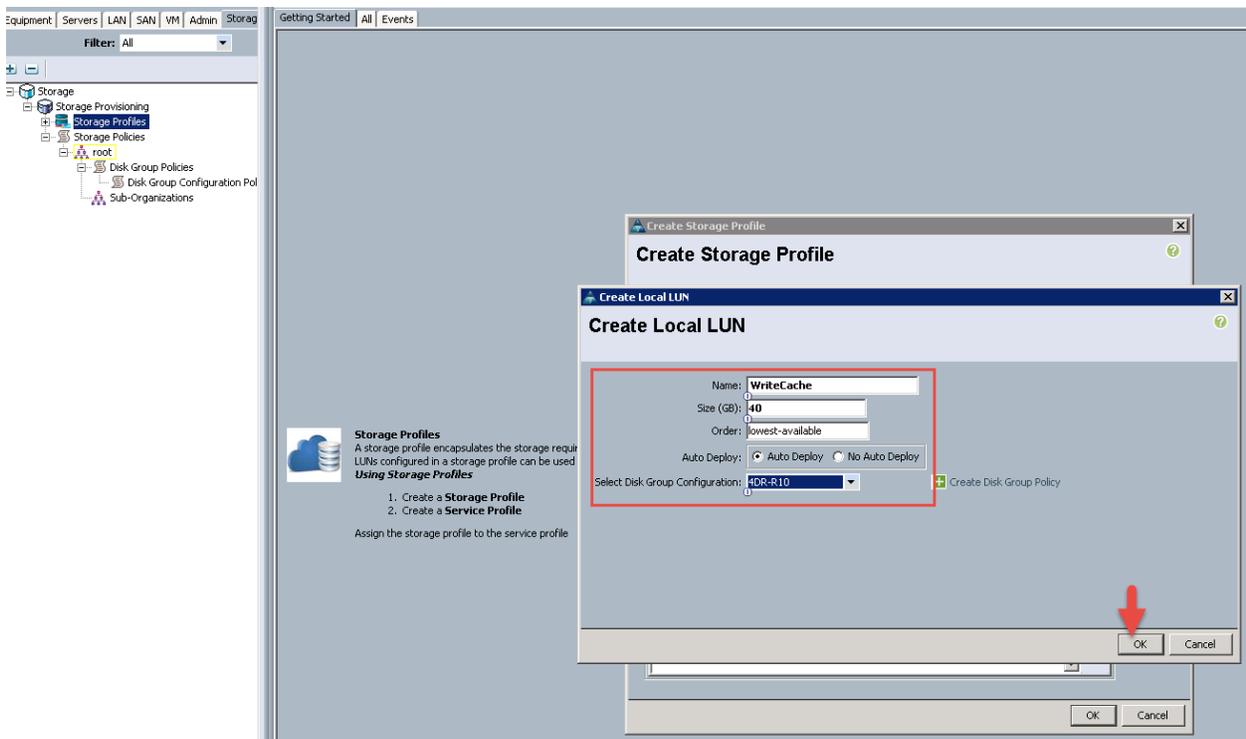
Configure Local Hard Disks for PVS Write Cache Manually

To manually configure the local hard disks for the PVS write cache, complete the following steps:

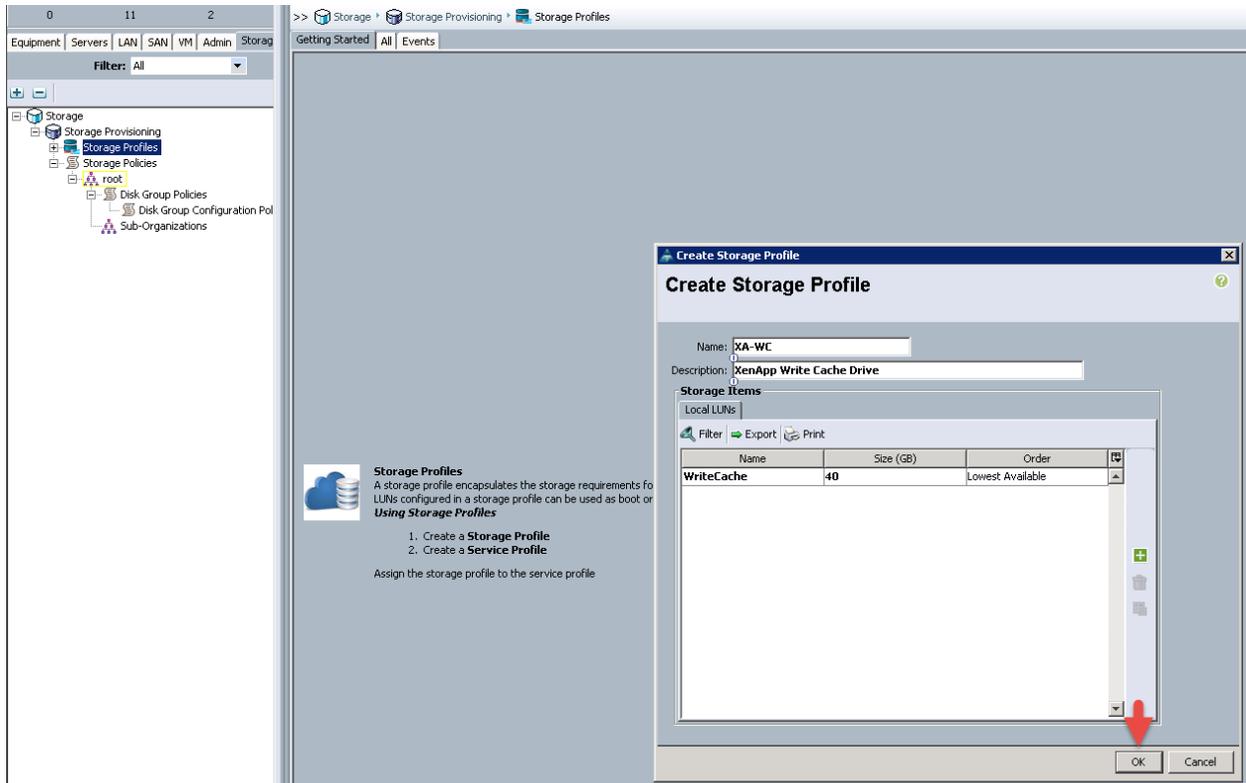
1. Create a new Storage Profile in UCSM on the Storage tab, Storage Profiles node called XA-WC as follows.



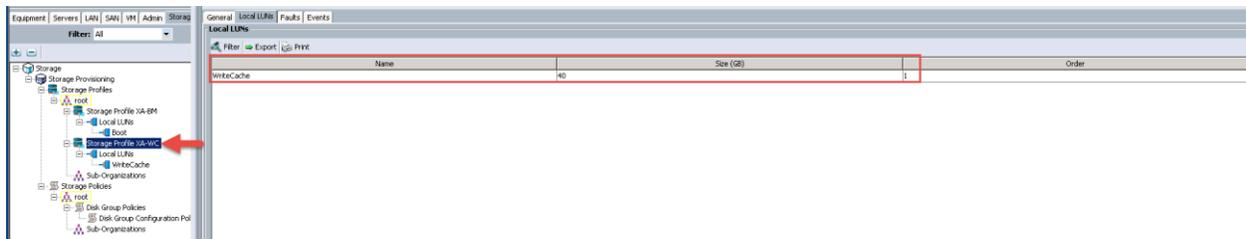
2. When you click the “+” control, name the LUN WriteCache, use 40GB for the size (2x RAM + over-head), choose the 4DR-R10 Disk Group created earlier, then click OK.



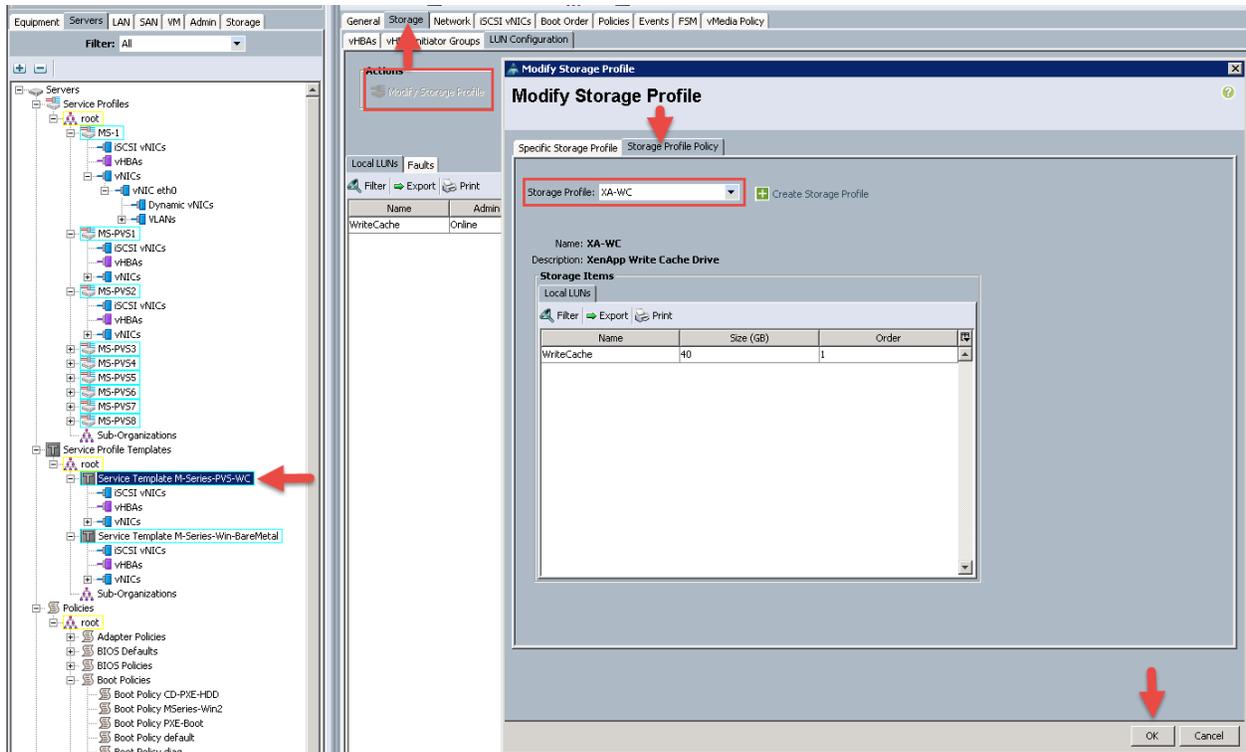
3. Click OK to save the Storage Profile.



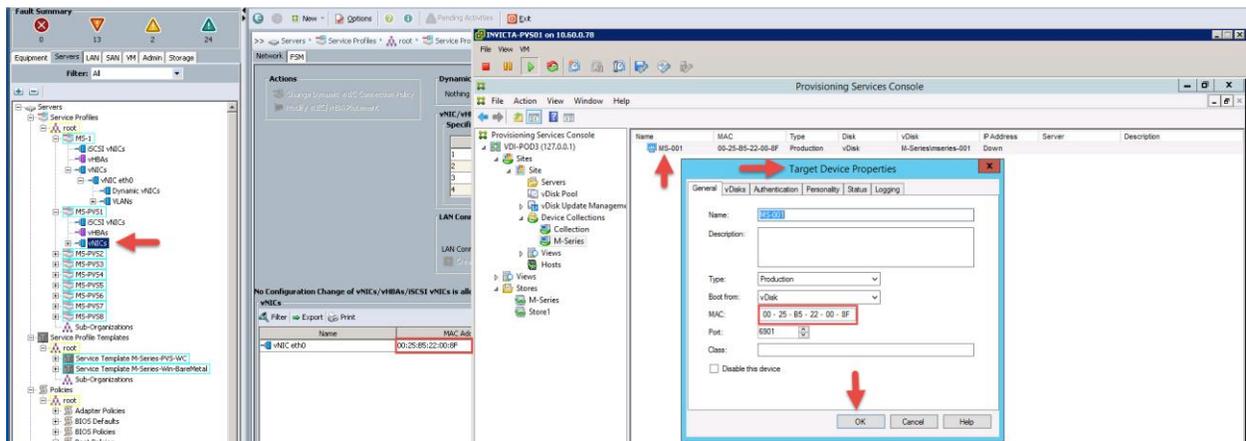
The policy will look like the screen shot below:



4. Clone your SP Template M-Series-Win-BareMetal and name the new template M-Series-PVS-WC in the same Org (Root in our case).
5. Modify the Storage Policy on the Storage tab and select the Storage Profile XA-WC on the Storage Profile Policy tab.

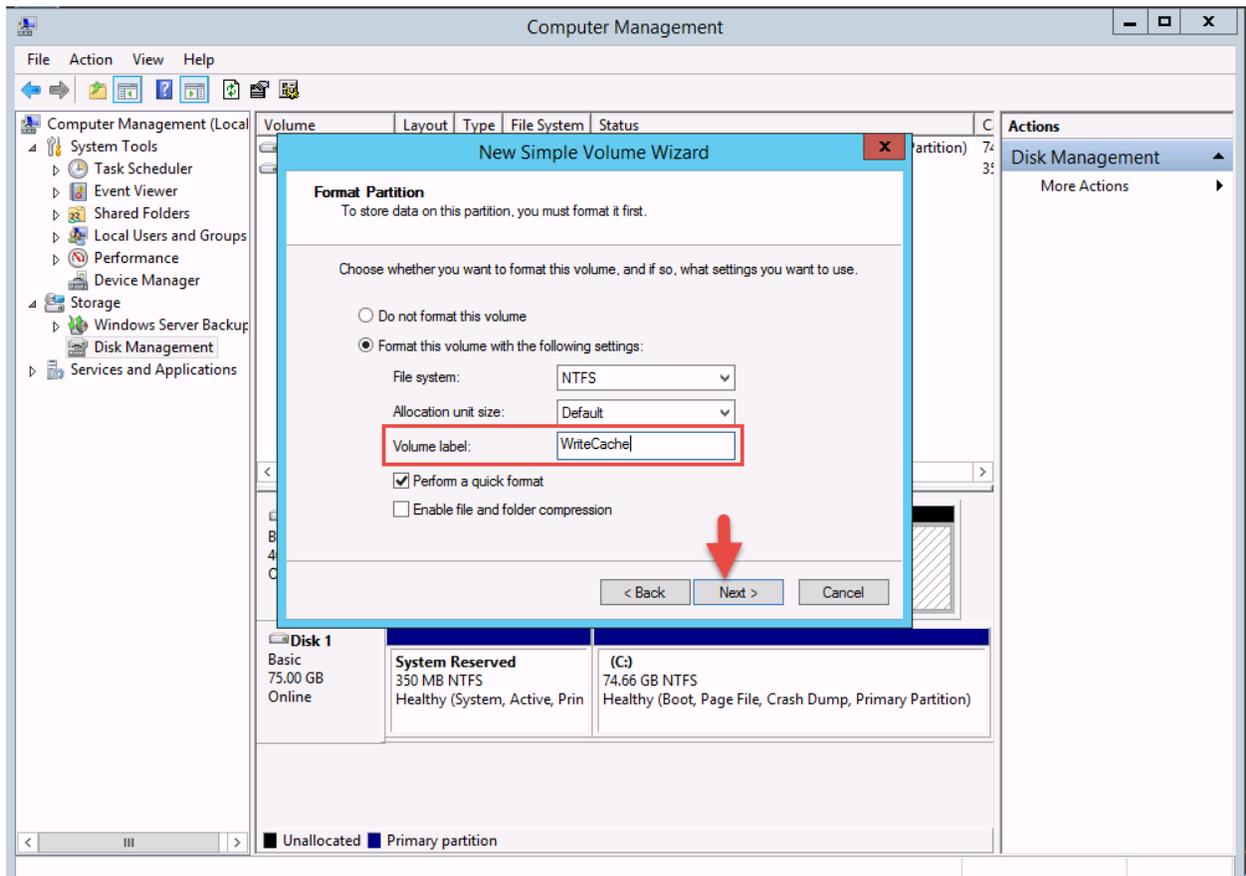


6. Create the number of Service Profiles you need for you deployment, two per M-Series cartridge. We recommend including an indication in the naming that PVS is involved. (Used MS-PVS as the prefix generating MS-PVS1, MS-PVS2, etc.)
7. Disassociate the MS-1 bare metal service profile from Cartridge 1, Server 1 and associate the same server with the MS-PVS1 Service Profile you just created. Associate the remaining Servers to their profiles to create the storage for each.
8. Update the Mac address in the PVS console for the mseries-001 machine Properties to the new MAC address in the MS-PVS1 Service Profile.

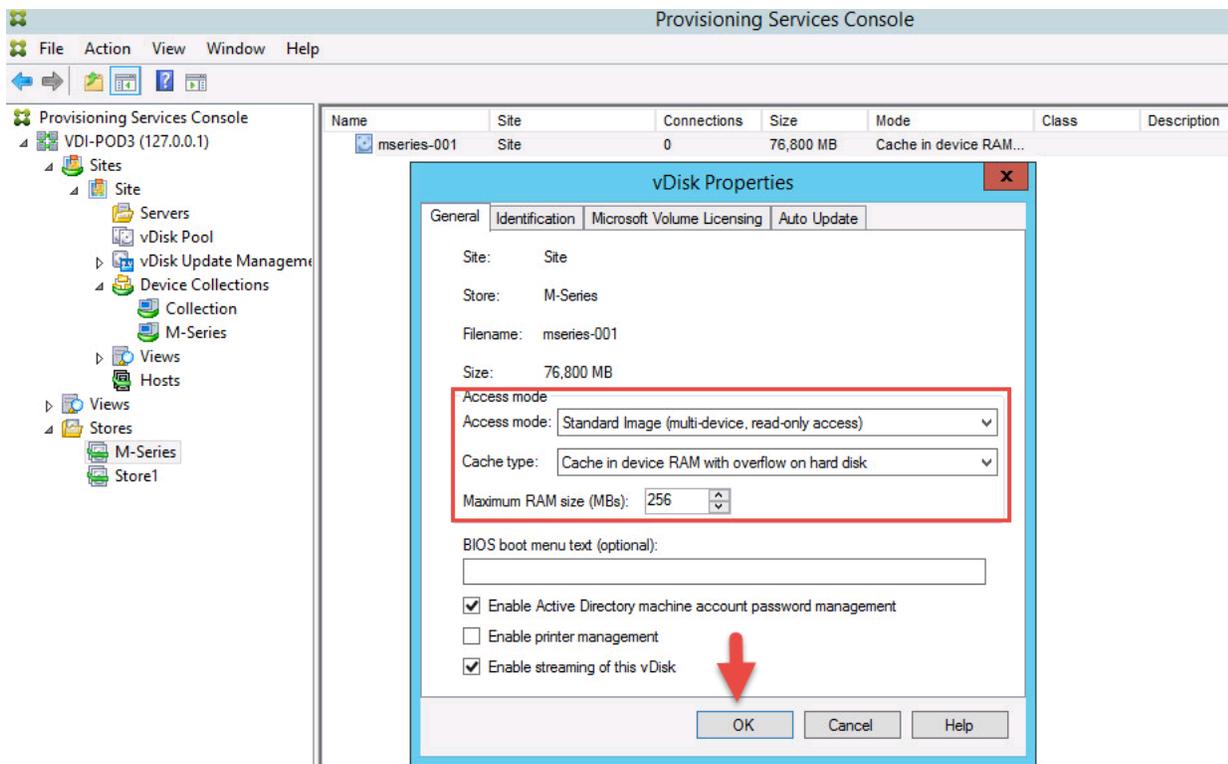


9. The new write cache drive is provisioned via the MS-PVS1 Service Profile, start the machine, open Server Manager, Local Machine, Tasks, Computer properties, Disk Manager.

10. Initialize the drive and set up a new Simple Volume using the wizard. Use all of the space, accept the drive letter assignment (D), format the volume with label: WriteCache and Perform a quick format.



11. Click Next and then restart the computer and validate that the D: drive is available with a label of WriteCache.
12. Shut down the machine and make a copy of the vDisk as a backup. Switch the vDisk properties to Standard Image, Cache in device RAM with Overflow on hard disk. Set the maximum device RAM to 256MB.

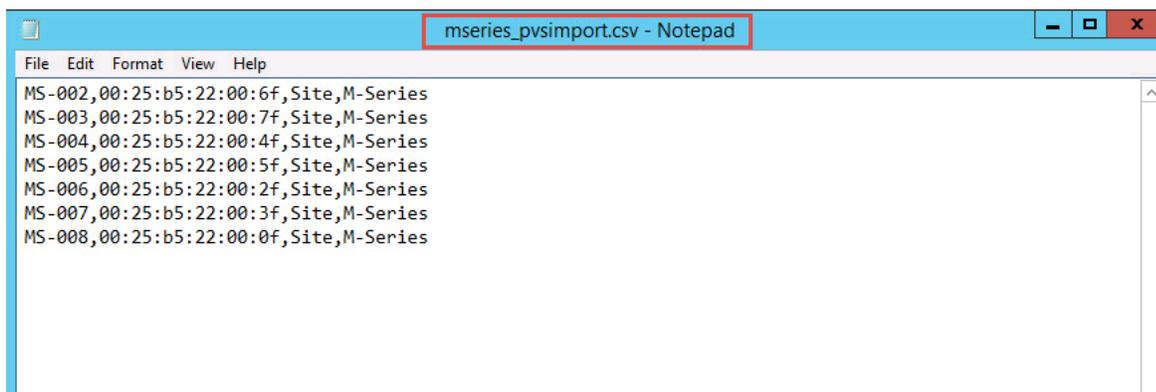


13. Click OK.

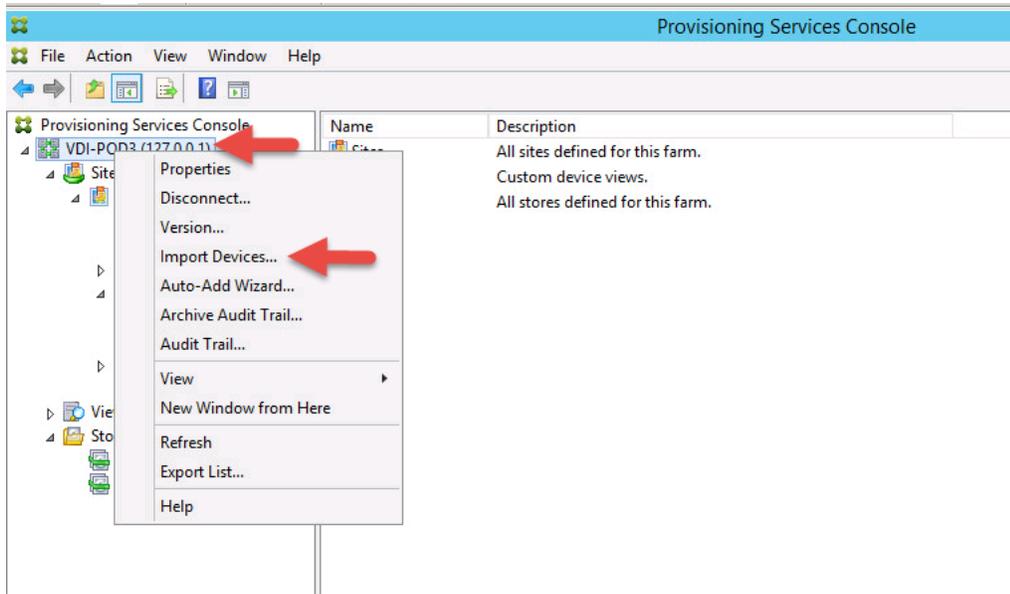
Import the Service Profiles as Machines and Create the XenDesktop Catalog and Group

To import service profiles as machines and create the XenDesktop Catalog and Group, complete the following steps:

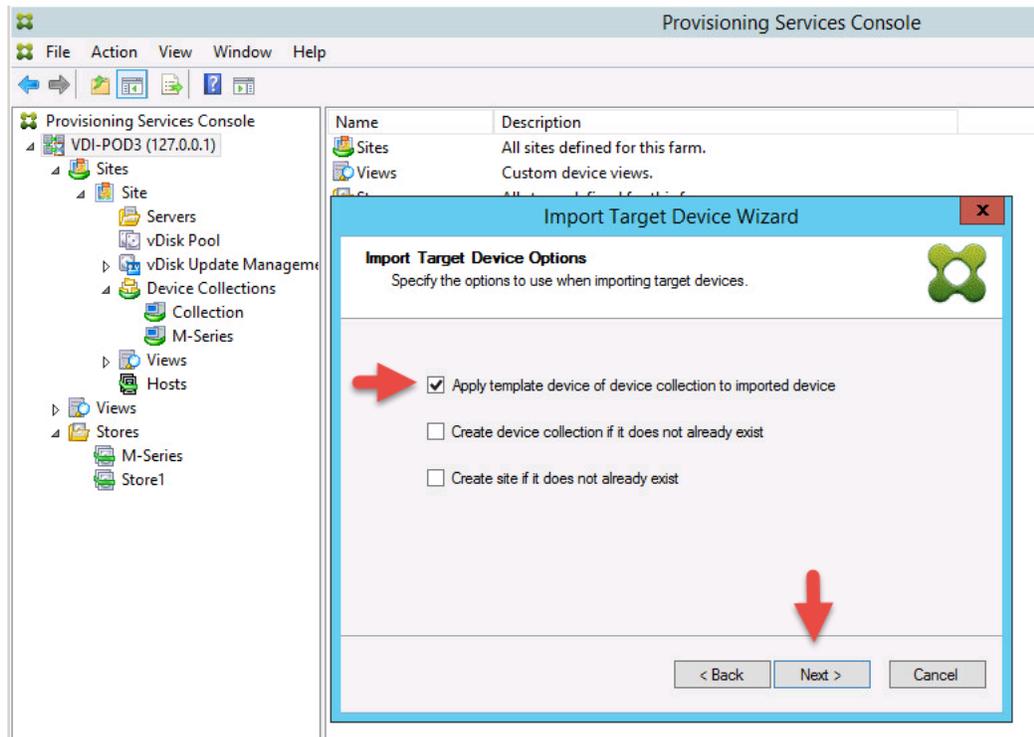
1. Create a CSV file with the following properties: <machine name>,<mac address>,<site name>,<collection name>. (MAC addresses can be gathered and exported from the MAC Pools area in UCSM).



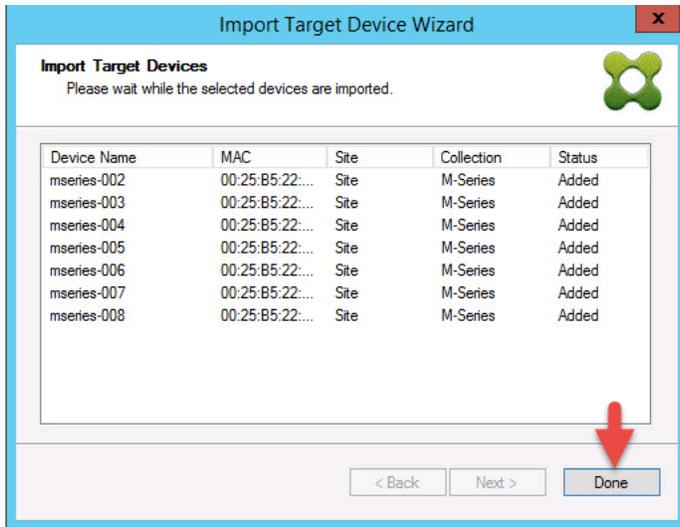
2. Use the CSV file to import the machines into PVS. Right-click the Farm node and select Import Devices.



3. Use the Wizard to point to the location of your CSV file, then uncheck the Create device collection and Create site check boxes and check the Apply template device check box before clicking Next on the Import Target Device Options dialogue.

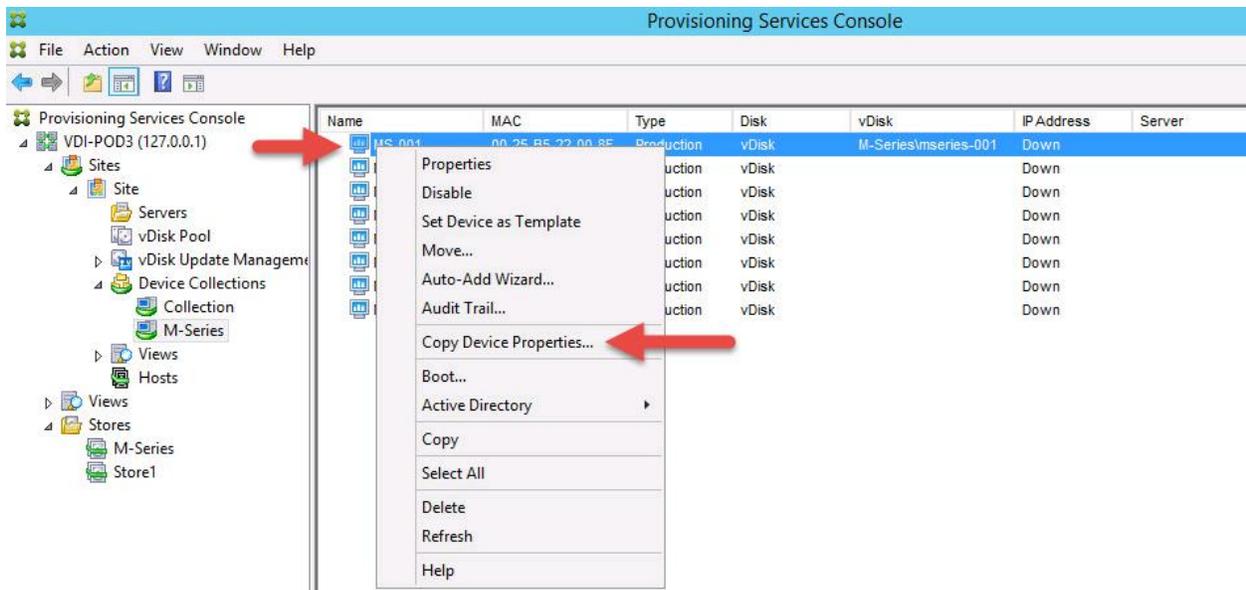


4. Click Next.

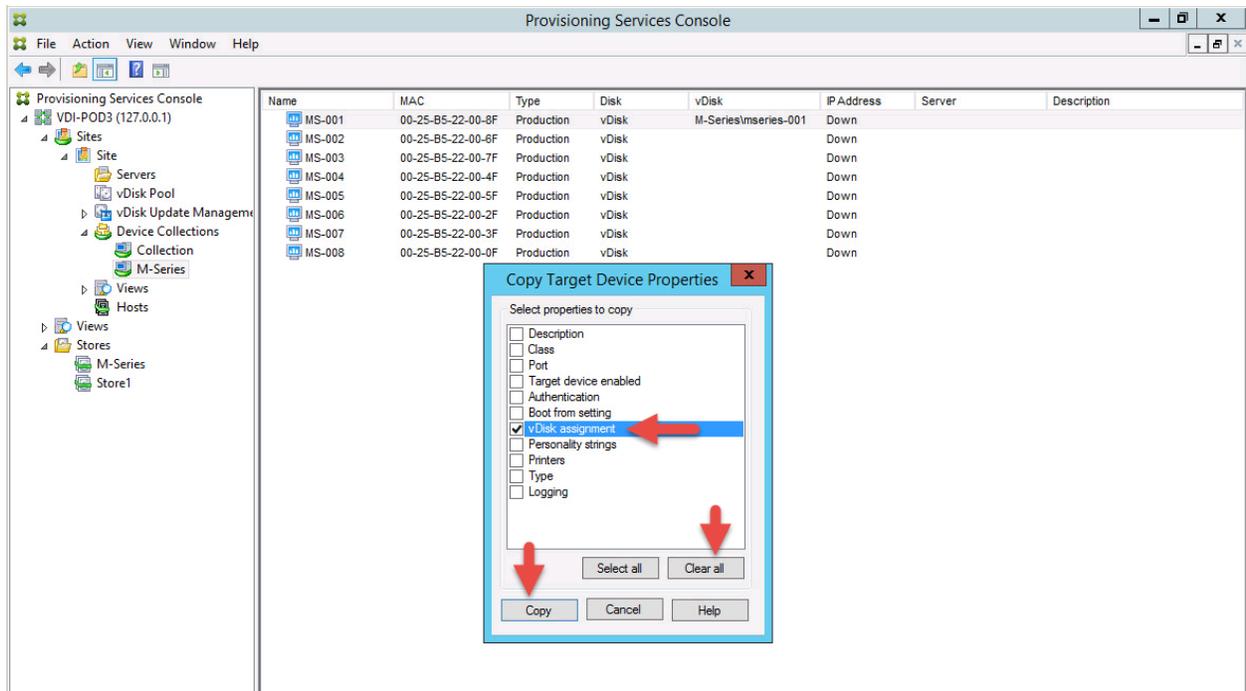


5. Click Done.

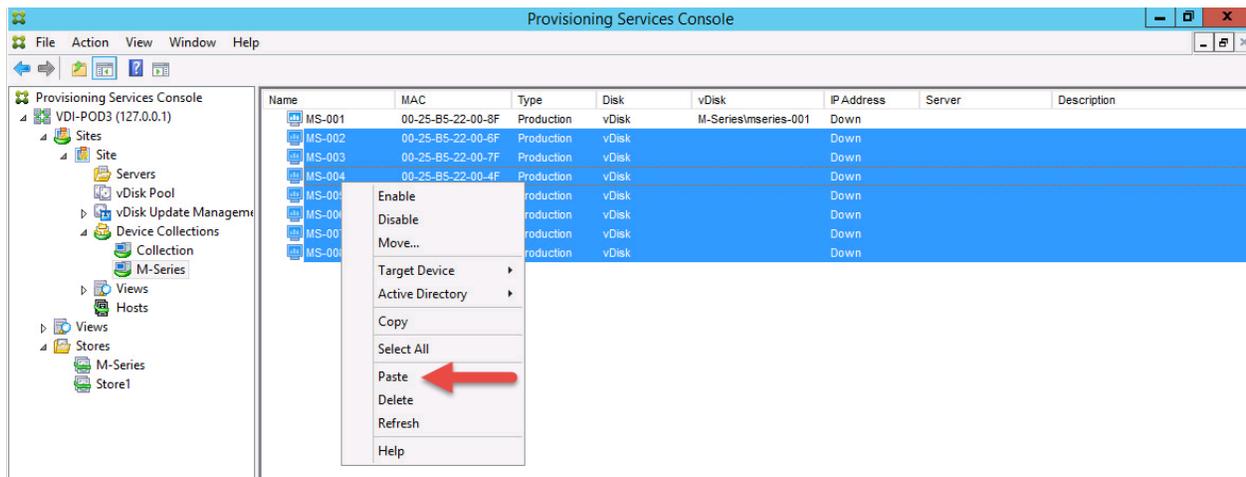
6. Click the M-Series device collection in the left pane, then right-click the MS-001 machine in the right pane, then click Copy Device Properties.



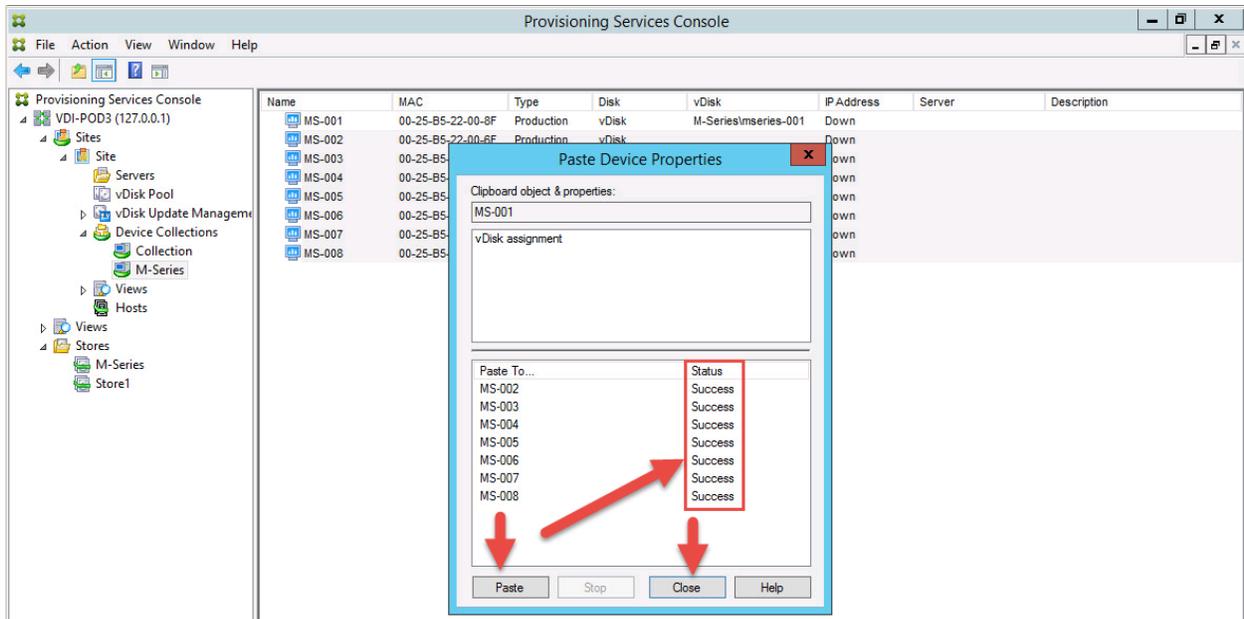
7. Click Clear All, click the vDisk assignment checkbox, and click Copy.



8. Click MS-002, then shift-click MS-008. Right-click the selected machines and click Paste.

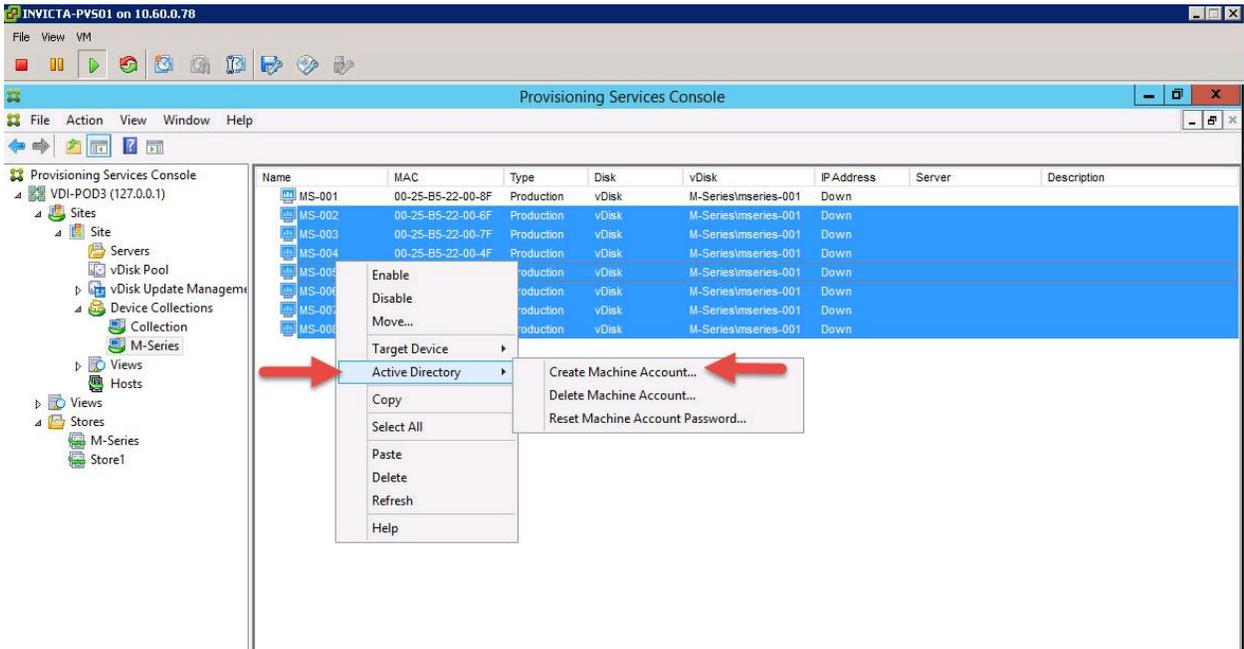


9. Click Paste in the Paste Device Properties dialog. Success displays in the Status column next to each machine.

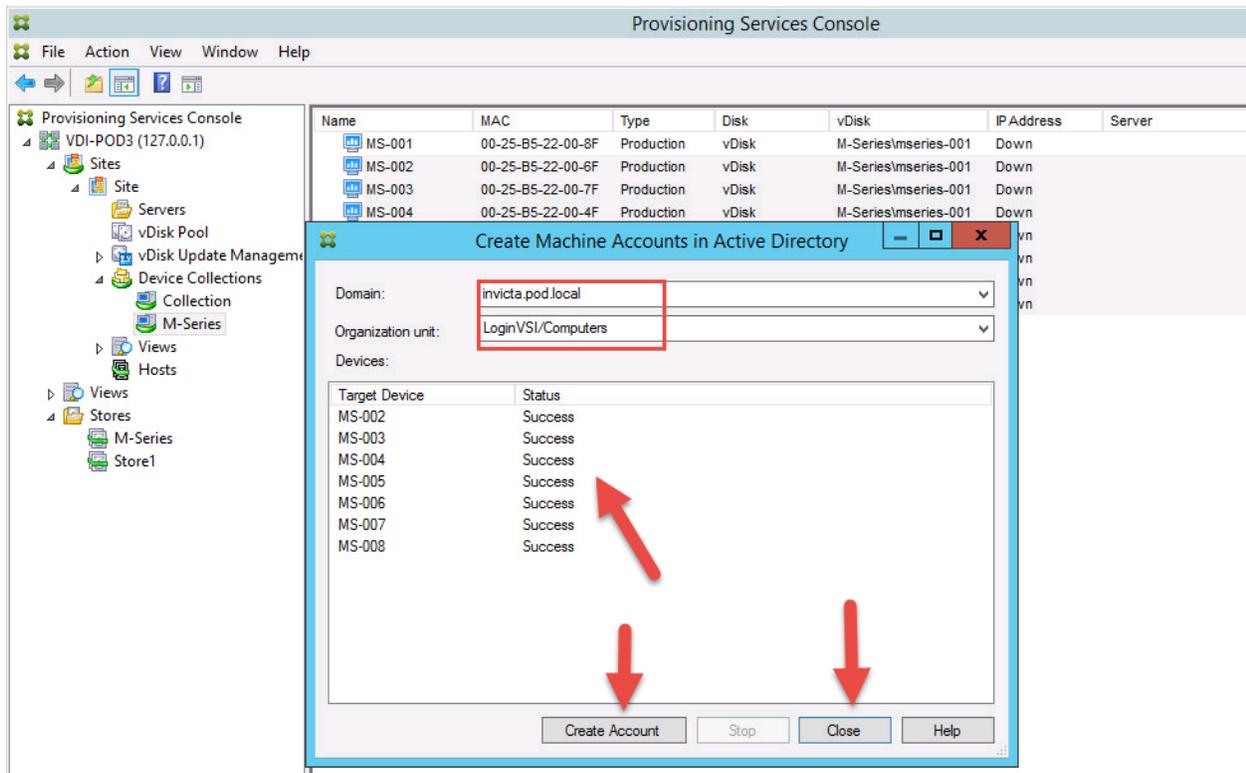


10. Click Close.

11. Highlight machines MS-002 through MS-008 in the right pane, right-click the group, click Active Directory, then Create Machine Account.

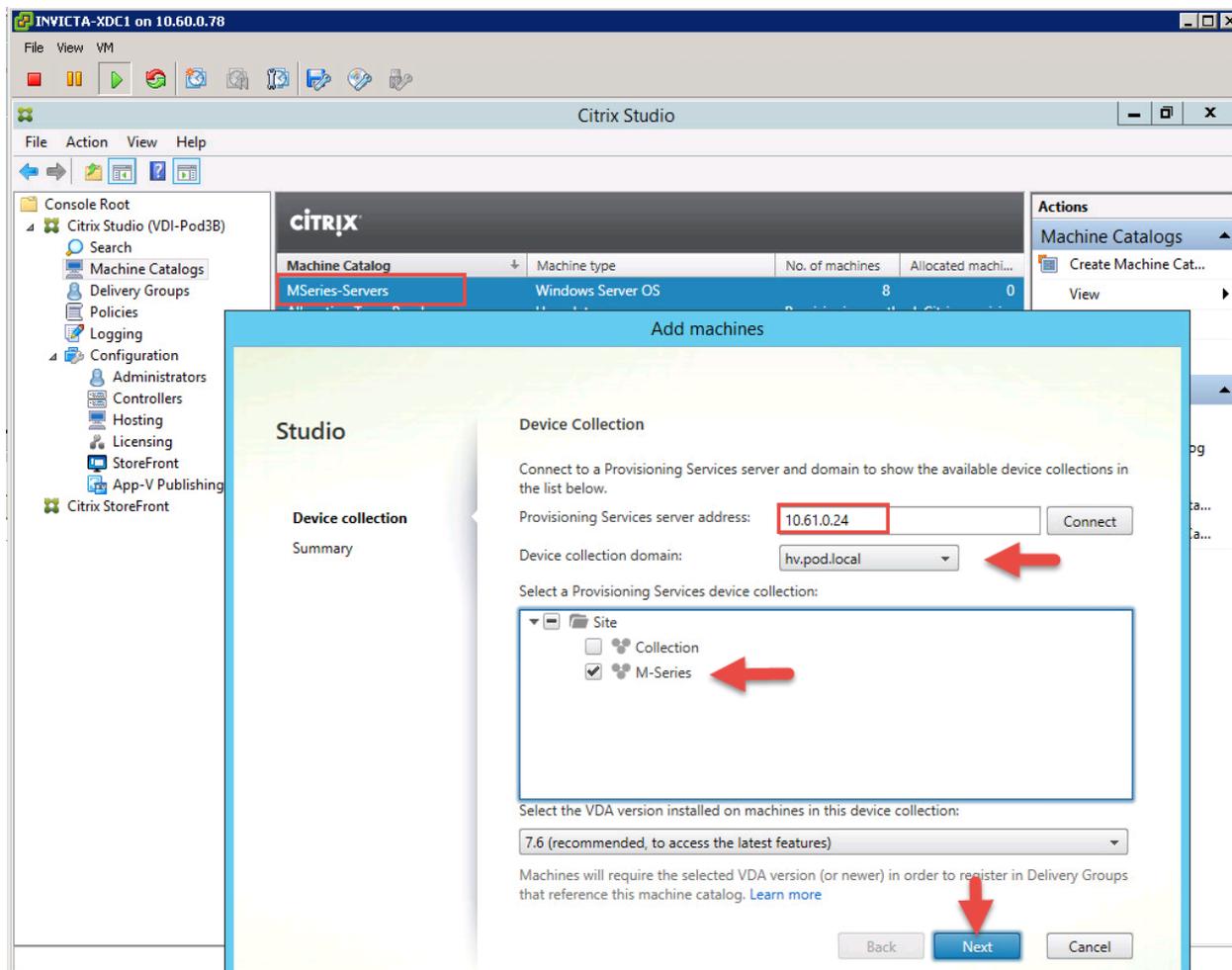


12. Select your domain, the correct OU, click Create Account. You should get Success in the Status column. Click Close.

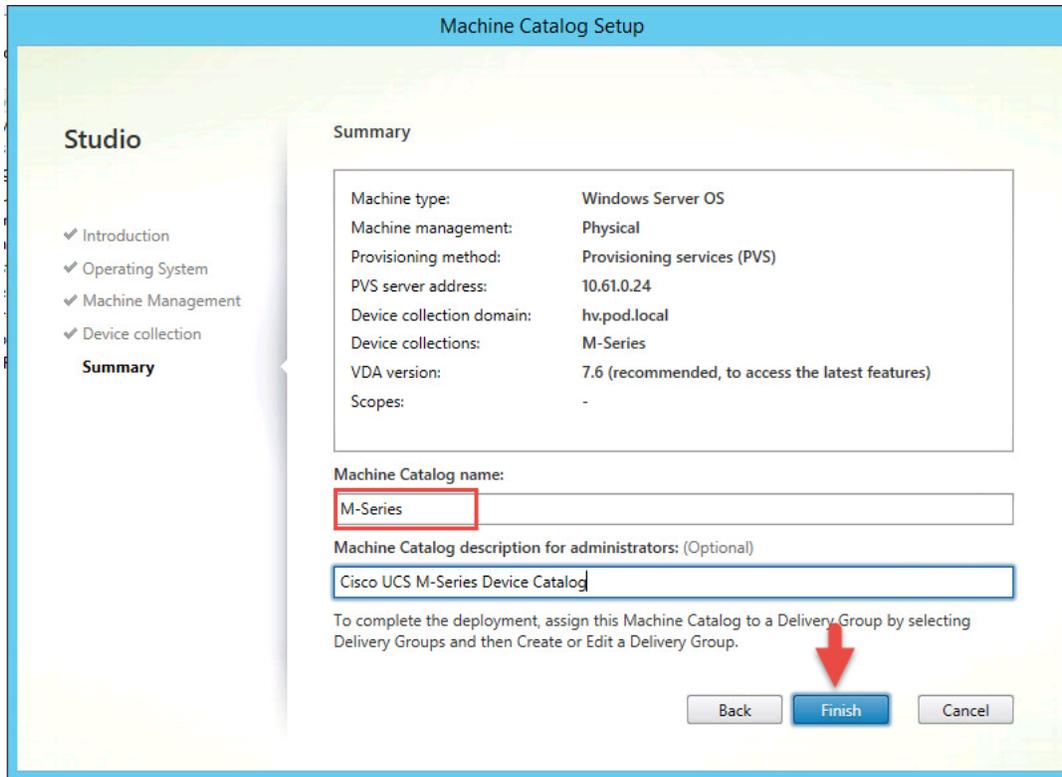


13. Open the Citrix XenApp 7.6 Studio.

14. Create a Machine Catalog for the M-Series servers. Provide the address of the PVS server and the device collection domain/OU. Click Connect, expand the Site and select the collection you will use.

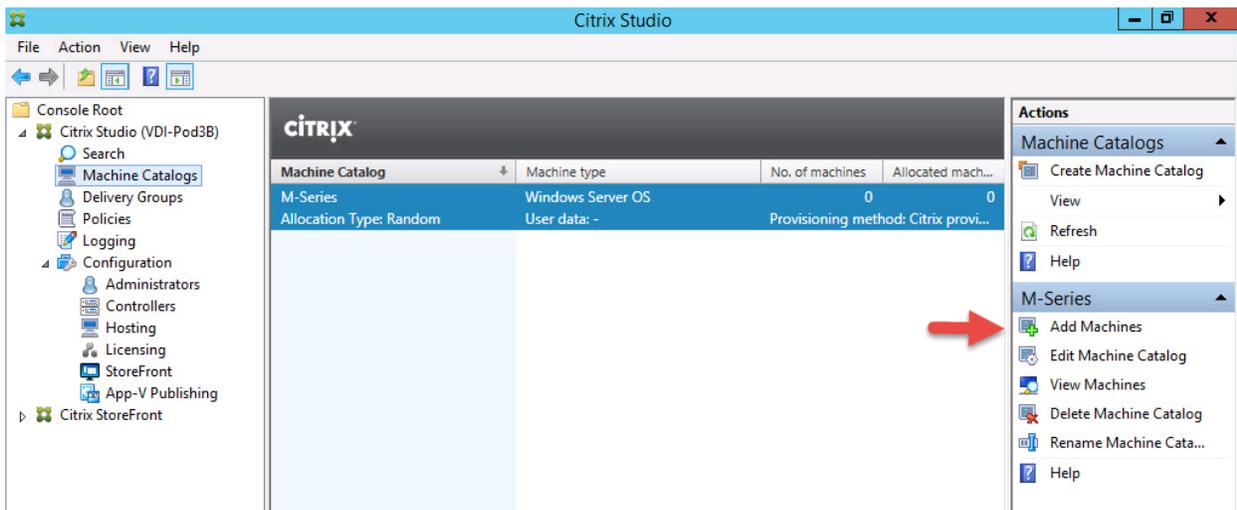


15. Provide a Machine Catalog name and description (optional).

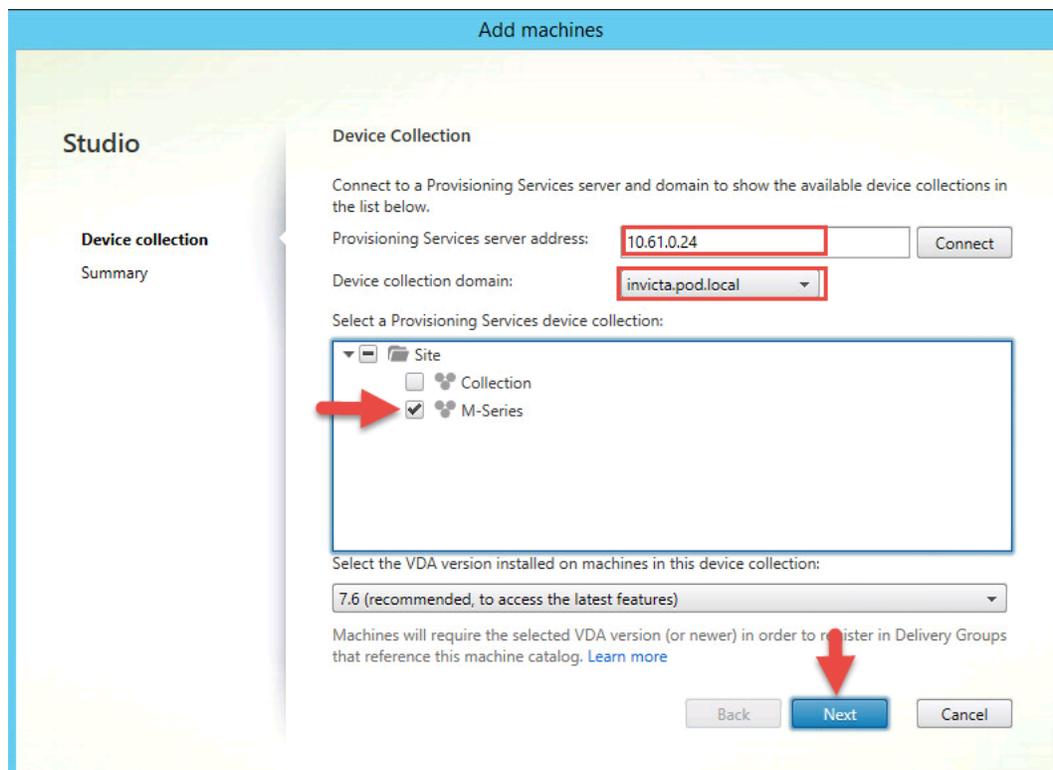


16. Click Finish.

17. Add the machines in your PVS Collection to the M-Series Machine Catalog; click the Add Machines task in the Actions pane.

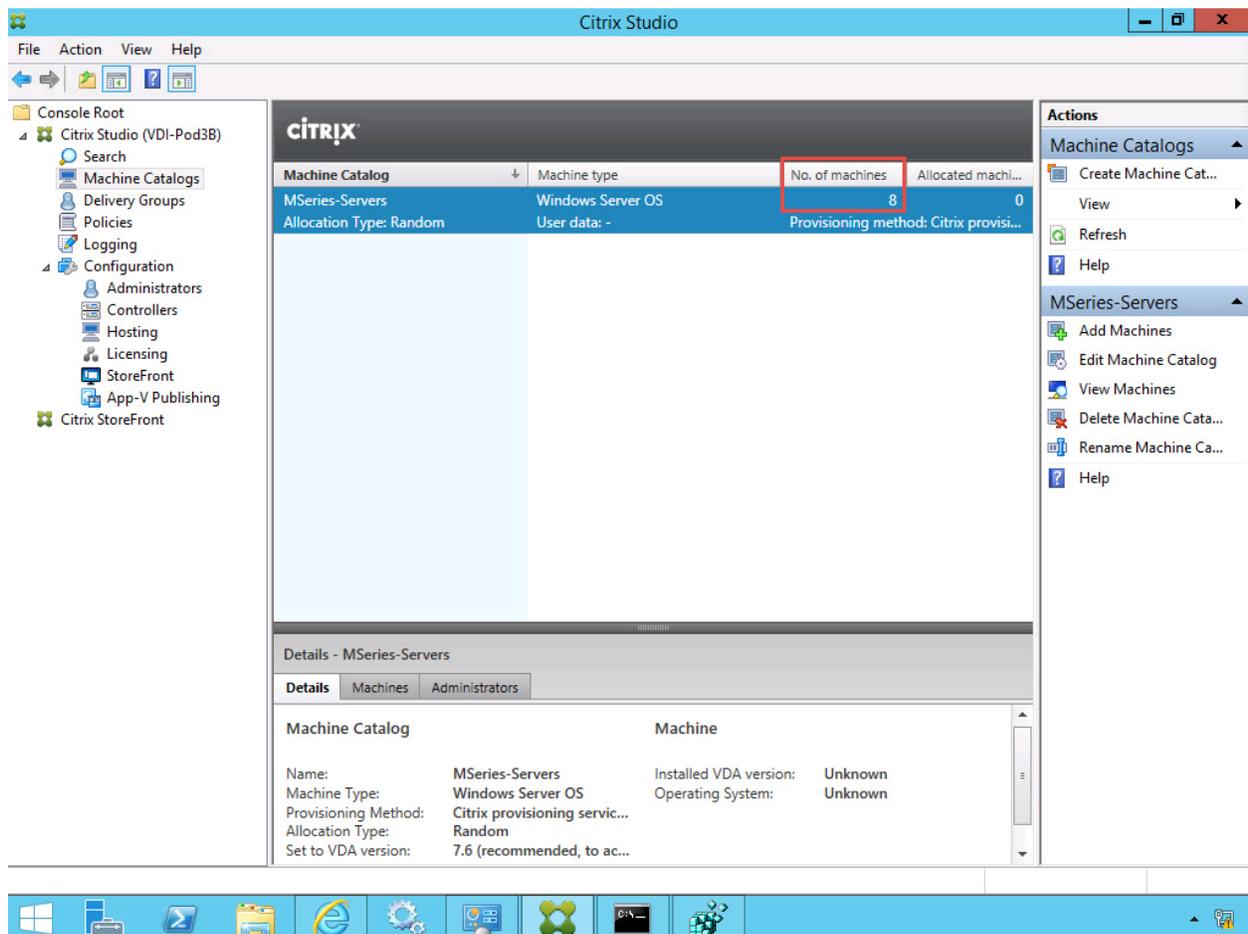


18. Input the PVS server's IP address, select the correct Device Collection domain, click Connect, select the PVS device collection, then click Next.

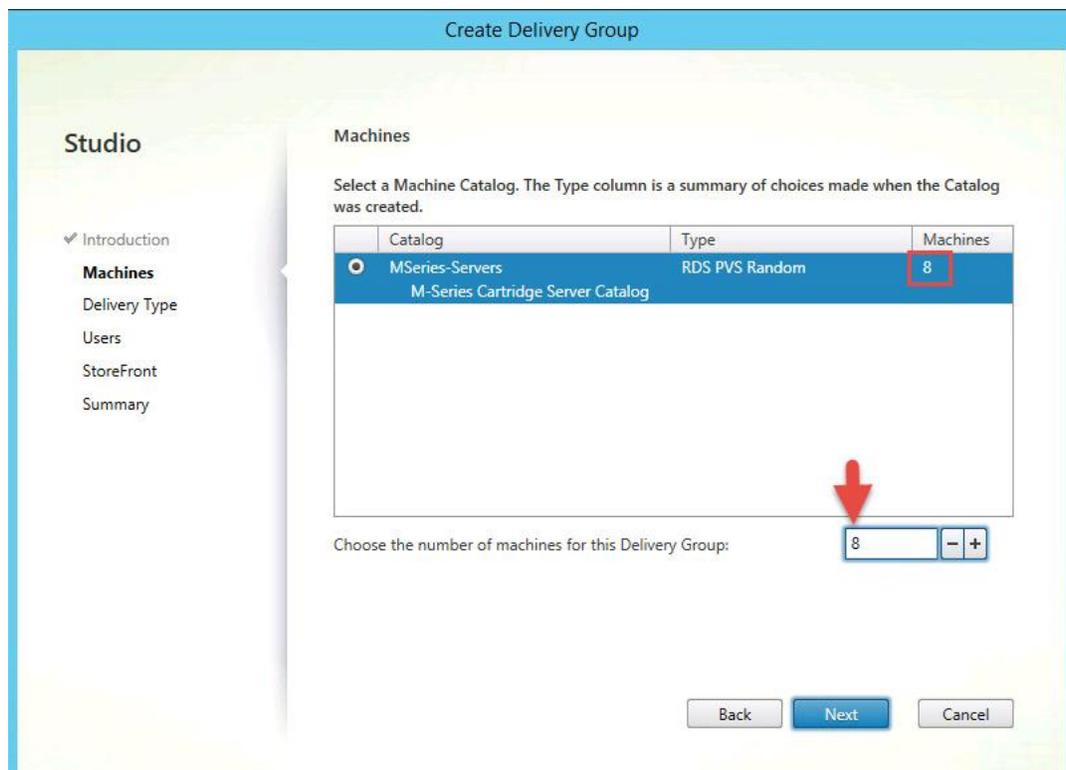


19. Click Finish on the Summary page.

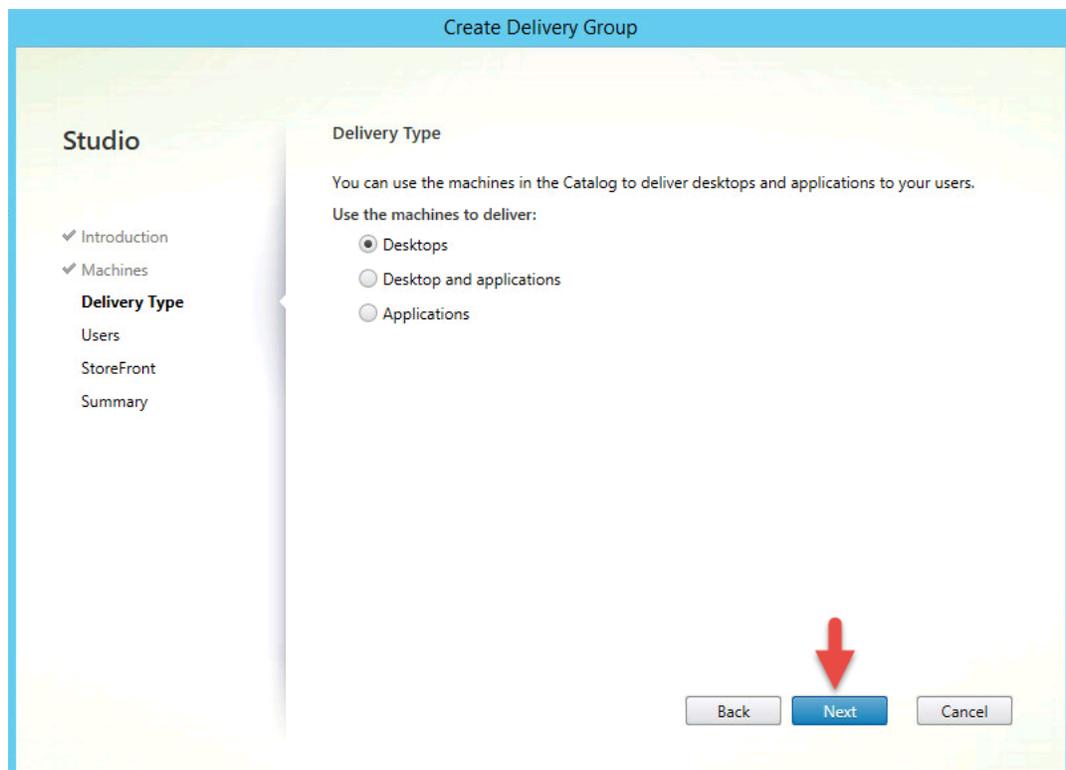
20. The eight servers you created with Provisioning Services in the M-Series site are imported.



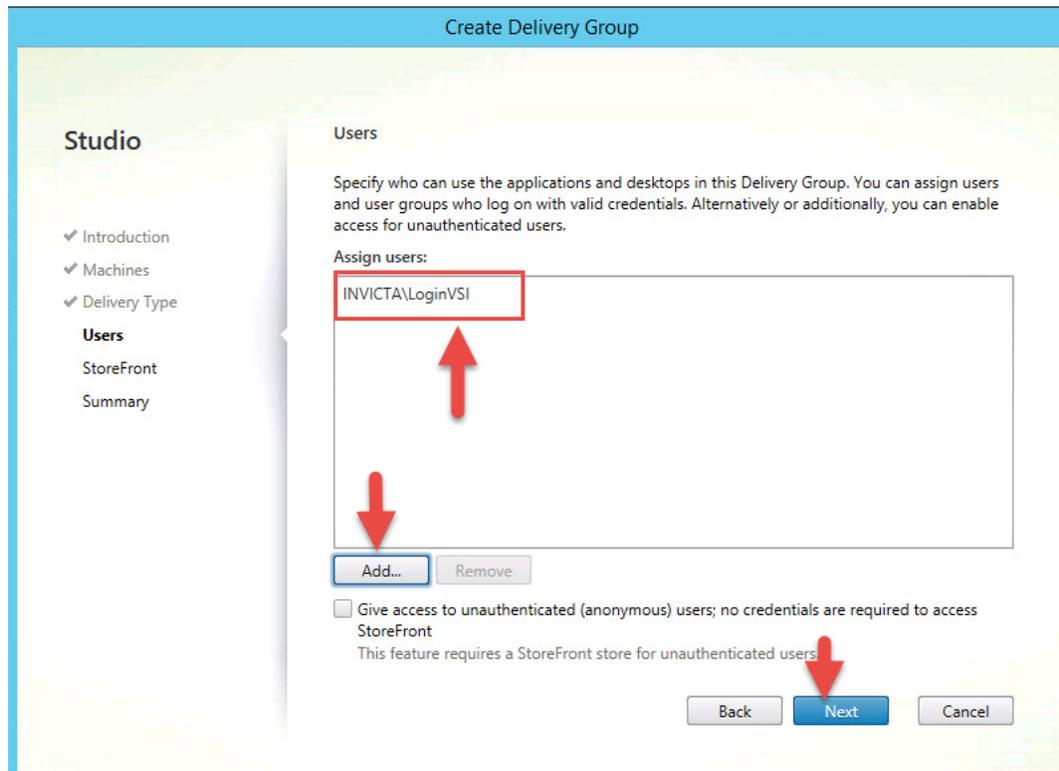
21. Click the Delivery Groups node in Studio, then click Create a Delivery Group in the action pane. Use the wizard to complete your configuration.



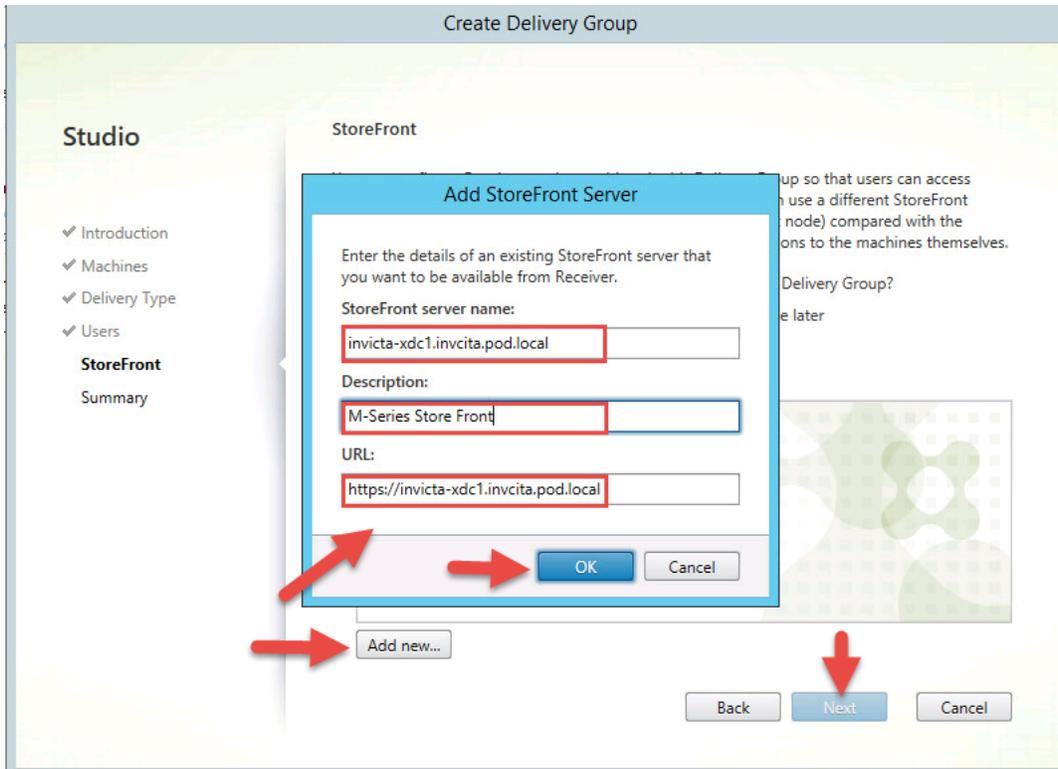
22. Click Desktops as the Delivery type and click Next.



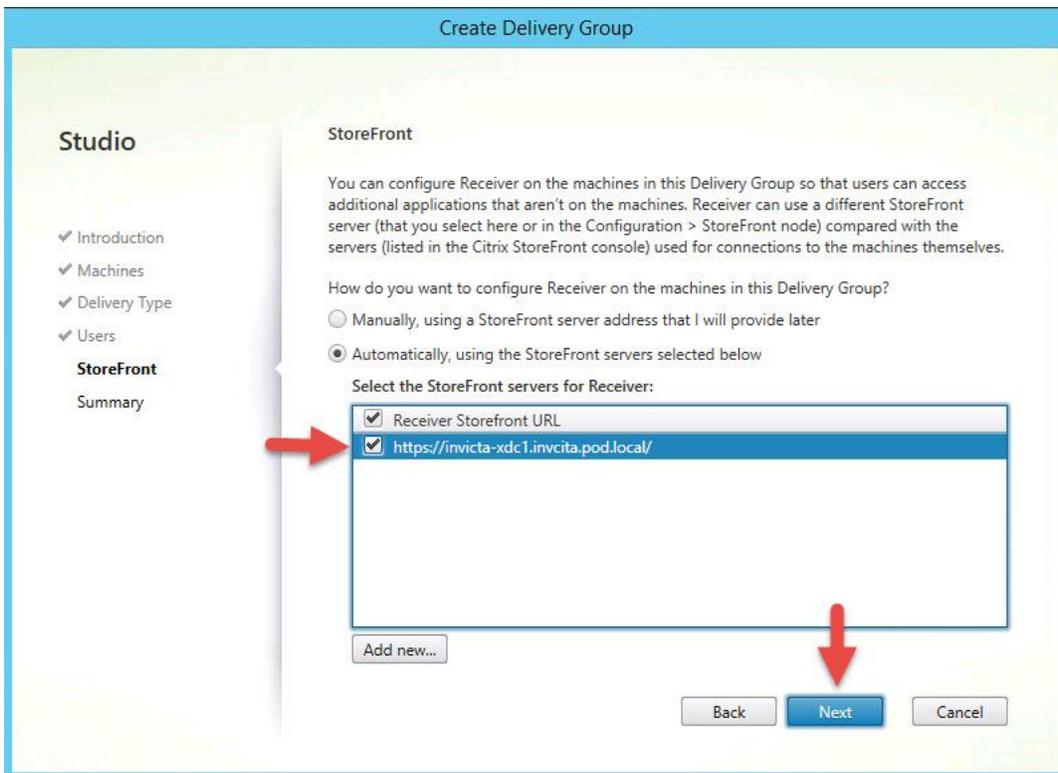
23. Click the Add button to browse for the user group that will be authorized for this Delivery Group, then click Next.



24. Add your StoreFront server information by clicking Add, providing the storefront server name, a description (required,) and the server URL.



25. Click the checkbox for your StoreFront server, then click Next.



26. Provide a Delivery Group Name and a Display name, then click Finish.

Create Delivery Group

Studio

- ✓ Introduction
- ✓ Machines
- ✓ Delivery Type
- ✓ Users
- ✓ StoreFront
- Summary**

Summary

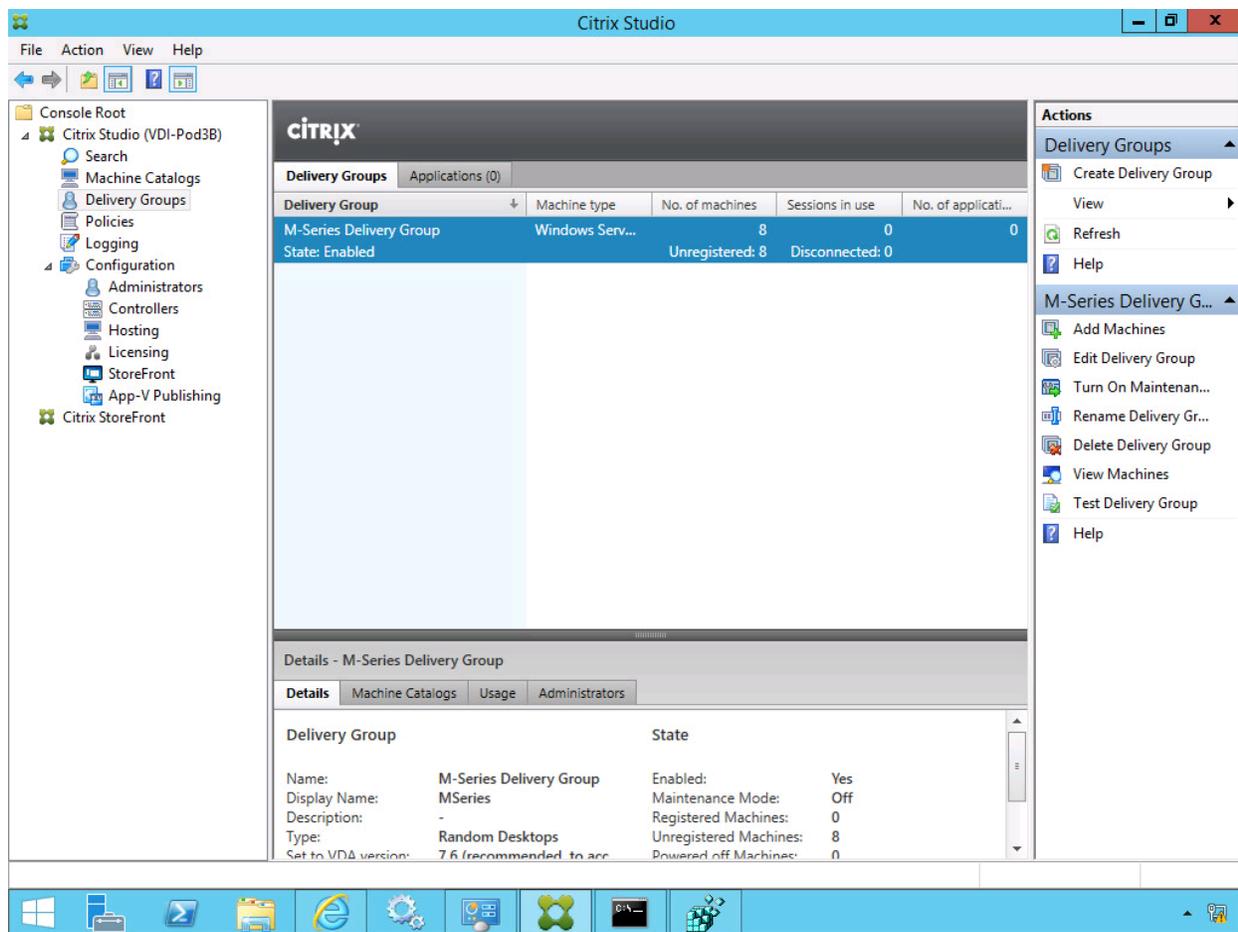
Machine Catalog:	MSeries-Servers
Machine type:	Windows Server OS
Allocation type:	Random
Machines added:	8 unassigned
Delivery type:	Desktops
Users:	INVICTA>LoginVSI
Storefronts:	1
Scopes:	-

Delivery Group name:

Display name:

Delivery Group description, used as label in Receiver (optional):

Your Delivery Group is created.



27. From the UCS Manager, boot all 8 servers. When all servers added to the Delivery Group have registered, they will be ready to accept user connections.

Citrix XenDesktop Policies and Profile Management

Policies and profiles allow the Citrix XenDesktop environment to be easily and efficiently customized. These policies should be implemented to ensure proper profile sizes, logon time efficiency and overall profile performance efficiency.

Configuring Citrix XenDesktop Policies

Citrix XenDesktop policies control user access and session environments, and are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types with each policy. Policies can contain multiple settings and are typically defined through Citrix Studio.



The Windows Group Policy Management Console can also be used if the network environment includes Microsoft Active Directory and permissions are set for managing Group Policy Objects.

The screenshot below shows policies for Login VSI testing in this CVD.

Figure 15 XenDesktop Policy

The screenshot displays the XenDesktop Policy configuration interface. On the left, a list of policies is shown, with 'Base Policy' selected. On the right, the 'Base Policy' settings are detailed, including various user and computer settings such as file redirection, printing, load management, and flash acceleration.

Policies	
1	Unfiltered
2	Base Policy
3	VDI Policy
4	RDS Policy

Base Policy	
Overview	Settings
▶	Auto connect client drives User setting - ICA\File Redirection Disabled (Default: Enabled)
▶	Auto-create client printers User setting - ICA\Printing\Client Printers Do not auto-create client printers (Default: Auto-create all client printers)
▶	Client printer redirection User setting - ICA\Printing Prohibited (Default: Allowed)
▶	Concurrent logons tolerance Computer setting - Load Management Value: 4 (Default: Value: 2)
▶	CPU usage Computer setting - Load Management Disabled (Default: Disabled)
▶	CPU usage excluded process priority Computer setting - Load Management Disabled (Default: Below Normal or Low)
▶	Flash acceleration User setting - ICA\Adobe Flash Delivery\Flash Redirection Disabled (Default: Enabled)
▶	Flash default behavior User setting - ICA\Adobe Flash Delivery\Flash Redirection Disable Flash acceleration (Default: Enable Flash acceleration)
▶	Memory usage Computer setting - Load Management Disabled (Default: Disabled)
▶	Memory usage base load Computer setting - Load Management Disabled (Default: Zero load: 768 MBs)

Configuring User Profile Management

Profile management provides an easy, reliable, and high-performance way to manage user personalization settings in virtualized or physical Windows environments. It requires minimal infrastructure and administration, and provides users with fast logons and logoffs. A Windows user profile is a collection of folders, files, registry settings, and configuration settings that define the environment for a user who logs on with a particular user account. These settings may be customizable by the user, depending on the administrative configuration. Examples of settings that can be customized are:

- Desktop settings such as wallpaper and screen saver
- Shortcuts and Start menu setting
- Internet Explorer Favorites and Home Page
- Microsoft Outlook signature
- Printers

Some user settings and data can be redirected by means of folder redirection. However, if folder redirection is not used these settings are stored within the user profile.

The first stage in planning a profile management deployment is to decide on a set of policy settings that together form a suitable configuration for your environment and users. The automatic configuration feature simplifies some of this decision-making for XenDesktop deployments. Screenshots of the User Profile

Management interfaces that establish policies for this CVD's RDS and VDI users (for testing purposes) are shown below. Basic profile management policy settings are documented here: <http://support.citrix.com/proddocs/topic/xendesktop-71/cds-policies-rules-pm.html>.

Figure 16 VDI User Profile Manager Policy

The screenshot displays the Citrix Policy Manager interface. On the left, a 'Policies' list shows 'VDI Policy' selected. The main pane shows the 'VDI Policy' configuration with tabs for 'Overview', 'Settings', and 'Assigned to'. The 'Settings' tab is active, showing a list of policy settings:

- Active write back**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)
- Delete locally cached profiles on logoff**: Computer setting - Profile Management\Profile handling, Enabled (Default: Disabled)
- Enable Profile management**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)
- Exclusion list - directories**: Computer setting - Profile Management\File system\Exclusions, AppData\Local;AppData\LocalLow;AppData\Roaming;\$Recycle.Bin (Default:)
- Path to user store**: Computer setting - Profile Management\Basic settings, \\NA-CIFS-01-13\Profiles\$\VDI (Default: Windows)
- Process logons of local administrators**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)

Figure 17 RDS User Profile Manager Policy

The screenshot displays the Citrix Policy Manager interface. On the left, a 'Policies' list shows 'RDS Policy' selected. The main pane shows the 'RDS Policy' configuration with tabs for 'Overview', 'Settings', and 'Assigned to'. The 'Settings' tab is active, showing a list of policy settings:

- Active write back**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)
- Delete locally cached profiles on logoff**: Computer setting - Profile Management\Profile handling, Enabled (Default: Disabled)
- Enable Profile management**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)
- Exclusion list - directories**: Computer setting - Profile Management\File system\Exclusions, AppData\Local;AppData\LocalLow;AppData\Roaming;\$Recycle.Bin (Default:)
- Path to user store**: Computer setting - Profile Management\Basic settings, \\NA-CIFS-01-13\Profiles\$\RDS (Default: Windows)
- Process logons of local administrators**: Computer setting - Profile Management\Basic settings, Enabled (Default: Disabled)

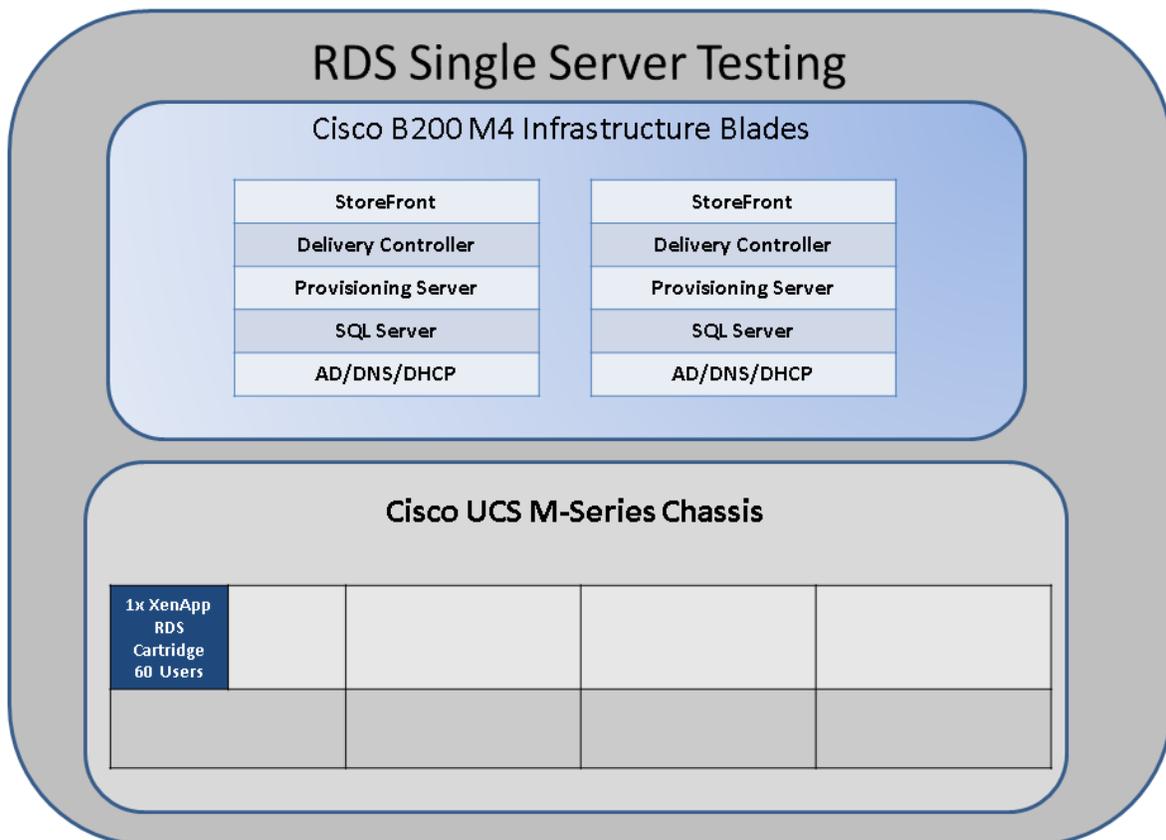
Validation

Test Setup and Configuration

In this project, we tested a single Cisco UCS M142-M4 Server compute node in a single chassis and a fully populated chassis with 16 compute nodes to illustrate linear scalability for each workload studied.

Cisco UCS Test Configuration for Single Blade Scalability

Figure 18 Cisco UCS M142-M4 Server for Single Server Scalability XenApp 7.6 RDS/HSD with PVS 7.6



Hardware components:

- Cisco UCS M4308 M-Series Server Chassis
- 2 Cisco UCS 6248UP Fabric Interconnects
- 1 Cisco M142-M4 M-Series Cartridges with 1 compute node for XenApp workload.
- 2 Cisco UCS B200 M4 Blade Servers (2 Intel Xeon processor E5-2660 v3 CPUs at 2.6 GHz, with 256 GB of memory per blade server [16 GB x 15 DIMMs at 2133 MHz]) for all Infrastructure blades
- Cisco sNIC CNA (1 per blade)

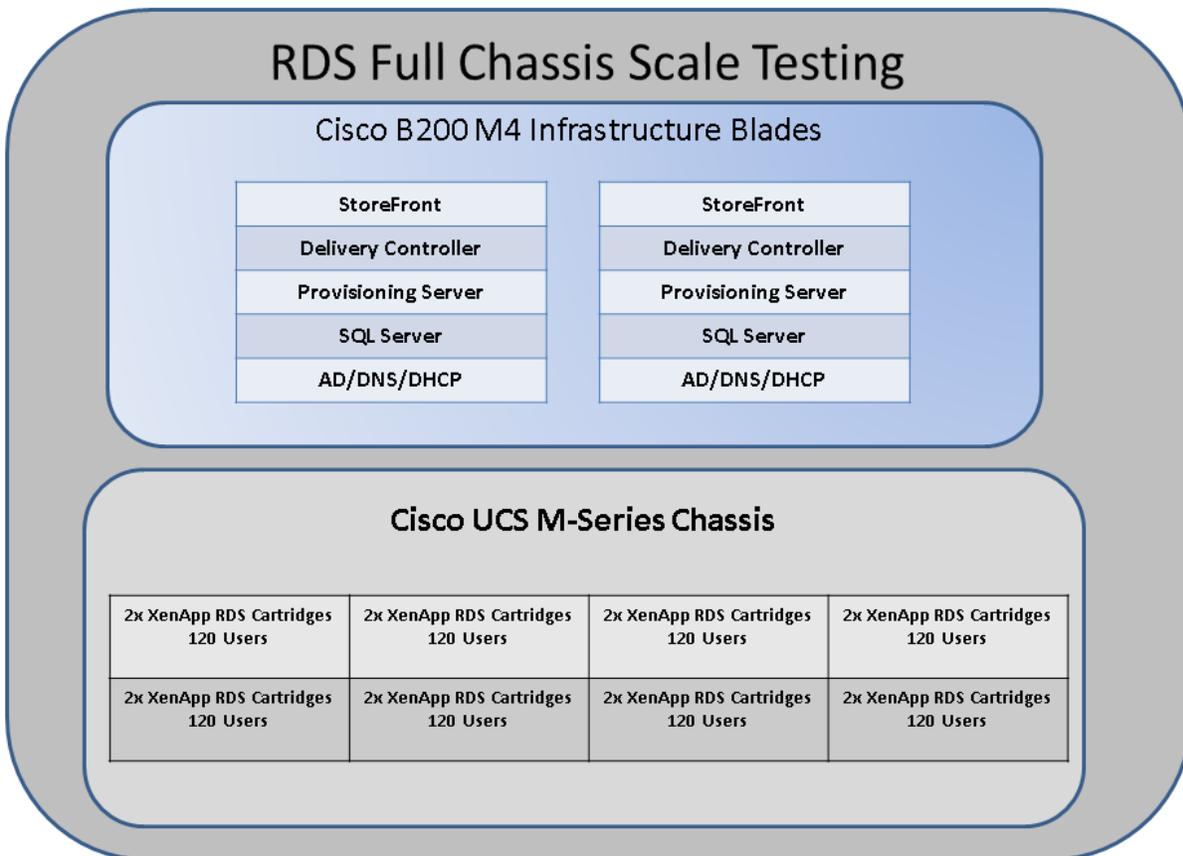
- 2 Cisco Nexus 5548UP Access Switches

Software components:

- Cisco UCS firmware 2.5(2a)
- Citrix XenApp 7.6 RDS Hosted Shared Desktops
- Citrix Provisioning Server 7.6
- Citrix User Profile Manager
- Microsoft SQL Server 2012
- Microsoft Windows Server 2012 R2, 5vCPU, 32GB RAM, 40 GB vdisk, 40GB Write Cache
- Microsoft Office 2010
- Login VSI 4.1.4

Cisco UCS Configuration for Scale Testing

Figure 19 Sixteen Server Workload XenApp 7.6 RDS Hosted Shared Desktops with 960 Users



Hardware components:

- Cisco UCS M4308 M-Series Server Chassis
- 2 Cisco UCS 6248UP Fabric Interconnects
- 8 Cisco M142-M4 M-Series Cartridges with 16 compute nodes for XenApp workloads.
- 2 Cisco UCS B200 M4 Blade Servers (2 Intel Xeon processor E5-2660 v3 CPUs at 2.6 GHz, with 256 GB of memory per blade server [16 GB x 15 DIMMs at 2133 MHz]) for all Infrastructure blades
- Cisco sNIC CNA (1 per blade)
- 2 Cisco Nexus 5548UP Access Switches

Software components:

- Cisco UCS firmware 2.5(2a)
- Citrix XenApp 7.6 RDS Hosted Shared Desktops
- Citrix Provisioning Server 7.6
- Citrix User Profile Manager
- Microsoft SQL Server 2012
- Microsoft Windows Server 2012 R2, 5vCPU, 32GB RAM, 40 GB vdisk, 40GB Write Cache
- Microsoft Office 2010
- Login VSI 4.1.4

Testing Methodology and Success Criteria

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

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 Citrix XenApp RDS Hosted Shared models under test.

Test metrics were gathered from the 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.

You can obtain additional information and a free test license from <http://www.loginvsi.com>.

Testing Procedure

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

Pre-Test Setup for Single and Multi-Blade Testing

All machines were shut down utilizing the XenApp 7.6 Administrator.

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.**

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 48 minutes. Additionally, we require all sessions started, whether 60 single server users or 900 full scale test users to become active within two minutes after the last session is launched.

In addition, Cisco requires that the Login VSI Benchmark method is used for all single server and scale testing. This assures that our tests represent real-world scenarios. For each of the three consecutive runs on single server tests, the same process was followed. Complete the following steps:

1. Time 0:00:00 Start PerfMon Logging on the following systems:
 - Infrastructure and VDI Host Blades used in test run
 - All Infrastructure VMs used in test run (AD, SQL, brokers, image mgmt., etc.)
2. Time 0:00:10 Start Storage Partner Performance Logging on Storage System.
3. Time 0:05: Boot RDS Machines using XenDesktop Studio UCSM KVM.
4. Time 0:06 First machines boot.
5. Time 0:35 Single Server or Scale target number of RDS Servers registered on XD.



No more than 60 Minutes of rest time is allowed after the last desktop is registered on the XD Studio or available in View Connection Server dashboard. Typically a 30 minute rest period for Windows 7 desktops and 15 minutes for RDS VMs is sufficient.

6. Time 1:35 Start Login VSI 4.1.4 Office Worker Benchmark Mode Test, setting auto-logoff time at 900 seconds, with Single Server or Scale target number of desktop VMs utilizing sufficient number of Launchers (at 20-25 sessions/Launcher).
7. Time 2:23 Single Server or Scale target number of desktop VMs desktops launched (48 minute benchmark launch rate).
8. Time 2:25 All launched sessions must become active.



All sessions launched must become active for a valid test run within this window.

9. Time 2:40 Login VSI Test Ends (based on Auto Logoff 900 Second period designated above).

10. Time 2:55 All active sessions logged off.



All sessions launched and active must be logged off for a valid test run. The XD Studio or View Connection Dashboard must show that all desktops have been returned to the registered/available state as evidence of this condition being met.

11. Time 2:57 All logging terminated; Test complete.

12. Time 3:15 Copy all log files off to archive; Set virtual desktops to maintenance mode through broker; Shutdown all Windows 7 machines.

13. Time 3:30 Reboot all hypervisors.

14. Time 3:45 Ready for new test sequence.

Success Criteria

Our “pass” criteria for this testing follows is 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 4.1 Office Worker workloads. The number of launched sessions must equal active sessions within two minutes of the last session launched in a test as observed on the VSI Management console.

The Citrix Desktop Studio or VMware Horizon with View Connection Server Dashboard will be monitored throughout the steady state to make sure of the following:

- All running sessions report In Use throughout the steady state
- No sessions move to unregistered, unavailable 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. Stuck sessions define a test failure condition.

Cisco requires three consecutive runs with results within +/-1% variability to pass the Cisco Validated Design performance criteria. For white papers written by partners, two consecutive runs within +/-1% variability are accepted. (All test data from partner run testing must be supplied along with proposed white paper.)

We will publish Cisco Validated Designs with our recommended workload following the process above and will note that we did not reach a VSImax dynamic in our testing. Cisco UCS M-Series Modular Servers with XenApp 7.6 Test Results

The purpose of this testing is to provide the data needed to validate Citrix XenApp 7.6 Hosted Shared Desktop with Citrix Provisioning Services 7.6 using Microsoft Windows Server 2012 R2 sessions on Cisco UCS M-Series M142-M4 Modular Compute Cartridges on Local Storage.

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 Citrix products.

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

VSImax 4.1.x Description

The philosophy behind Login VSI is different to conventional benchmarks. In general, most system benchmarks are steady state benchmarks. These benchmarks execute one or multiple processes, and the measured execution time is the outcome of the test. Simply put: the faster the execution time or the bigger the throughput, the faster the system is according to the benchmark.

Login VSI is different in approach. Login VSI is not primarily designed to be a steady state benchmark (however, if needed, Login VSI can act like one). Login VSI was designed to perform benchmarks for SBC or VDI workloads through system saturation. Login VSI loads the system with simulated user workloads using well known desktop applications like Microsoft Office, Internet Explorer and Adobe PDF reader. By gradually increasing the amount of simulated users, the system will eventually be saturated. Once the system is saturated, the response time of the applications will increase significantly. This latency in application response times show a clear indication whether the system is (close to being) overloaded. As a result, by nearly overloading a system it is possible to find out what its true maximum user capacity is.

After a test is performed, the response times can be analyzed to calculate the maximum active session/desktop capacity. Within Login VSI this is calculated as VSImax. When the system is coming closer to its saturation point, response times will rise. When reviewing the average response time it will be clear the response times escalate at saturation point.

This VSImax is the “Virtual Session Index (VSI)”. With Virtual Desktop Infrastructure (VDI) and Terminal Services (RDS) workloads this is valid and useful information. This index simplifies comparisons and makes it possible to understand the true impact of configuration changes on hypervisor host or guest level.

Server-Side Response Time Measurements

It is important to understand why specific Login VSI design choices have been made. An important design choice is to execute the workload directly on the target system within the session instead of using remote sessions. The scripts simulating the workloads are performed by an engine that executes workload scripts **on every target system, and are initiated at logon within the simulated user’s desktop session context.**

An alternative to the Login VSI method would be to generate user actions client side through the remoting protocol. These methods are always specific to a product and vendor dependent. More importantly, some protocols simply do not have a method to script user actions client side.

For Login VSI the choice has been made to execute the scripts completely server side. This is the only practical and platform independent solution, for a benchmark like Login VSI.

Calculating VSImax v4.1.x

The simulated desktop workload is scripted in a 48 minute loop when a simulated Login VSI user is logged on, performing generic Office worker activities. After the loop is finished it will restart automatically. Within each loop the response times of sixteen specific operations are measured in a regular interval: sixteen times in within each loop. The response times of these five operations are used to determine VSImax.

The five operations from which the response times are measured are:

- Notepad File Open (NFO)

Loading and initiating VSINotepad.exe and opening the openfile dialog. This operation is handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an **end-user's point of view**.

- Notepad Start Load (NSLD)

Loading and initiating VSINotepad.exe and opening a file. This operation is also handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an **end-user's point of view**.

- Zip High Compression (ZHC)

This action copy's a random file and compresses it (with 7zip) with high compression enabled. The compression will very briefly spike CPU and disk IO.

- Zip Low Compression (ZLC)

This action copy's a random file and compresses it (with 7zip) with low compression enabled. The compression will very briefly spike disk IO and creates some load on the CPU.

- CPU

Calculates a large array of random data and spikes the CPU for a short period of time.

These measured operations within 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 become 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. If such operations consistently consume multiple seconds the user will regard the system as slow and unresponsive.

Figure 20 Sample of a VSI Max Response Time Graph, Representing a Normal Test

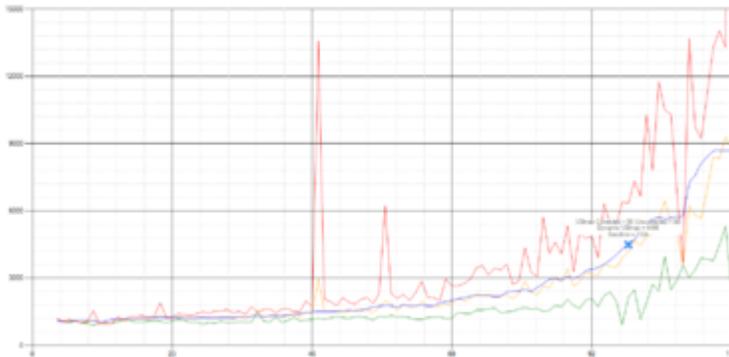
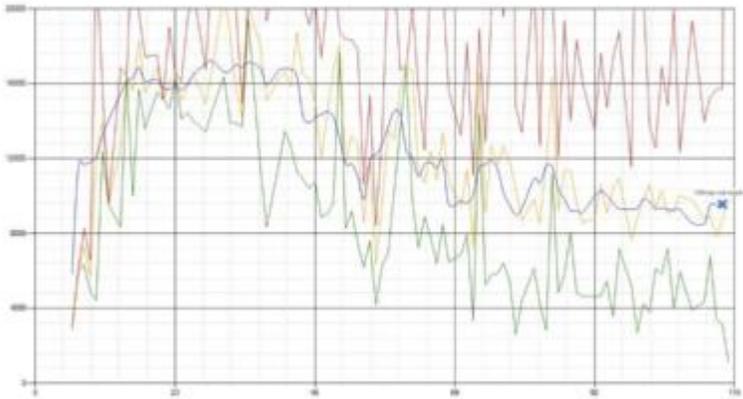


Figure 21 Sample of a VSI Test Response Time Graph with a Clear Performance Issue



When the test is finished, VSImax can be calculated. When the system is not saturated, and it could complete the full test without exceeding the average response time latency threshold, VSImax is not reached and the amount of sessions ran successfully.

The response times are very different per measurement type, for instance Zip with compression can be around 2800 ms, while the Zip action without compression can only take 75ms. These response time of these actions are weighted before they are added to the total. This ensures that each activity has an equal impact on the total response time.

In comparison to previous VSImax models, this weighting much better represent system performance. All actions have very similar weight in the VSImax total. The following weighting of the response times are applied.

The following actions are part of the VSImax v4.1 calculation and are weighted as follows (US notation):

- Notepad File Open (NFO): 0.75
- Notepad Start Load (NSLD): 0.2
- Zip High Compression (ZHC): 0.125
- Zip Low Compression (ZLC): 0.2
- CPU: 0.75

This weighting is applied on the baseline and normal Login VSI response times.

With the introduction of Login VSI 4.1 we also created a new method to calculate the basephase of an environment. With the new workloads (Taskworker, Powerworker, etc.) enabling 'basephase' for a more reliable baseline has become obsolete. The calculation is explained below. In total 15 lowest VSI response time samples are taken from the entire test, the lowest 2 samples are removed and the 13 remaining samples are averaged. The result is the Baseline. The calculation is as follows:

- Take the lowest 15 samples of the complete test
- From those 15 samples remove the lowest 2
- Average the 13 results that are left is the baseline

The VSImax average response time in Login VSI 4.1.x is calculated on the amount of active users that are logged on the system.

Always a 5 Login VSI response time samples are averaged + 40% of the **amount of “active” sessions**. For example, if the active sessions is 60, then latest 5 + 24 (=40% of 60) = 31 response time measurement are used for the average calculation.

To remove noise (accidental spikes) from the calculation, the top 5% and bottom 5% of the VSI response time samples are removed from the average calculation, with a minimum of 1 top and 1 bottom sample. As a result, with 60 active users, the last 31 VSI response time sample are taken. From those 31 samples the top 2 samples are removed and lowest 2 results are removed (5% of 31 = 1.55, rounded to 2). At 60 users the average is then calculated over the 27 remaining results.

VSImax v4.1.x is reached when the VSImax + a 1000 ms latency threshold is not reached by the average VSI response time result. Depending on the tested system, VSImax response time can grow 2 - 3x the baseline average. In end-user computing, a 3x increase in response time in comparison to the baseline is typically regarded as the maximum performance degradation to be considered acceptable.

In VSImax v4.1.x this latency threshold is fixed to 1000ms, this allows better and fairer comparisons between two different systems, especially when they have different baseline results. Ultimately, in VSImax v4.1.x, the performance of the system is not decided by the total average response time, but by the latency is has under load. For all systems, this is now 1000ms (weighted).

The threshold for the total response time is: average weighted baseline response time + 1000ms.

When the system has a weighted baseline response time average of 1500ms, the maximum average response time may not be greater than 2500ms (1500+1000). If the average baseline is 3000 the maximum average response time may not be greater than 4000ms (3000+1000).

When the threshold is not exceeded by the average VSI response time during the test, VSImax is not hit and the amount of sessions ran successfully. This approach is fundamentally different in comparison to previous VSImax methods, as it was always required to saturate the system beyond VSImax threshold.

Lastly, VSImax v4.1.x is now always reported with the average baseline VSI response time result. For **example: “The VSImax v4.1 was 125 with a baseline of 1526ms”**. This helps considerably in the comparison of systems and gives a more complete understanding of the system. The baseline performance helps to understand the best performance the system can give to an individual user. VSImax indicates what the total user capacity is for the system. These two are not automatically connected and related:

When a server with a very fast dual core CPU, running at 3.6 GHZ, is compared to a 10 core CPU, running at 2,26 GHZ, the dual core machine will give an individual user better performance than the 10 core machine. This is indicated by the baseline VSI response time. The lower this score is, the better performance an individual user can expect.

However, the server with the slower 10 core CPU will easily have a larger capacity than the faster dual core system. This is indicated by VSImax v4.1.x, and the higher VSImax is, the larger overall user capacity can be expected.

With Login VSI 4.1.x a new VSImax method is introduced: VSImax v4.1. This methodology gives much better insight in system performance and scales to extremely large systems.

Single-Server Recommended Maximum Workload

For Citrix XenApp 7.6 RDS Hosted Shared Desktop use cases, the recommended maximum workload was determined based on both Login VSI Medium workload with flash end user experience measures and blade server operating parameters.

This recommended maximum workload approach allows you to determine the server N+1 fault tolerance load the blade can successfully support in the event of a server outage for maintenance or upgrade.

Our recommendation is that the Login VSI Average Response and VSI Index Average should not exceed the Baseline plus 2000 milliseconds to insure that end user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95%.



Memory should never be oversubscribed for Desktop Virtualization workloads.

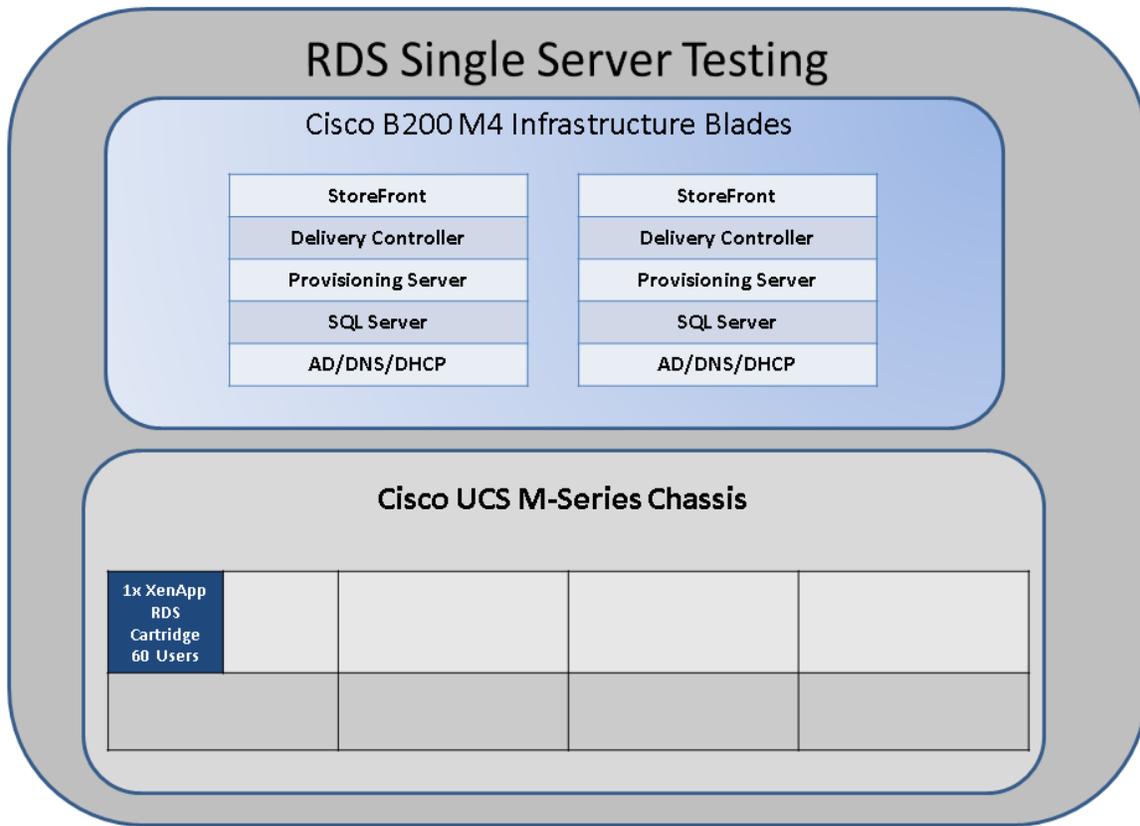


Callouts have been added throughout the data charts to indicate each phase of testing.

Test Phase	Description
Boot	Start all RDS and VDI virtual machines at the same time
Login	The Login VSI phase of test is where sessions are launched and start executing the workload over a 48 minutes duration
Steady state	The steady state phase is where all users are logged in and performing various workload tasks such as using Microsoft Office, Web browsing, PDF printing, playing videos, and compressing files
Logoff	Sessions finish executing the Login VSI workload and logoff

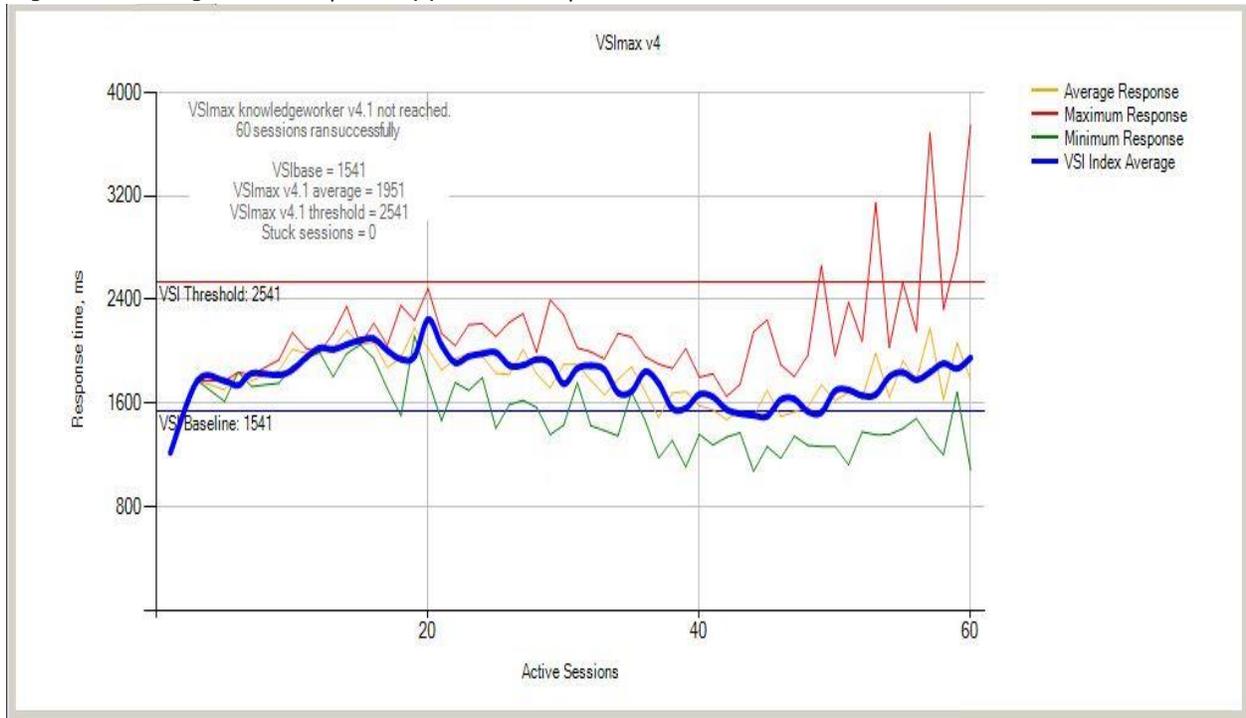
Test Results

Figure 22 Single-Server Recommended Maximum Workload for RDS with 60 Users



The recommended maximum workload for a M142-M4 cartridge server with E-1275L v3 processors and 32GB of RAM is 60 per Windows Server 2012 R2 Hosted Shared Desktops.

Figure 23 Single Server | XenApp 7.6 RDS | VSI Score



Performance data for the server running the workload follows:

Figure 24 Single Server | XenApp 7.6 RDS | Host CPU Utilization

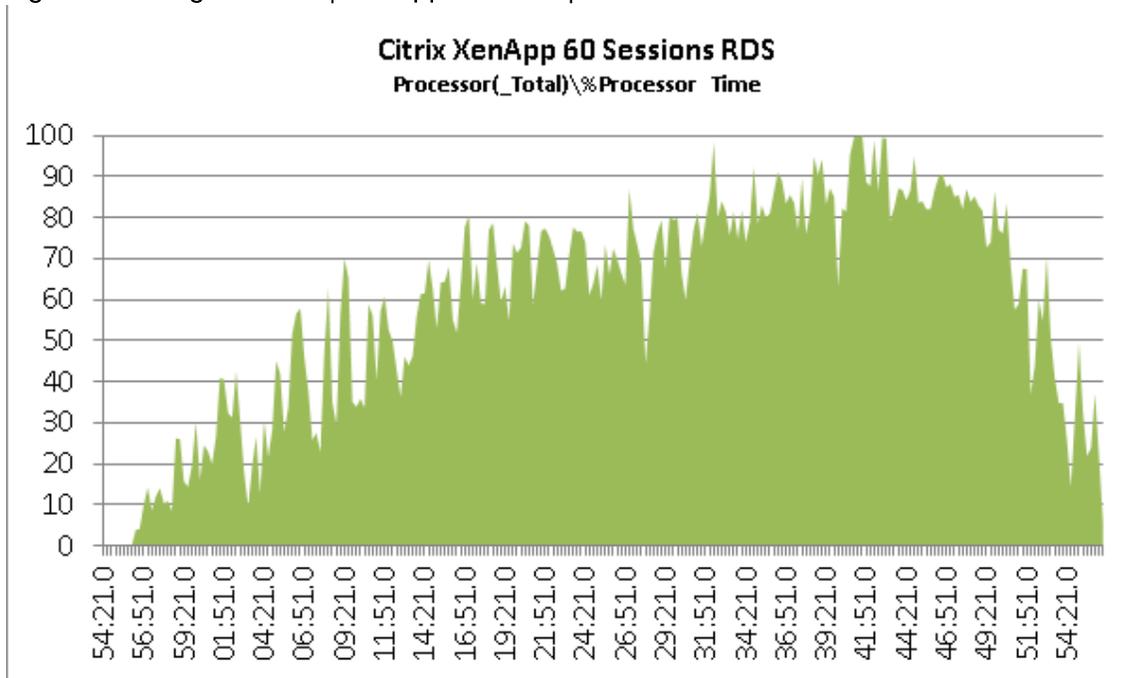


Figure 25 Single Server | XenApp 7.6 RDS | Host Memory Utilization

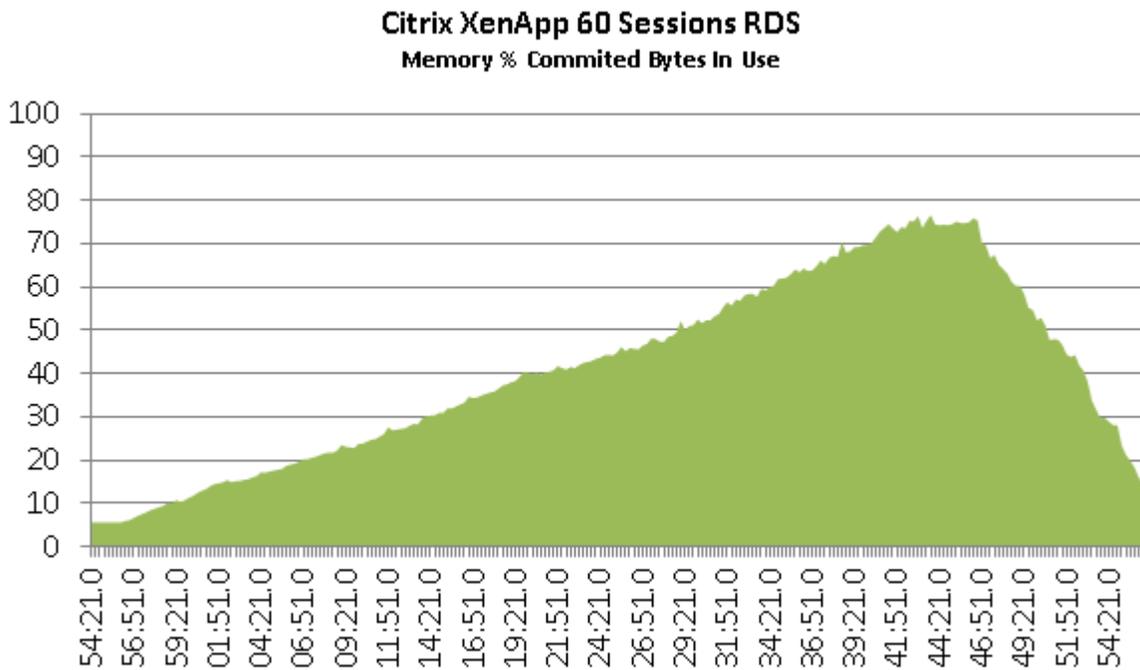
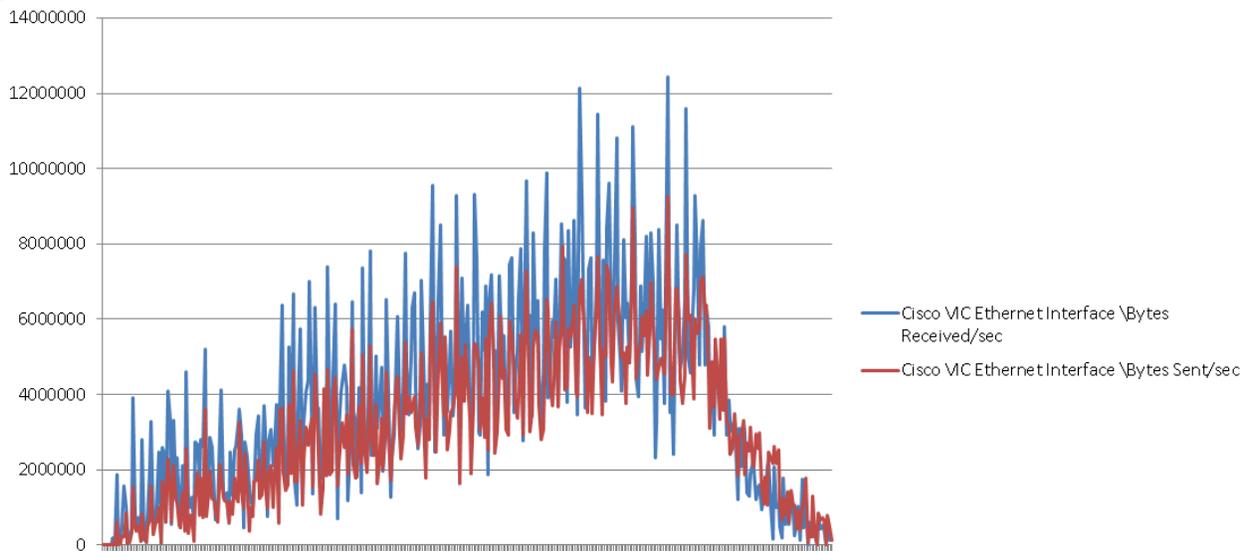


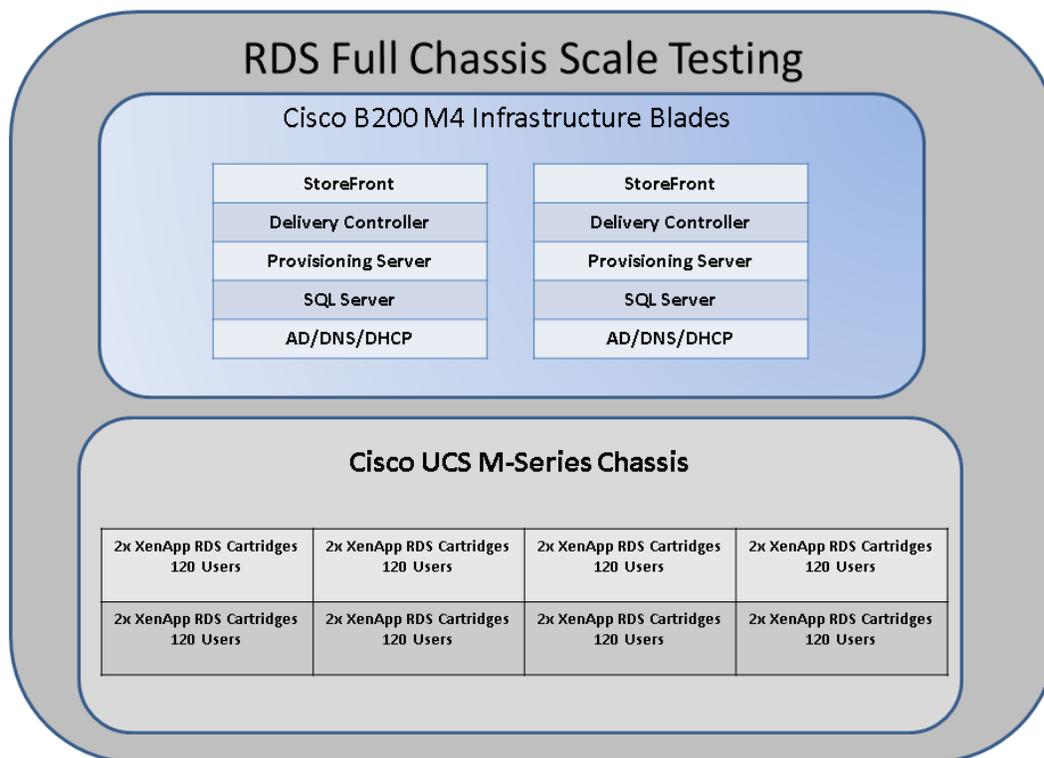
Figure 26 Single Server | XenApp 7.6 RDS | Host Network Utilization



Full Scale Testing

This section shows the key performance metrics that were captured on the Cisco UCS M-Series Modular Server Chassis. The full-scale testing comprised of testing a fully loaded M-Series Chassis with 16 compute nodes housed in 8 M142-M4 cartridges.

Figure 27 Fully Populated Chassis Workload with 960 Users



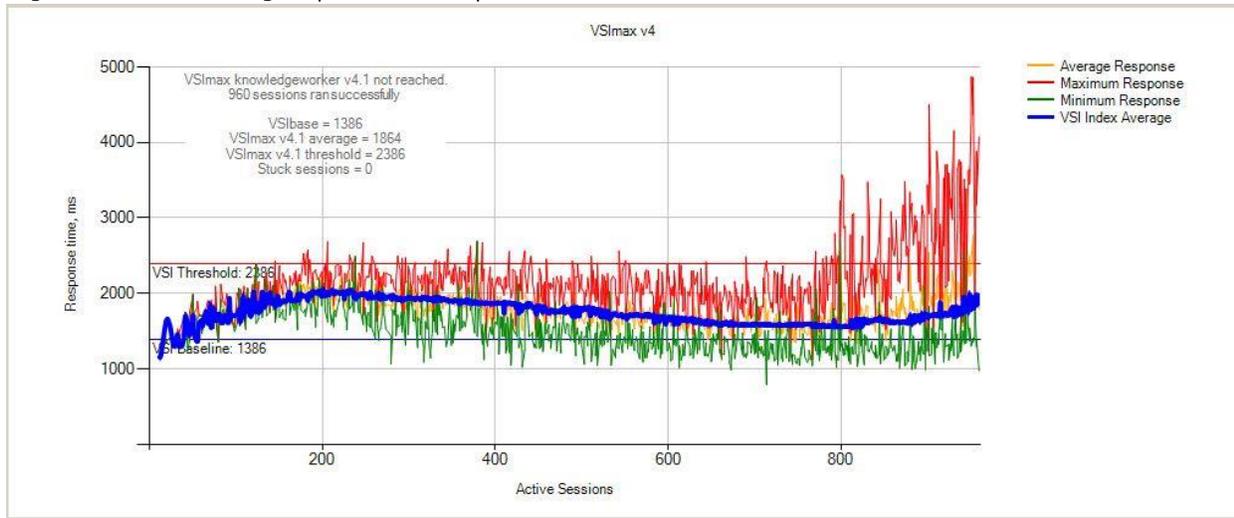
The XenApp workload for the study was 900-960 seats using 8 M-Series cartridges which accounts for N+1 high availability. To achieve the target, we launched the sessions against both use cases concurrently. We specify in the Cisco Test Protocol for XenDesktop described above that all sessions must be launched within 48 minutes (through VSI Benchmark Mode) and that all launched sessions must become active within two minutes subsequent to the last logged in session.

The configured system efficiently and effectively delivered the following results.

The storage test setup for all tests included the following:

- Four 400GB SSDs for the Local Storage Pool
- Cisco UCS Manager Firmware 2.5(2a)

Figure 28 8 Cartridges | 960 Users | VSI Score



Scalability Considerations and Guidelines

There are many factors to consider when you begin to scale beyond 500 Users; a single chassis, HSD workload configuration, which this reference architecture has successfully tested. In this section we give guidance to scale beyond the 500 user system.

Cisco UCS System Scalability

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

Cisco UCS 2.5(2a) management software supports up to 1 Cisco UCS M-Series chassis within a single Cisco UCS domain on our Cisco UCS Fabric Interconnect 6248UP models. Our single UCS domain can grow to 8 blades with 7 C-Series servers for an enterprise edge deployment.

With Cisco UCS 2.5(2a) management software, released in July 2015, each Cisco UCS Management domain is extensively manageable by Cisco UCS Central, our 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 percent of the time.

To accommodate the Cisco Nexus 9000 upstream connectivity in the way we describe in the network configuration section, we need two Ethernet uplinks to be configured on the Cisco UCS Fabric Interconnect 6248UP.

Scalability of Citrix XenDesktop 7.6 Configuration

XenDesktop environments can scale to large numbers. When implementing Citrix XenDesktop, consider the following in scaling the number of hosted shared and hosted virtual desktops:

- Types of storage in your environment

- Types of desktops that will be deployed
- Data protection requirements
- For Citrix Provisioning Server pooled desktops, the write cache sizing and placement

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

When designing and deploying this CVD environment, best practices were followed including the following:

- Citrix recommends using N+1 schema for virtualization host servers to accommodate resiliency. In all Reference Architectures (such as this CVD), this recommendation is applied to all host servers.
- All Provisioning Server Network Adapters are configured to have a static IP and management.

Conclusion

With this reference architecture, we are able to show configurations to ensure efficient use of the Cisco UCS M-Series technology with Citrix XenApp 7.6 and its complimentary products. Our testing shows uniform resource usage across all cartridges in the system and linear scalability of the system.

This solution was architected to highlight features that will enable an enterprise class XenApp RDS solution for end user sessions. In this solution we highlighted the ability to provide desktops utilizing local hard disk storage using the shared virtual storage controller in the M-Series chassis and prove that it was able to handle the workload of Citrix Provisioning Server write cache disks. We also highlighted the Cisco System Link technology and the sNIC technology that makes the disaggregation of the server components possible. It was proven that the workload properly scaled across cartridge servers and each cartridge was able to handle an equal amount of the load.

With the landscape of the virtual desktop constantly changing, the new Cisco UCS M-Series Modular servers running Citrix XenApp 7.6, complimented by Citrix Provisioning Server 7.6, offers a low cost, small foot print solution with high density XenApp workloads. This solution has proven that the M-Series servers can run 60 user sessions per server, 120 sessions per cartridge which works out to 960 user sessions per 2RU chassis. The use of the Intel E3 family of processors greatly reduces the cost from the traditional Intel E5 family of processors used in the B-Series or C-Series XenApp solutions.

About the Authors

Jeff Nichols, Technical Marketing Engineer, VDI Performance and Solutions Team, Cisco Systems, Inc.

Jeff Nichols is a Cisco Unified Computing System architect, focusing on Virtual Desktop and Application solutions with extensive experience with VMware ESX/ESXi, XenDesktop, XenApp and Microsoft Remote Desktop Services. He has expert product knowledge in application, desktop and server virtualization across all three major hypervisor platforms and supporting infrastructures including but not limited to Windows Active Directory and Group Policies, User Profiles, DNS, DHCP and major storage platforms

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

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

Acknowledgements

- Steve McQueery, Technical Marketing Engineer, CCIE #6108, Cisco Systems, Inc.

Appendix A – Scripts for Configuring Local Write Cache

In order to automatically format and mount the local LUNs to be used for Citrix PVS write cache, the following script was added to a startup GPO for the XenApp servers.

Format Local Storage Script

```
'-----  
  
Const wbemFlagReturnImmediately = &h10  
Const wbemFlagForwardOnly = &h20  
Const DiskLetter = " D"  
Const DiskPartScriptPath = " C:\Windows\Temp\DISKPART.TXT"  
Const DiskIndex = " 0"  
  
Main()  
  
Sub Main()  
if VolumeCacheExist() then  
    WriteLog " AUTOFORMATPVS: Cache Volume Already Formatted"  
Else  
    GenerateDiskPartScript DiskPartScriptPath , DiskIndex , DiskLetter  
    if RunDiskpartScript(DiskPartScriptPath) then  
        RunFormat DiskLetter  
    End If  
End If  
End Sub
```

```
Function VolumeCacheExist()
On Error Resume Next
VolumeCacheExist = False
Set objWMIService = GetObject("winmgmts:\\.\root\CIMV2")
Set collItems = objWMIService.ExecQuery("SELECT * FROM Win32_LogicalDisk WHERE VolumeName = 'Cache'", "WQL", _
    wbemFlagReturnImmediately + wbemFlagForwardOnly)
For Each objItem In collItems
    VolumeCacheExist = True
Next
End Function

Sub GenerateDiskPartScript( ScriptPath , DiskIndex , Letter)
on error resume next
err.clear
Set ObjFso = CreateObject("Scripting.FileSystemObject")
Set DPScript = ObjFso.CreateTextFile(ScriptPath, True)
DPScript.WriteLine "SELECT DISK " & DiskIndex
DPScript.WriteLine "CLEAN"
DPScript.WriteLine "CREATE PARTITION PRIMARY"
DPScript.WriteLine "ASSIGN LETTER=" & Letter
DPScript.WriteLine "EXIT"
DPScript.close
if err then WriteErrorLog "AUTOFORMATPVS: Impossible to create the DISKPART script: " &
err.description
End Sub
```

```
Function RunDiskpartScript( ScriptPath )  
on error resume next  
Set ObjShell = CreateObject(" Wscript.Shell" )  
if ObjShell.run(" DISKPART.EXE /s "" & ScriptPath & """" , 0 , True) = 0 Then  
    RunDiskpartScript = True  
    Writelog " AUTOFORMATPVS: Cache partition creation : SUCCESS"  
Else  
    RunDiskpartScript = False  
    WriteErrorlog " AUTOFORMATPVS: Cache partition creation : ERROR"  
End If  
End Function  
  
Function RunFormat( Letter )  
on error resume next  
Set ObjShell = CreateObject(" Wscript.Shell" )  
if ObjShell.run(" FORMAT " & Letter & " : /FS:NTFS /V:Cache /Q /Y" , 0 , True) = 0 Then  
    RunFormat = True  
    Writelog " AUTOFORMATPVS: Cache Partition Format : SUCCESS"  
Else  
    RunFormat = False  
    WriteErrorlog " AUTOFORMATPVS: Cache Partition Format : ERROR"  
End If  
End Function  
  
Sub WriteLog( msg )  
on error resume next
```

```

Set oShell = wscript.CreateObject(" Wscript.Shell" )

oCommand = " eventcreate /T INFORMATION /SO " " FormatStartupScript" " /ID 1 /D "" & msg & "" "
/L Application" 'Create the log entry using eventcreate

oShell.Run oCommand 'Run the command

End Sub

Sub WriteErrorLog( msg )

on error resume next

Set oShell = wscript.CreateObject(" Wscript.Shell" )

oCommand = " eventcreate /T ERROR /SO " " FormatStartupScript" " /ID 911 /D "" & msg & "" " /L
Application" 'Create the log entry using eventcreate

oShell.Run oCommand 'Run the command

End Sub

```

Registry Keys for Automated Write Cache Deployment

The following keys were injected into the master image to ensure that all cartridges could format and connect to the local LUNs created during the Service Profile creation.

Windows Registry Editor Version 5.00

```

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]

"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000000"

```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000100#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000100"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000100#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000200#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000200"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000200#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000300#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000300"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000300#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000400#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000400"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000400#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000500#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000500"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000500#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000600#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000600"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000600#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000700#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000700"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000700#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000800#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000800"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000800#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000900#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000900"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000900#\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000a00#\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000a00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000a00#\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000b00#\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000b00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000b00#\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000c00#\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000c00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000c00#\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000d00#\#]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000d00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000d00#\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000e00#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000e00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000e00#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000f00#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&000f00"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000f00#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&001000"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001100#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
```

```
"DeviceInstance"="SCSI\\Disk&Ven_Cisco&Prod_UCSME-MRAID12G\\9&26d55d42&0&001100"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001100#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#]
```

```
{3375baf4-9e15-4b30-b765-67acb10d607b}
{35fa2e29-ea23-4236-96ae-3a6ebacba440}
▶ {378de44c-56ef-11d1-bc8c-00a0c91405dd}
▶ {3abff62d-71c4-462a-8a92-1e6861e6af27}
▶ {3ff2c92b-6598-4e60-8e1c-0ccf4927e319}
▶ {4116f60b-25b3-4662-b732-99a6111edc0b}
▶ {4747b320-62ce-11cf-a5d6-28db04c10000}
▶ {4afa3d51-74a7-11d0-be5e-00a0c9062857}
▶ {4afa3d53-74a7-11d0-be5e-00a0c9062857}
▶ {4d1e55b2-f16f-11cf-88cb-001111000030}
▶ {4d36e978-e325-11ce-bfc1-08002be10318}
▶ {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000100#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000200#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000300#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000400#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000500#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000600#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000700#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000800#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000900#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000a00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000b00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000c00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000d00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000e00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&000f00#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001000#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Cisco&Prod_UCSME-MRAID12G#9&26d55d42&0&001100#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#SCSI#Disk&Ven_Citrix&Prod_Virtual_Disk#1&2afd7d61&0&000080#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ #
▶ ##?#USBSTOR#Disk&Ven_Cisco&Prod_CIMC-Mapped_vHDD&Rev_1.22#20111102-00000002&4#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
▶ ##?#USBSTOR#Disk&Ven_Cisco&Prod_vKVM-Mapped_vHDD&Rev_1.22#20111102-00000002&1#(53f56307-b6bf-11d0-94f2-00a0c91efb8b)
```

Appendix B – Complete Performance Charts for all Cartridges

The following are the complete performance charts for all 16 individual servers in the solution. Our findings were consistent across all cartridges with efficient load balancing from XenDesktop 7.6, all cartridges were nearly identical during our scale workloads for the full chassis.

Figure 29 Server 1

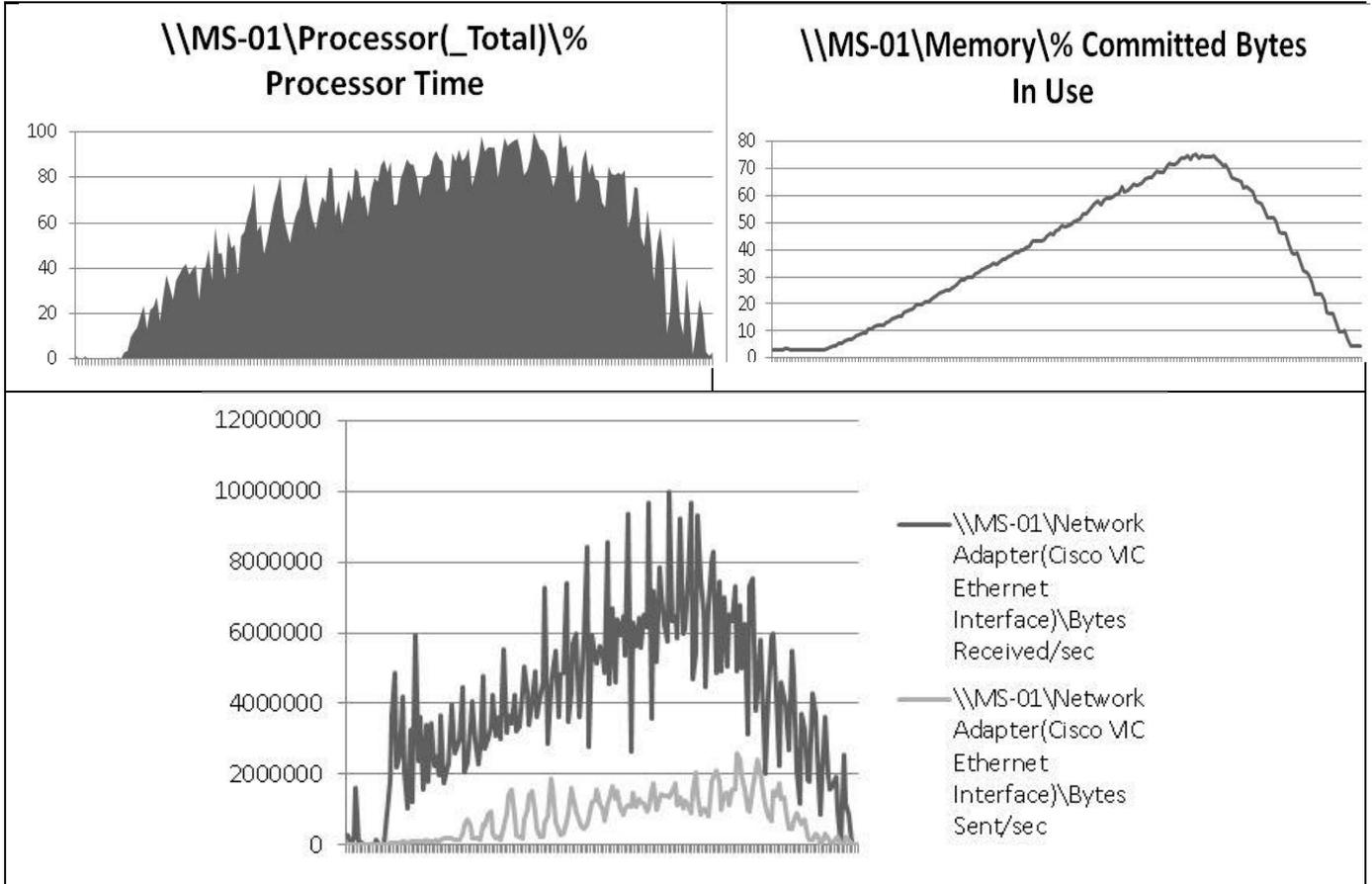
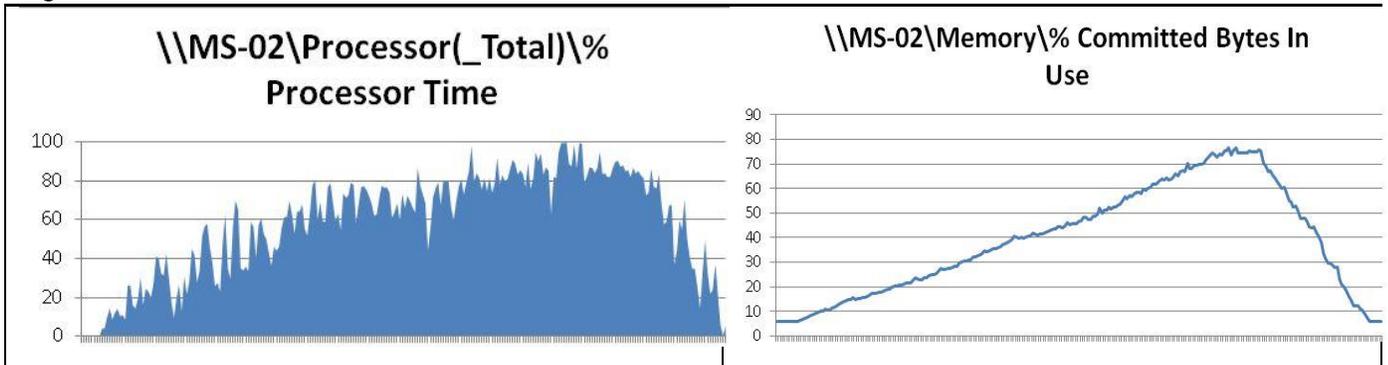


Figure 30 Server 2



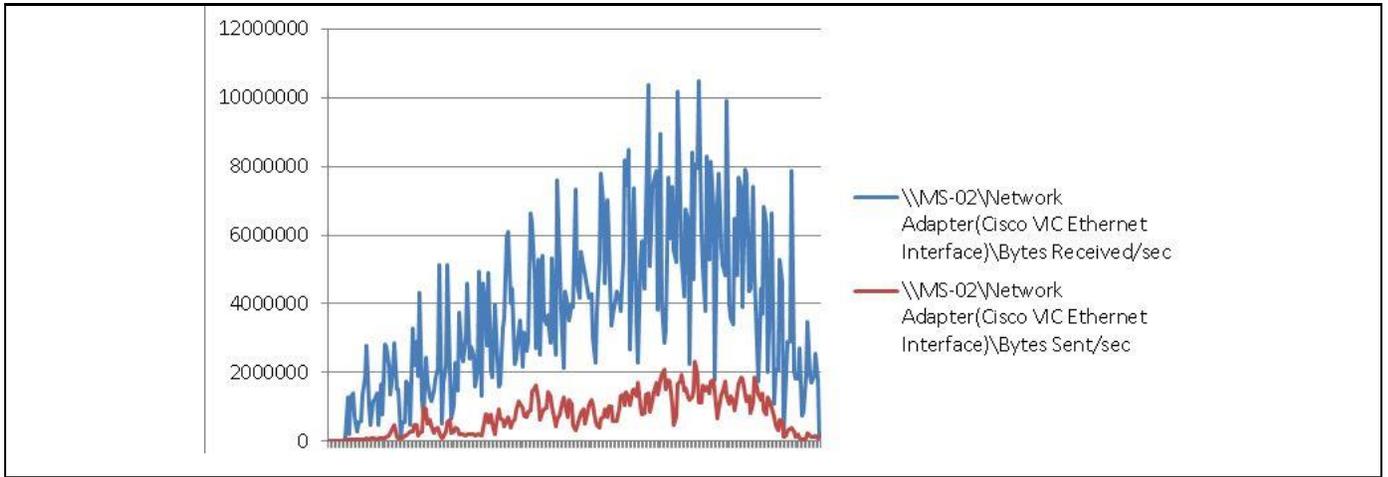


Figure 31 Server 3

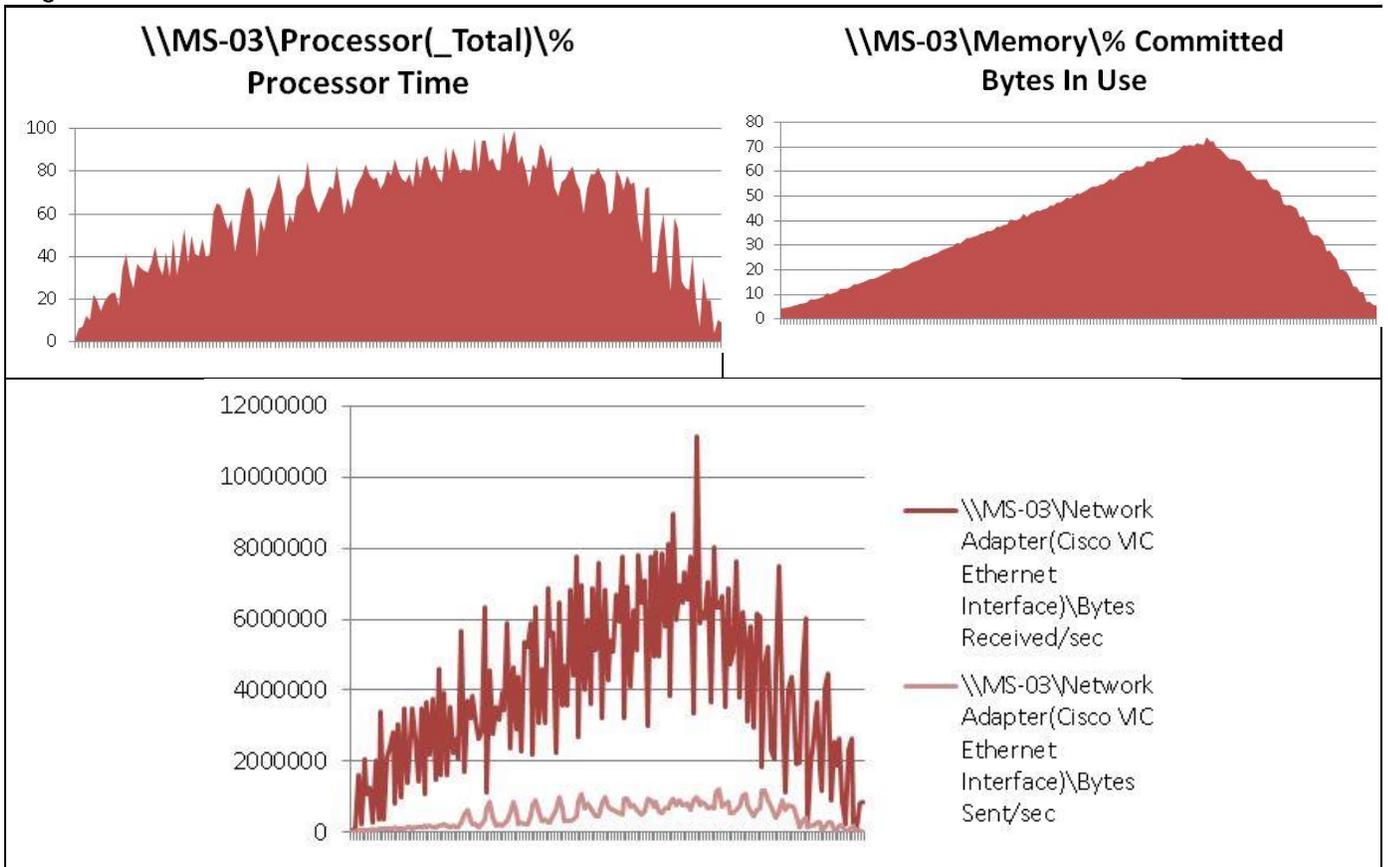


Figure 32 Server 4

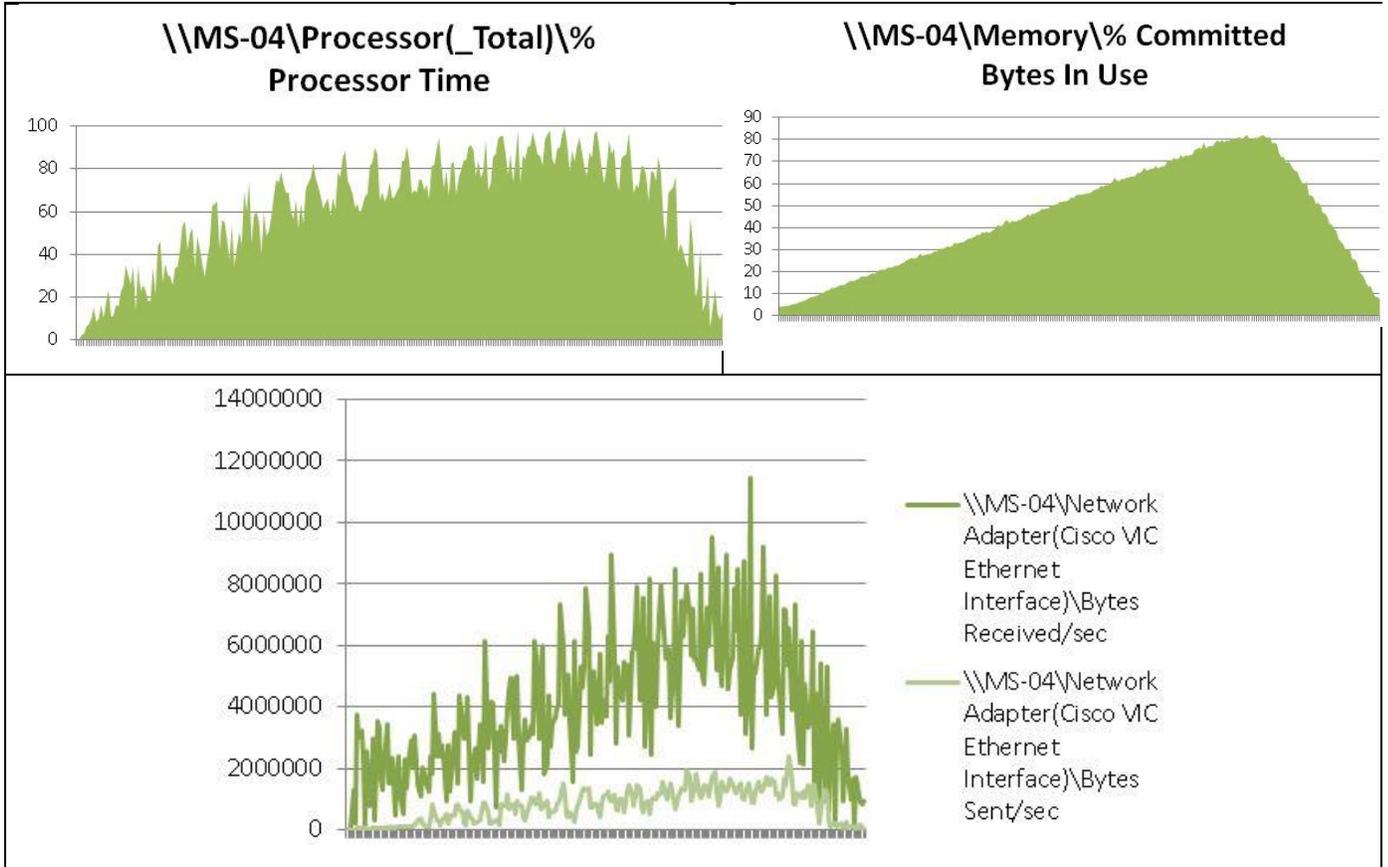


Figure 33 Server 5

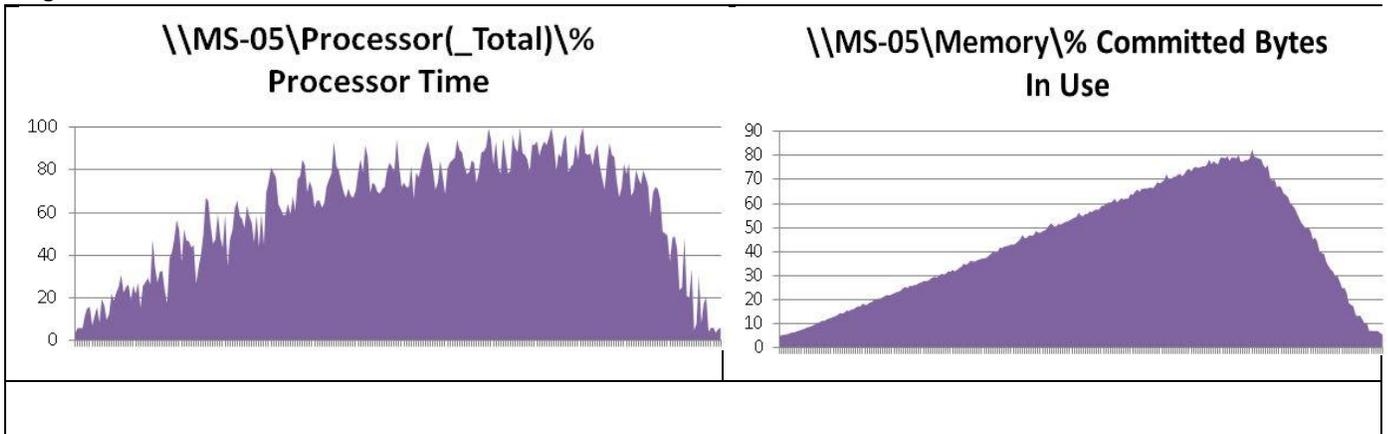


Figure 34 Server 6

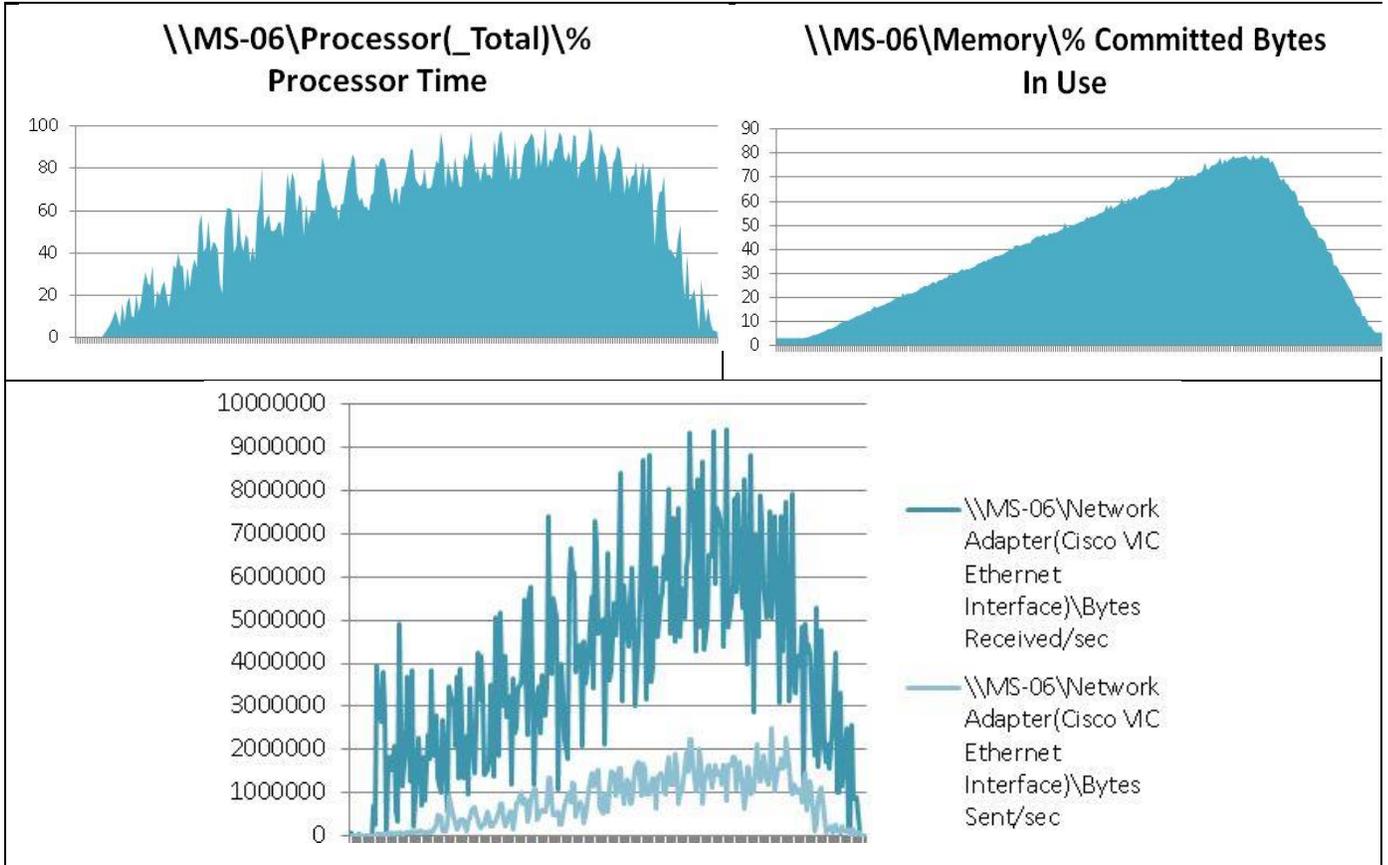
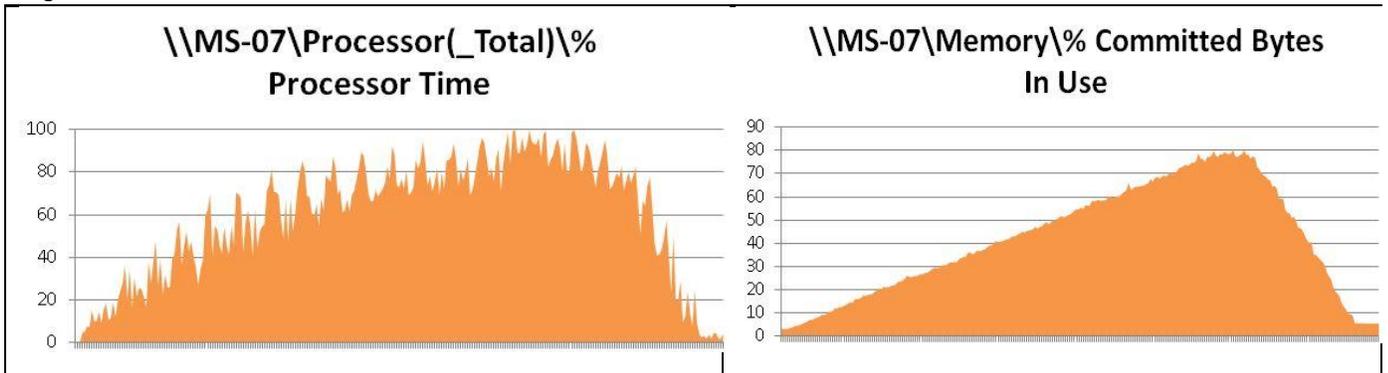


Figure 35 Server 7



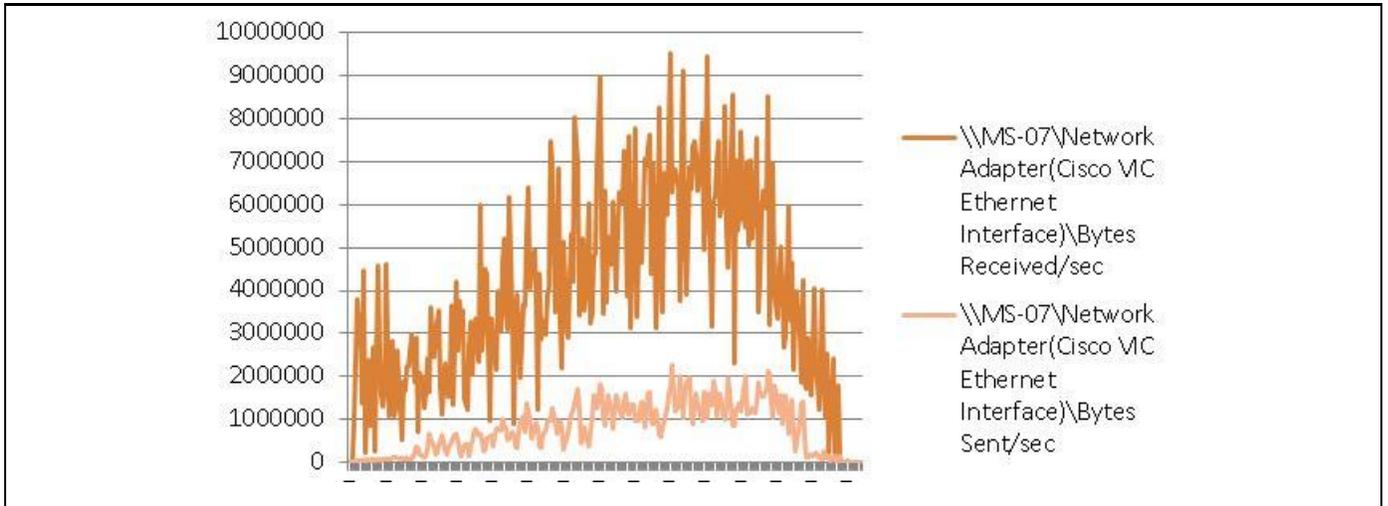


Figure 36 Server 8

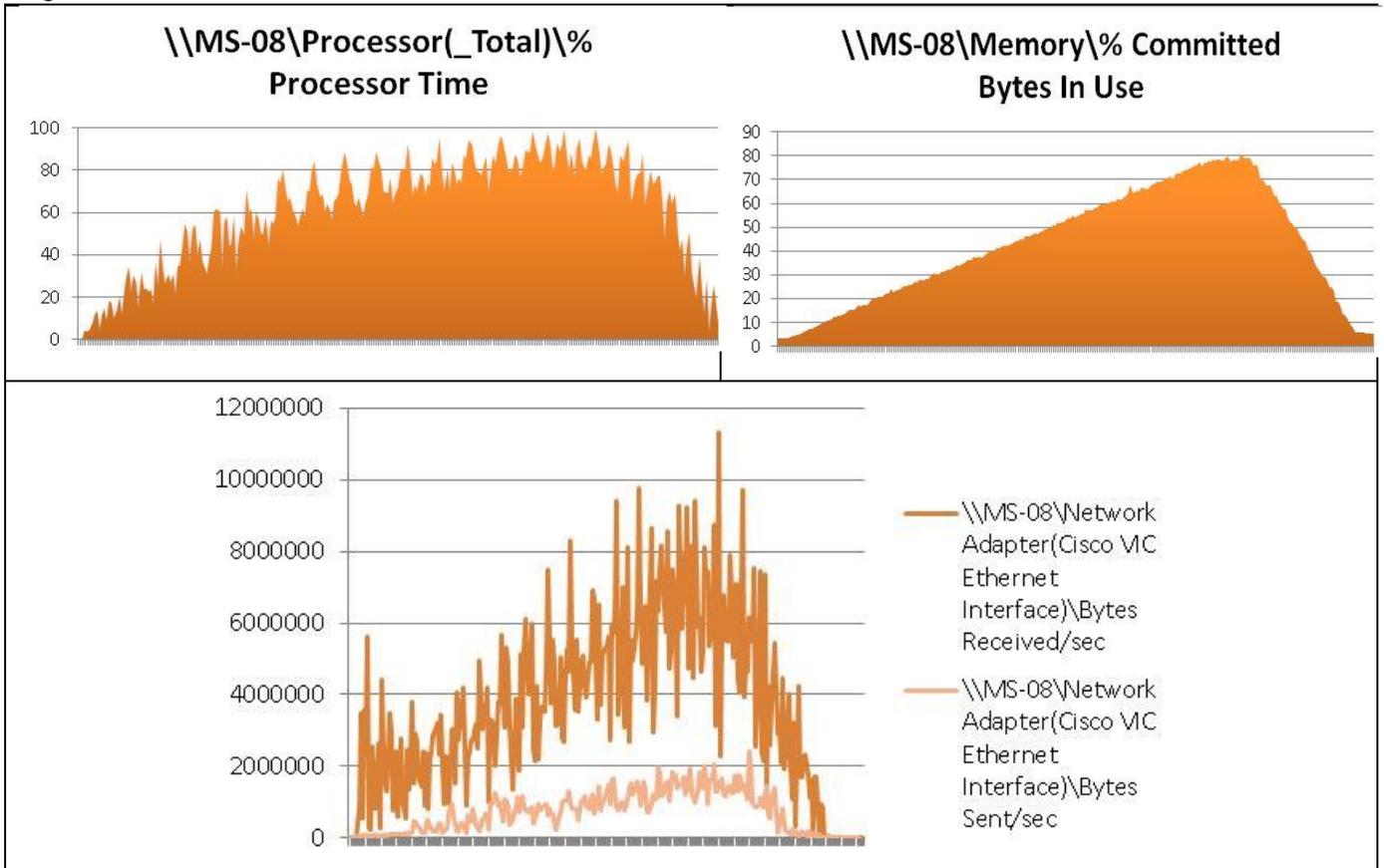


Figure 37 Server 9

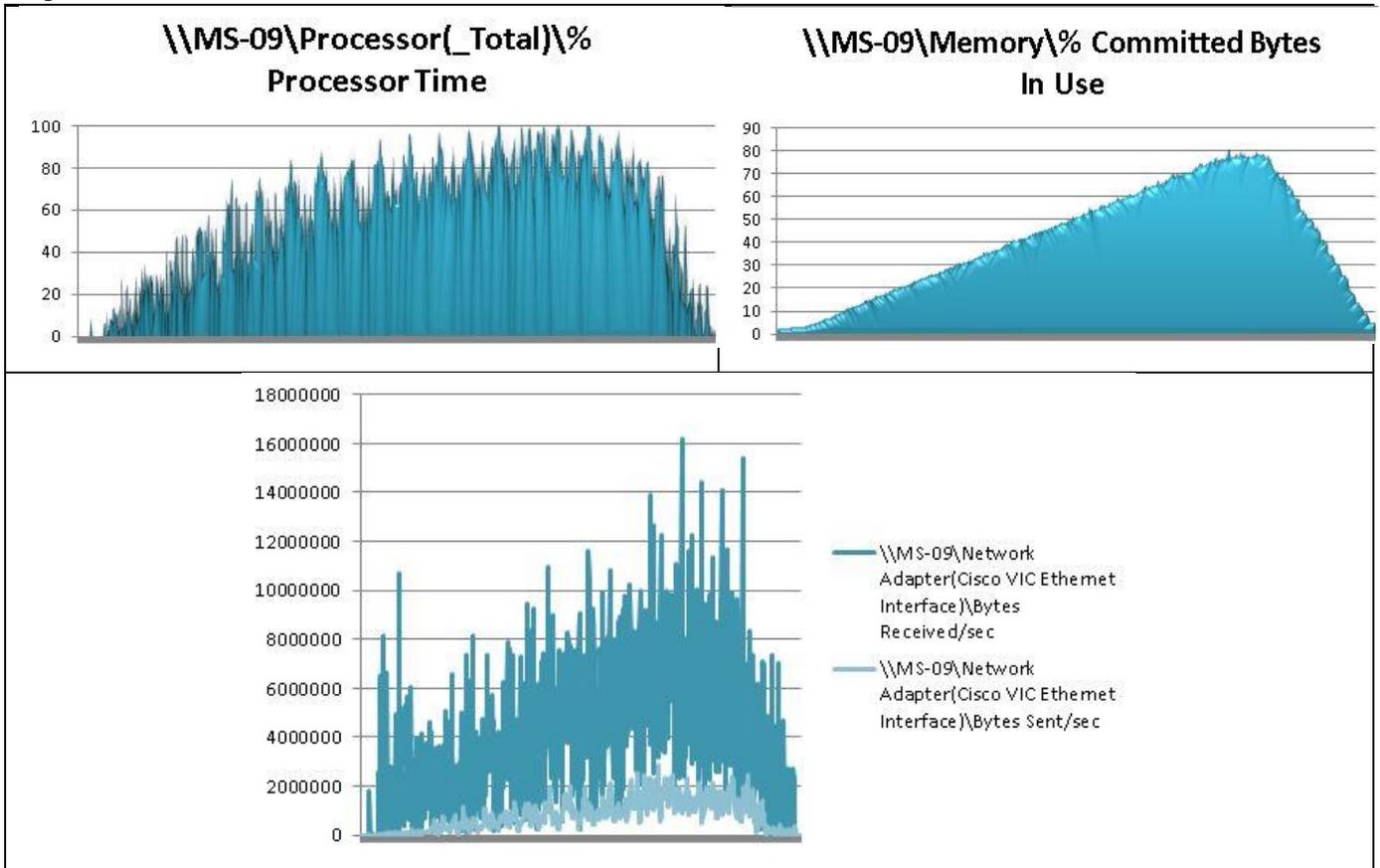
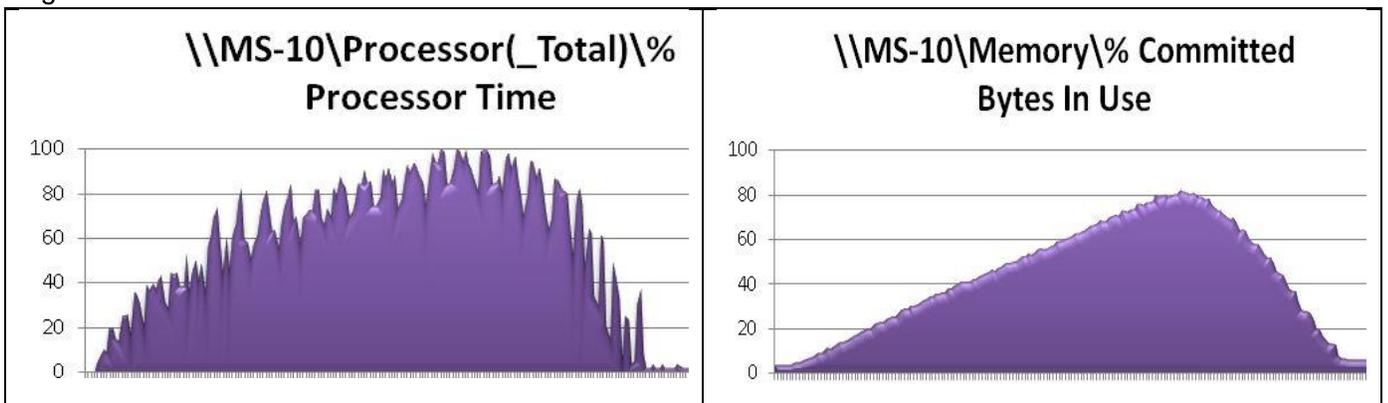


Figure 38 Server 10



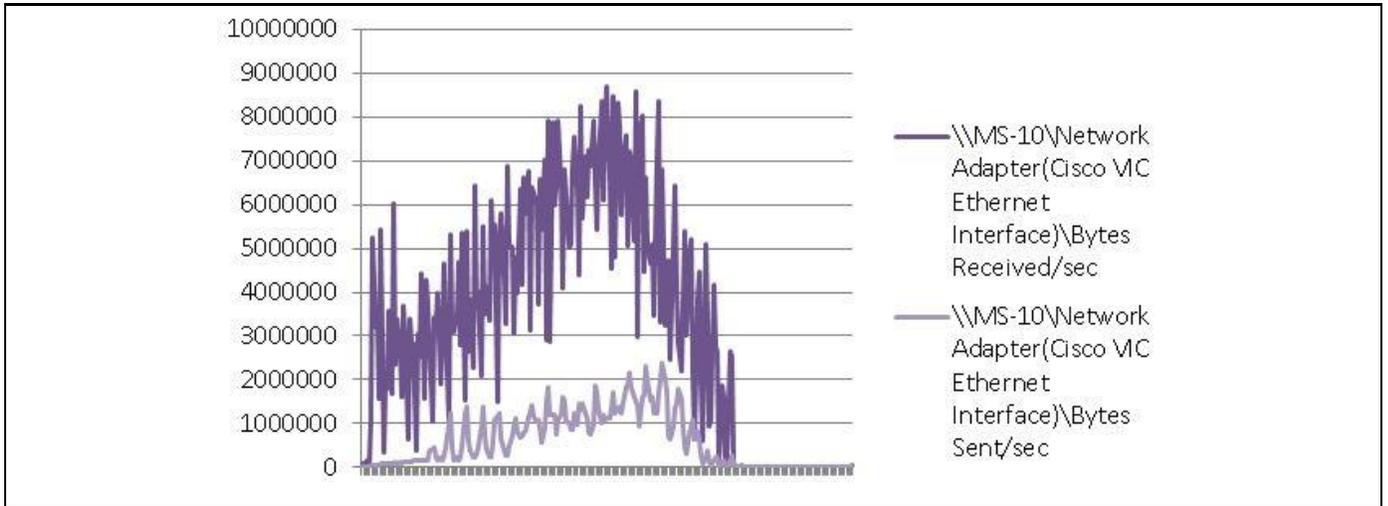


Figure 39 Server 11

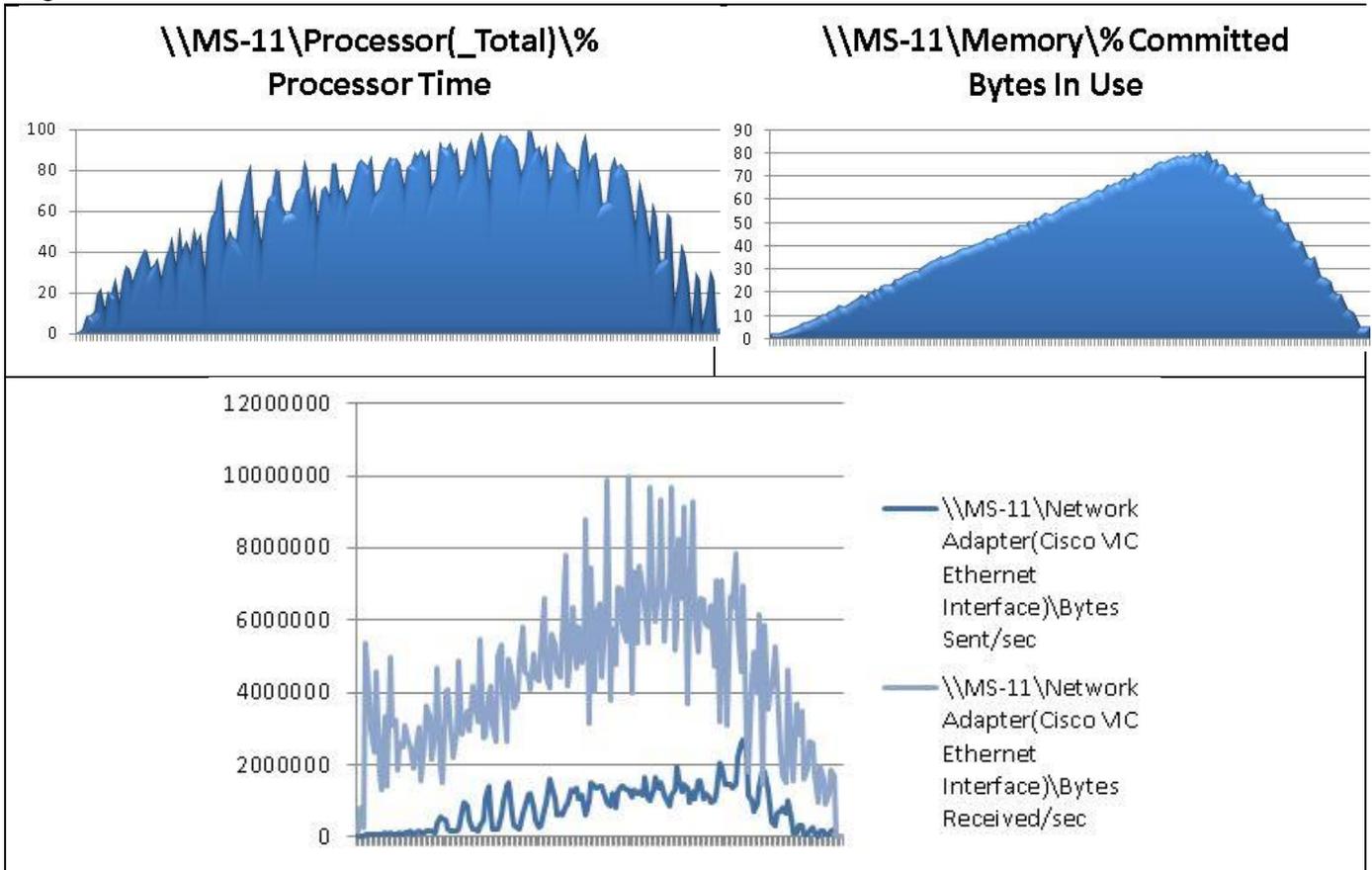


Figure 40 Server 12

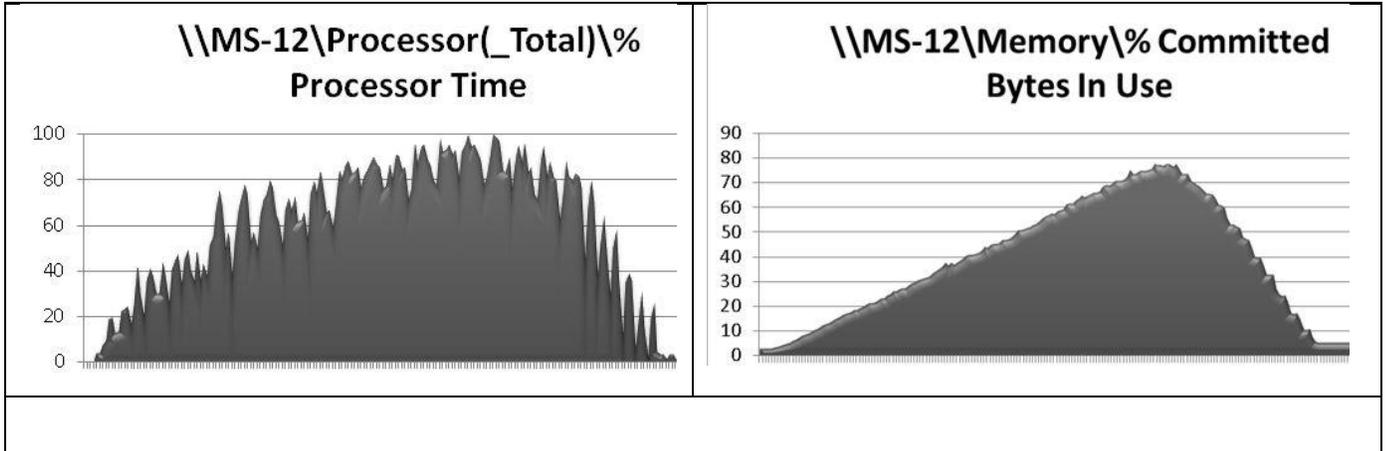


Figure 41 Server 13

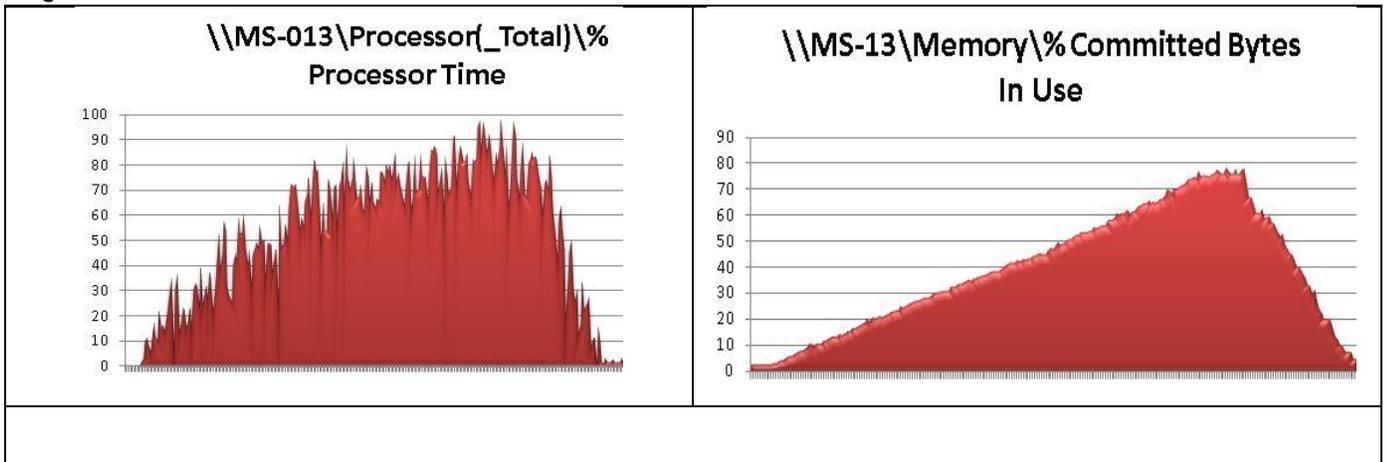
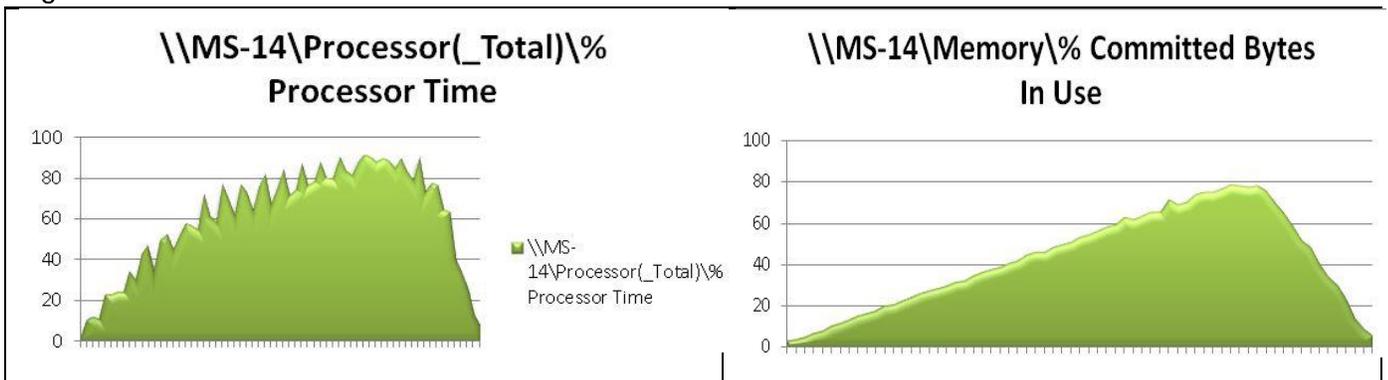


Figure 42 Server 14



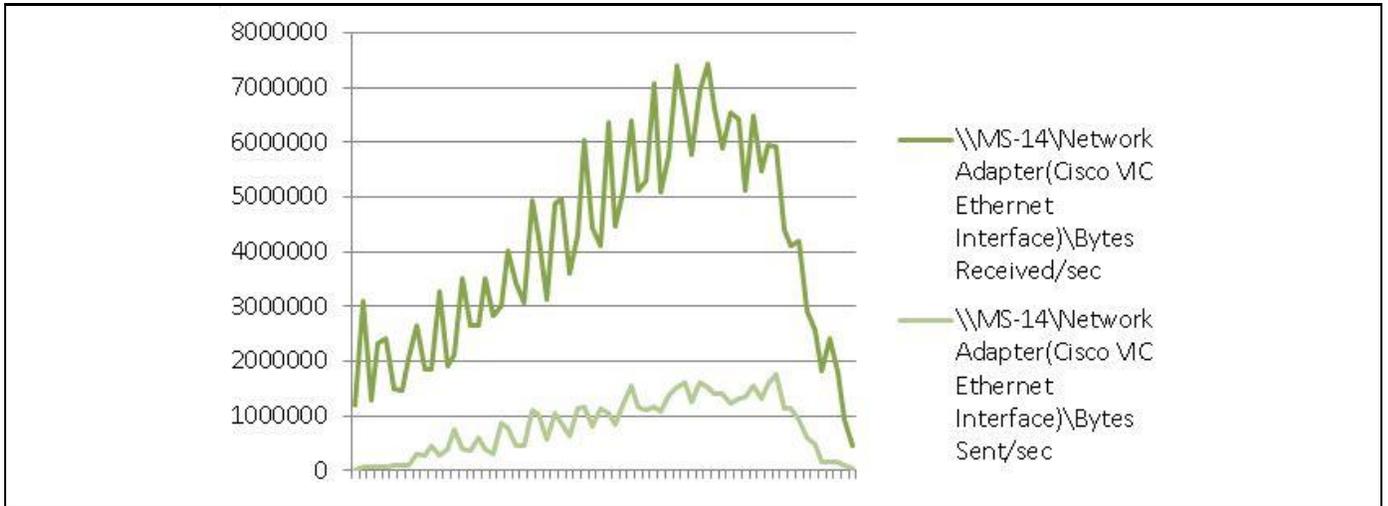


Figure 43 Server 15

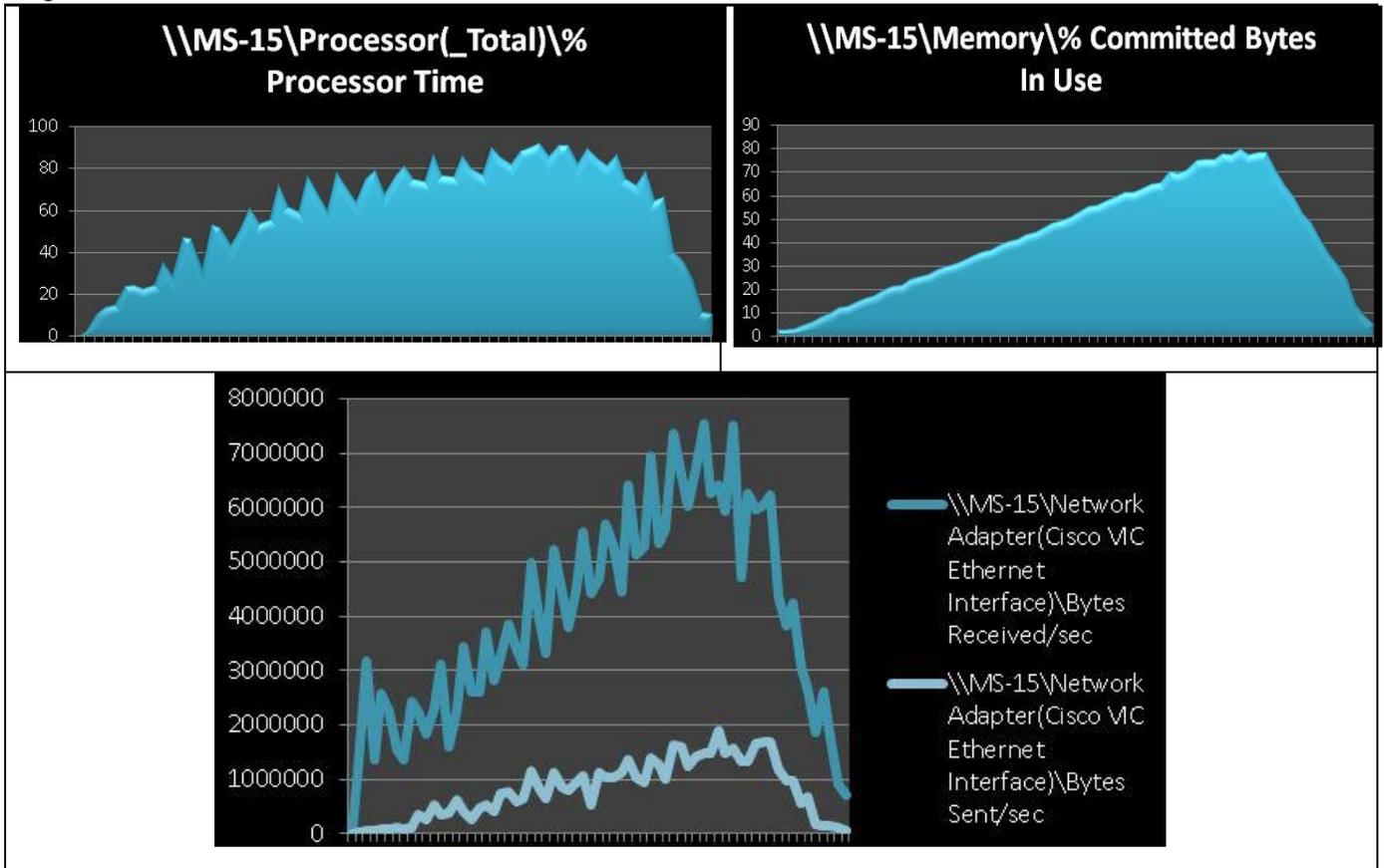


Figure 44 Server 16

