VDI—Cisco UCS with VMware Hypervisors and Citrix XenDesktop Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide 1
- Cisco SBA Solutions 1
- Route to Success 1
- About This Guide 1

Introduction 2
- Related Reading 2
- Business Overview 3
- Technology Overview 3

Deployment Details 9
- Preparing the Data Center for Citrix Installation 9
- Installing and Configuring Citrix XenDesktop 13
- Deploying Citrix Provisioning Services (PVS) 24
- Installing and Configuring Citrix XenApp 66
- Installing and Testing Citrix Receiver Access 89

Appendix A: Product List 98

Appendix B: Data Center Network Infrastructure Configuration 101
- Cisco Nexus 5596UPa 101
- Cisco Nexus 5596UPb 102
- Cisco ASA 5585—Primary 102
- Cisco ASA 5585—Secondary 103

What's In This SBA Guide

Cisco SBA Solutions

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

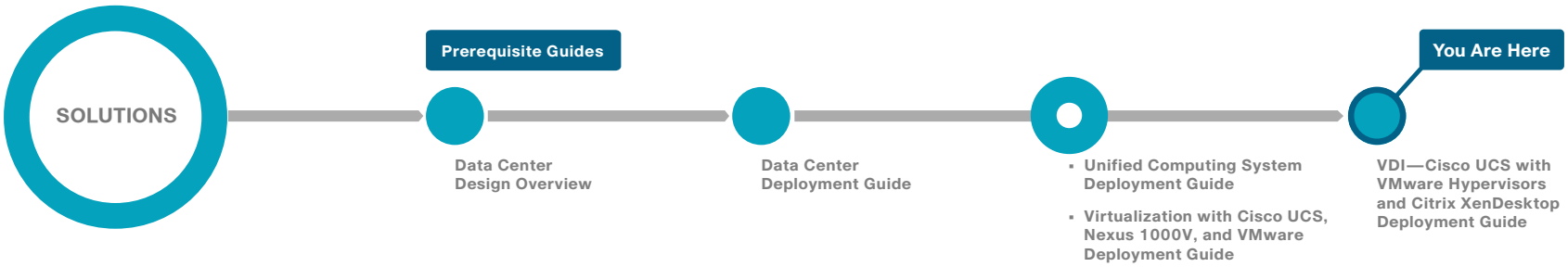
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

Desktop virtualization separates a personal desktop environment, including the operating system, desktop applications, and personal files and settings, from the physical device on which the desktop environment runs. In a virtual desktop infrastructure (VDI) deployment, the operating system typically runs in a virtual machine on a server hosted in a data center, known as a *hosted virtual desktop*. A *hosted shared desktop* is a complementary virtualization technology that allows you to deliver a session-based virtual desktop from a single server operating system to multiple end-point devices. This technology is also known as *Remote Desktop Session Host (RDSH)* or *Terminal Services*. Virtualization software delivers an appropriate set of work resources and enables users access to their workspaces from any device.

The *VDI—Cisco UCS with VMware Hypervisors and Citrix XenDesktop Deployment Guide* describes how to use Citrix XenDesktop, Citrix XenApp, VMware ESXi, and Cisco Unified Computing System in order to deploy and scale desktop virtualization for the enterprise. This guide builds upon the Cisco Unified Computing System (UCS) B-Series and C-Series server deployments detailed in the *Cisco SBA—Data Center Unified Computing System Deployment Guide*, in which you configure Cisco UCS, VMware ESXi, and storage area networking (SAN). Additionally, this guide builds upon the data center foundation from the *Cisco SBA—Data Center Deployment Guide*.

Related Reading

The *VDI—Cisco UCS with VMware Hypervisors and Citrix XenDesktop Deployment Guide* depends on the foundation and customization from the guides previously mentioned. Organizations wishing to further customize or scale their deployments by using additional servers, blade servers, Cisco UCS Manager, RAID-based shared storage, a different hypervisor, or networking components may benefit from referring to other guides in the Cisco Smart Business Architecture (SBA) series. The following guides may be required for your particular deployment:

- The *Cisco SBA—Data Center Unified Computing System Deployment Guide* provides the processes and procedures necessary to deploy a Cisco Unified Computing System using both the Cisco B-Series blade server system and Cisco C-Series rack-mount servers, to a point where they are ready to deploy an operating system or hypervisor software.
- The *Cisco SBA—Data Center Virtualization with Cisco UCS, Nexus 1000V, and VMware Deployment Guide* describes how to deploy a VMware hypervisor on the Cisco Unified Computing System, including both the Cisco B-Series blade servers and Cisco C-Series rack-mount servers. It also describes how to install and deploy a Cisco Nexus 1000V Series switch as a full-featured virtual switch for the VMware servers.
- The *Cisco SBA—Data Center Design Overview* provides an overview of the data center architecture. This guide discusses how the Cisco SBA data center architecture is built in layers—the foundation of Ethernet and storage networks and computing resources; the data center services of security, application resilience, and virtual switching; and the user-services and applications layer.
- The *Cisco SBA—Data Center Deployment Guide* focuses on the processes and procedures necessary to deploy your data center foundation, Ethernet, and storage transport. The data center foundation supports the flexibility and scalability of the Cisco Unified Computing System and provides details for the integration of the server and the network for Cisco and non-Cisco servers. The foundation design includes data center security services such as firewall and intrusion prevention systems, and it includes application resiliency services such as advanced server load-balancing techniques. This guide also discusses the considerations and options for data center power and cooling. The supplemental *Data Center Configuration Files Guide* provides snapshots of the actual platform configurations used in the design.
- The supplemental *NetApp Storage Deployment Guide* provides a concise yet detailed process of deploying a NetApp storage array in your data center in order to complete the design.
- The supplemental *Application Optimization Deployment Guide* shows how to boost network performance for sites connected over a WAN, and it describes how to use Cisco Wide Area Application Services (Cisco WAAS) in order to view the accelerated performance. Citrix performance is enhanced with Cisco WAAS.

There are also a number of related Cisco SBA Bring Your Own Device (BYOD) guides, which are helpful for deploying the client connectivity to the network in order to provide VDI access. They include the following:

- *Cisco SBA Solutions—BYOD—Design Overview*
- *Cisco SBA Solutions—BYOD—Virtual Desktop Access Deployment Guide*
- *Cisco SBA Solutions—BYOD—Advanced Guest Wireless Access Deployment Guide*
- *Cisco SBA Solutions—BYOD—Identity and Authentication Deployment Guide*
- *Cisco SBA Solutions—BYOD—Internal Corporate Access Deployment Guide*
- *Cisco SBA Solutions—BYOD—Remote Mobile Access Deployment Guide*

Business Overview

Smaller organizations face many of the same IT challenges as larger organizations when trying to accommodate increasing demand for new IT capabilities and services. They often place even greater emphasis on cost savings and on protecting business-critical systems and data because they have smaller IT staffs and budgets, and they need to leverage IT assets to their fullest extent. Organizations require cost-effective solutions that can better utilize their existing server, storage, and network resources.

To improve availability and ensure business continuity, organizations need efficient ways to maintain production systems while minimizing downtime. Virtualization technology simplifies IT so that organizations can more effectively use their storage, network, and computing resources to control costs and respond faster to the ever-changing landscape. The virtual approach to IT management creates virtual services out of the physical IT infrastructure, enabling administrators to allocate these resources efficiently.

With virtualization, hardware management is decoupled from software management, and hardware equipment can be treated as a single pool of processing, storage, and networking resources that can be reallocated as needed to various software applications. In a virtual infrastructure environment, users access desktop and application resources as if they were dedicated to them—while administrators gain the ability to efficiently manage and optimize resources in order to serve the constantly changing needs of the organization.

An organization also achieves a strategic benefit when centralizing the compute and storage resources by extending the virtualization concept to desktops and applications. Because the devices used for accessing the data can be configured to view important data without actually downloading it, a virtualized desktop environment can support regulatory compliance initiatives. When the data does not leave the confines of the data center, controls and tracking for security and data retention are easier to implement and audit. Though protecting transaction, customer, and business information is beneficial to all organizations, the increased control of data is particularly important for healthcare and financial organizations.

Technology Overview

Virtual Desktop Infrastructure

VDI delivers a desktop and workspace virtualization solution that can dramatically improve business operations and data security while increasing end-user productivity, mobility, and flexibility. The premise of VDI is to decouple the location of the execution of the application from where the client resides, allowing new client compute paradigms. These tools help organizations rapidly respond to events such as mergers and acquisitions, the opening of new branch offices, and maintaining continuity across business interruptions. By keeping the work data centrally located and preventing it from leaving the organization's facilities via a device with storage, such as a laptop, the organization retains data in the data center, where it can be protected.

Managing the virtual machines on the physical servers and the connected networks requires a design that integrates all of these systems so that they work together without creating an operational burden on the IT staff who must maintain them. Using proven and tested designs minimizes the time needed to deploy these new solutions and reduces the time required to deploy new applications.

In a VDI deployment, a user's desktop operating system and applications run in a virtual machine on a server hosted in a data center or server room. A *VDI client* views and operates the user's virtual desktop. VDI clients can be in the same building as the server, on the same network, or across the Internet. The organization can deploy VDI client software on desktops, laptops, or dedicated appliances. When organizations permit a Bring Your Own Device (BYOD) environment, users can access virtual desktops via personal laptops, tablets, and even smartphones.

For *knowledge workers*, who require frequent updates and changes to permissions, you can use a *dedicated* hosted VDI deployment that allows for individual customization and control of the desktop. For *task workers*, who have a consistent and well-defined set of applications not requiring persistent daily customizations, you can deploy *pooled* VDI desktops. For these users, such as those in call centers, retail sales, and order entry departments, a standard desktop is always displayed on login, and no

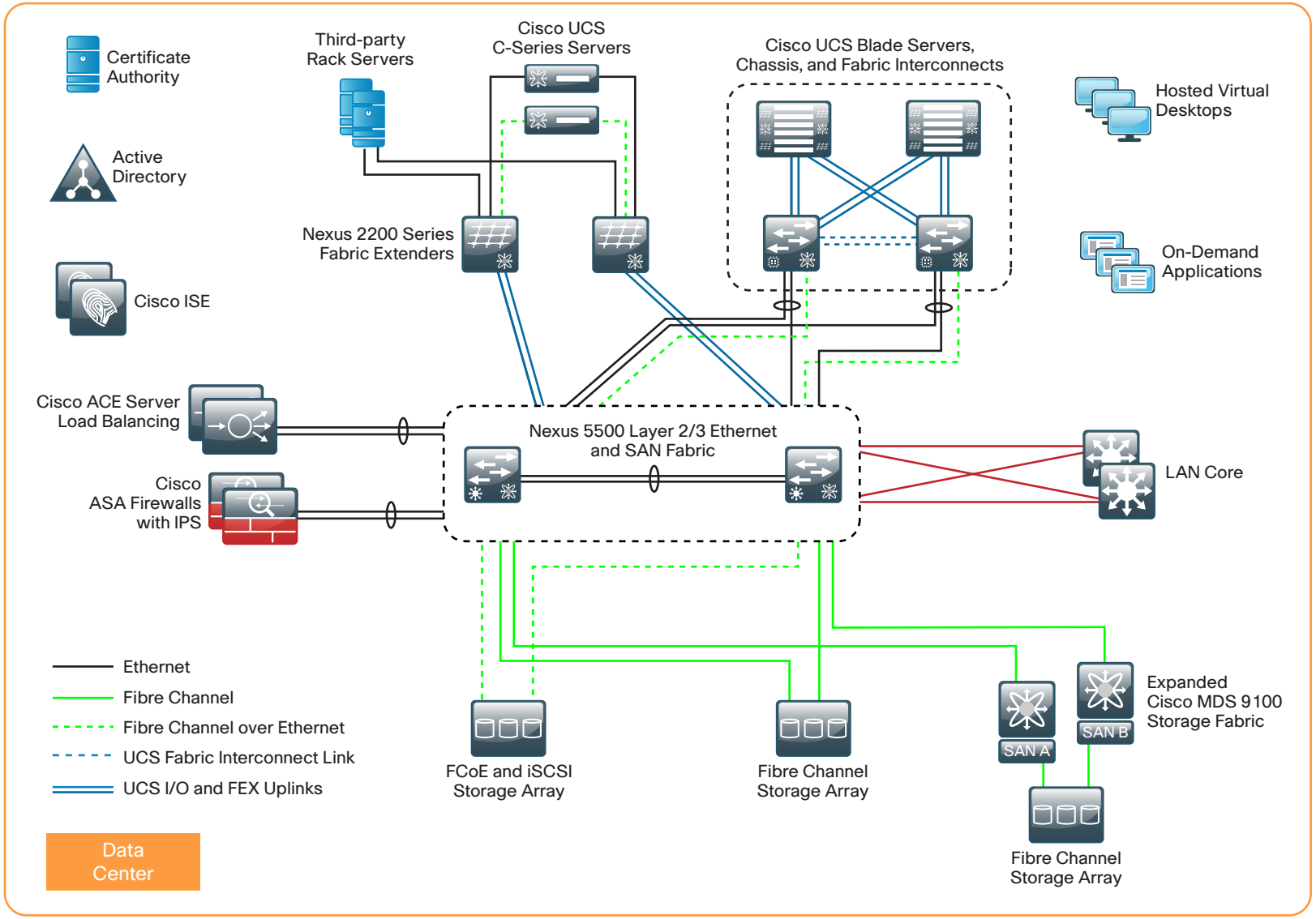
desktop changes persist, offering a fresh desktop upon the next login. Using a pooled VDI deployment that removes desktop personalization allows for more scalability, better efficiency, and cost savings over hosting multiple customized, personal environments with a dedicated VDI deployment.

In the data center, this deployment uses Cisco UCS servers to host the virtual desktops and other data center services required to complete the virtualization solution, such as Microsoft Active Directory servers, certificate authorities, and Cisco Identity Solution Engine (ISE). Deploying the initial VDI solution with Cisco UCS B-Series blade servers ensures that, as an organization grows, the VDI deployment can grow by using the advantages of unified computing and can integrate into the tested Cisco SBA data center architecture.

Cisco Adaptive Security Appliance (ASA) firewalls are used in the data center in order to implement security policies between the virtual desktop VLANs and the application servers in the server VLANs, which contain confidential information belonging to the organization or its customers. A separate set of Cisco ASA firewalls in the Internet edge isolate and protect the organization from Internet-originated attacks. The firewalls also provide the remote-access VPN termination point, allowing users to access the virtualization solution from remote locations.

Notes

Figure 1 - Cisco SBA data center design with VDI



Hosted Shared Virtualization for On-Demand Applications

Instead of offering client OS-based desktop instances made available when deploying a VDI environment, an organization may only require session virtualization or delivery of a single application or subset of applications to endpoints. A Windows Server can host multiple instances of an application and can present an entire server-based desktop to multiple users, which is called a *hosted shared deployment model*. This model uses Remote Desktop Session Host capabilities, also known as Terminal Services. For additional flexibility and scalability, you can virtualize the Windows Server operating system that is providing the services, allowing users to access applications, and different versions of the same application, across multiple virtual servers using the same compute resources.

Many common applications, such as email, web browsers, instant messaging, and social networking, have already been developed and customized to offer the best user experience for the unique end-device used, making it unnecessary and unnatural to use those applications from a complete virtual desktop presented to the same device. This becomes apparent when you try to manipulate a full virtual desktop from a tablet or smartphone, where likely most of the virtual desktop capabilities are unused. In these contexts, manipulating the full virtual desktop can become a burden to productivity, as opposed to the convenience of direct access to the required applications.

However, it may be cost prohibitive or impractical for some applications to have custom versions created for each endpoint used, making hosted shared on-demand applications a better choice for an organization. Security policies may also dictate that data remains centralized, and a virtualized on-demand application approach provides access; for example, devices at remote offices can access a custom application for medical or financial records.

Additionally, removing the requirement to virtualize and present entire desktops results in benefits to scale and performance, because processor cycles on the data center computing systems can be dedicated solely to running the applications on a per-session basis.

Cisco Unified Computing System Hardware

The primary computing platforms deployed in the Cisco SBA reference architecture are Cisco UCS B-Series blade servers and Cisco UCS C-Series rack-mount servers. The Cisco UCS Manager graphical interface provides ease of use that is consistent with the goals of Cisco SBA. When deployed in conjunction with the SBA data center network foundation, the environment provides the flexibility to support concurrent use of the Cisco UCS B-Series blade servers, Cisco UCS C-Series rack-mount servers, and third-party servers, including 1- and 10-Gigabit Ethernet and storage network connectivity.

The *Cisco SBA—Data Center Unified Computing System Deployment Guide* is used to setup the Cisco UCS B-Series blade server's compute infrastructure for the deployment in this guide. The Cisco UCS B-Series blade servers offer a dense and scalable deployment option managed by Cisco UCS Manager. For data centers with the Cisco UCS B-Series blade servers already installed, you can simply add blade servers as required for the virtualization deployment. For smaller environments or proof-of-concept deployments, you may choose to use Cisco UCS C-Series servers, either integrated into a UCS Manager environment or individually managed. For smaller deployments, Cisco UCS C-Series servers containing multiple drive bays, providing flexible on-server RAID storage features, are a cost-effective option that eliminates the need for SAN-attached storage.

Citrix XenDesktop

Citrix is a cloud-computing provider that enables mobile workstyles, with technology solutions that equip organizations for optimizing the use of their existing IT assets and resources, as well as protecting the systems, data, and applications that run the business. As virtualization adoption increases, the benefits are making this compelling virtualization technology a mainstream mandate. Citrix XenDesktop enables a desktop virtualization environment by letting you deliver on-demand virtual desktops and applications to a variety of device types. Because the XenDesktop installation is agnostic to the chosen hypervisor, it fits well into the Cisco SBA data center, building on the virtualization, Cisco UCS, storage, and data center guidance available for the architecture.

In a Citrix XenDesktop deployment, you virtualize Windows desktops directly on a hypervisor and install the Citrix XenDesktop management components as applications in a Windows Server 2008 R2 operating system. For the Cisco SBA installation, the Windows Server OS is virtualized on the hypervisor, instead of running natively on the server hardware, which increases efficiency by allowing multiple VMs to share the hardware.

The Citrix XenDesktop download includes a number of server subcomponents:

- Web Interface—Used to provide users access to their virtual desktops
- Desktop Delivery Controller—Operated by a web interface and responsible for distributing desktops, managing user access, and optimizing connections in the XenDesktop environment
- License Server—Operated by a web-based License Administration Console and used to validate Citrix licenses for the installation
- Desktop Studio—A Microsoft Management Console snap-in used to manage sites created with XenDesktop
- Desktop Director—An application used to provide a detailed overview and monitoring of hosted desktops created with Citrix XenDesktop and Citrix XenApp sessions, for support teams to monitor, maintain, and troubleshoot the system

Citrix Provisioning Services

Citrix Provisioning Services (PVS) is a component added to the Citrix XenDesktop deployment in order to enhance scalability and performance by using an additional virtualization technique. Instead of each hosted virtual desktop maintaining its own disk image on a one-to-one basis, Citrix Provisioning Services allows a many-to-one relationship of virtual machines to a single virtual disk (vDisk). As the number of virtual machines increases, allowing all to boot from a single, read-only vDisk is operationally efficient from an image-maintenance standpoint, and it can also enhance performance of the system.

After Citrix Provisioning Services is installed, you designate a master target device and take a snapshot image of the OS and application. This creates a vDisk that other target devices use as their boot device. Thus, the VMware hypervisor itself does not offer a virtualized disk, but rather the virtualized desktop machines are network-booted from the read-only vDisk. Citrix Provisioning Services also updates machine information that needs to be unique among machines, such as system names, which isn't possible directly from a shared read-only disk image. Additionally, because virtual desktops can't write to the vDisk, a unique write cache is assigned to each virtual machine, allowing each VM the required functionality to update its associated disk storage.

Citrix XenApp

Citrix XenApp software is used to deliver Microsoft Windows on-demand applications, which are centralized and managed in the data center. You can deploy Citrix XenApp software on its own or along with Citrix XenDesktop, and it is available as a component bundled with some Citrix XenDesktop editions. To deliver the Microsoft Windows applications, Citrix XenApp integrates tightly with Windows Server—in this guide, Citrix XenApp 5.6 is coupled with Microsoft Windows Server 2008 R2 Standard with Service Pack 1.

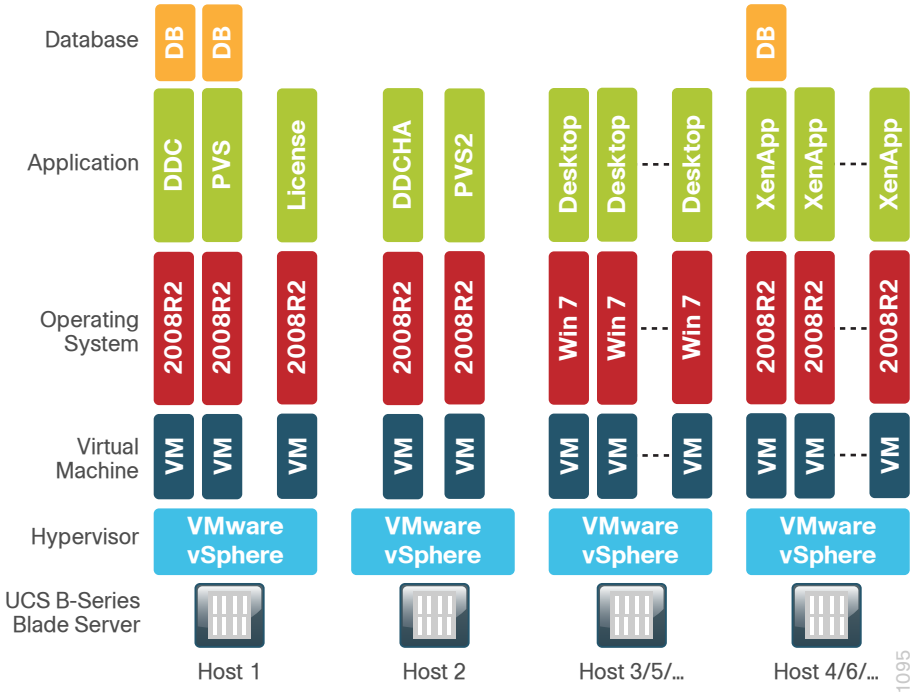
Citrix XenApp can be configured in many ways, optimizing different aspects of virtualization. XenApp delivers user access to applications that are hosted in the virtualized Windows Server environment, referred to as a *hosted shared* deployment model or *Remote Desktop Session Host*. In this deployment, XenApp is not used in other available roles, such as streaming delivery of applications to hosted virtual desktops.

Data Store Database

Citrix XenDesktop, Citrix Provisioning Services, and Citrix XenApp all require database instances in order to store operational information. Many organizations already have a Structured Query Language (SQL) database available, with appropriate redundancy, support staff, and maintenance procedures in place. If your organization has already deployed a database server, you do not require an entirely new database server for the Citrix server applications, as you can use new database instances on the existing database server.

Many database server versions are supported, and deployments vary among organizations. An appropriate production database is assumed to be available, so the integration with the production database is left to the organization. For simplicity and to demonstrate a database installation that is also useful for pre-production, proof-of-concept deployments, this guide uses the default Microsoft SQL Server 2008 R2 Express Edition, which is included as part of the Citrix XenDesktop installation. In production, these databases are database instances in an organization's chosen enterprise database scheme.

Figure 2 - Citrix XenDesktop, PVS, virtual desktop, and XenApp server layout



Citrix Receiver

Citrix Receiver helps provide Citrix XenDesktop and Citrix XenApp users with secure connections to their virtual desktops from any end-point device type with a high-definition user experience. Although the desktops and applications run on remote servers, the user experience is equivalent to that of a local Windows desktop or application. From the user's perspective, logging on to a virtual desktop is the same as logging on to a local desktop, and a virtualized application behaves the same as a locally installed application.

Citrix has incorporated Citrix FlexCast delivery technology into Citrix Receiver, allowing the delivery endpoint to access hosted virtual desktops and on-demand applications used in this guide, along with other virtualization options available from Citrix. The Citrix Receiver client runs on many types of devices, such as PCs, tablets, and smartphones. In this guide, you test Citrix Receiver access in order to validate solution functionality by using a Microsoft Windows 7 endpoint. This guide also provides Apple iOS and Android installation examples.

The basis for transporting content to the endpoint is Citrix Independent Computing Architecture (ICA) protocol. Citrix Receiver employs Citrix HDX (High Definition User Experience) technology enhancements when using the ICA transport, for improved multimedia and quality of service (QoS). The Cisco Wide Area Application Services (WAAS) appliances that are part of the Cisco SBA architecture provide acceleration techniques that optimize ICA transport bandwidth usage.

Deployment Details

Process

Preparing the Data Center for Citrix Installation

1. Prepare servers for Citrix installation
2. Connect servers to data center VDI VLAN
3. Configure the data center firewall

Procedure 1 Prepare servers for Citrix installation

Before Citrix software can be installed, a base data center infrastructure must be in place, including networking, server hardware, virtualization software, and storage access. This procedure serves as an outline for those preparations. For specific guidance, see the Cisco SBA guides referenced in this procedure.

Step 1: Procure and assign server hardware to the VDI installation. The number of servers required is specific to the goals of the deployment. The installation in this guide uses six servers:

- Virtual infrastructure components on one server
- Virtual desktops on a separate server
- Applications hosted on a third server
- Replication of all three servers for high-availability purposes

Optionally, you can add more servers as dictated by the required scale. All servers for this installation are Cisco UCS B-Series blade servers.

Step 2: Verify supporting servers for Dynamic Host Configuration Protocol (DHCP) and Microsoft Active Directory are available for use by this installation.

Step 3: If you have an existing SQL database that is used for development or production, verify that it is available to be used by this installation and inform database administrators that three database instances will need to be created and managed in conjunction with the VDI installation. This installation uses the default SQL Express database as a means to show a common implementation, for proof-of-concept purposes.

Step 4: In Cisco UCS Manager, deploy assigned server hardware into the UCS system. For detailed steps, see the *Cisco SBA—Data Center Unified Computing System Deployment Guide*.

Step 5: In VMware vCenter, enable the VMware vSphere Hypervisor environment on the servers. For detailed steps, see the *Cisco SBA—Data Center Virtualization with Cisco UCS, Nexus 1000V, and VMware Deployment Guide*.

Step 6: In VMware vCenter, configure server Cisco virtual interface card (VIC) connectivity. For detailed steps, see the *Cisco SBA—Data Center Virtualization with Cisco UCS, Nexus 1000V, and VMware Deployment Guide*.

If your deployment uses a Cisco Nexus 1000V distributed virtual switch, use the same guide in order to attach the server hardware to the distributed virtual switch, allowing the server access to the VDI VLAN 157.

Step 7: Allocate storage disk space and associate the storage with the server hardware assigned for the VDI deployment. For more details about using NetApp filers to supply network storage, see the *Cisco SBA—Data Center NetApp Storage Deployment Guide*. This installation uses a large allocation disk space on FCoE-attached, block-based NetApp storage, shared among all Cisco UCS B-Series blade servers.

If your organization's data policies permit doing so, you can substitute direct attached storage integrated directly on the Cisco UCS servers, instead of using network-based storage. The direct attached storage can be used for local caching disk functionality or even for the complete Citrix software installation. This can be a cost-effective alternative to using highly available network storage.

Procedure 2 Connect servers to data center VDI VLAN

The Cisco UCS B-Series server includes multiple Ethernet connections. The two Cisco VIC adapters are associated for use together as dual active connections to the Cisco SBA data center, allowing resiliency and load sharing between links. Because the servers are hosting client virtual desktop machines, much of the server behavior can be characterized as being similar to the activity of many desktops, and thus server connectivity is placed in the VDI desktop VLAN created in the data center.

Traffic to and from the server network interfaces is tagged with the VDI desktop data center VLAN 157. This procedure includes instructions for creating VLAN 157, installing a route to the new VLAN and adding it to the route table, creating port-channel connections to the firewall, and adding firewall policies to the virtual desktops in order to allow them to access necessary business functions. For simplicity, a single VDI VLAN is used in this deployment. As deployments scale, you can add VLANs, to segment traffic as required for bandwidth and policies of an organization.

The Cisco UCS server VICs are connected through the UCS infrastructure, which is connected to dual Cisco Nexus 5500 Series core switches. The following information is used in this procedure to configure the data center core Cisco Nexus 5500 Series switches:

- VDI VLAN—157
- VDI VLAN name—VDI_Desktop
- Virtual port-channel to DC firewall-A—port-channel 53
- Virtual port-channel to DC firewall-B—port-channel 54

You must assign the port-channel interface configuration on both data center core Cisco Nexus 5500 Series switches. Failure to configure the port-channel with matching VLAN assignments on both Nexus 5500 Series switches puts the port-channel interface into an inconsistent state.

Step 1: Log in to the Cisco Nexus 5500 Series data center core switch-A, and then create VLAN 157.

```
vlan 157
  name VDI_Desktop
exit
```

Step 2: Add VLAN 157 as an allowed VLAN on the virtual port-channel trunks to the data center firewall.

```
interface port-channel 53-54
   switchport trunk allowed vlan add 157
exit
```

Step 3: Configure a static route pointing to the trusted subnets behind the Cisco ASA firewall.

```
ip route 10.4.57.0/24 Vlan 153 10.4.53.126
```

Step 4: Redistribute the trusted subnet into the existing Enhanced Interior Gateway Routing Protocol (EIGRP) routing process. This design uses route maps to control which static routes are redistributed, requiring an additional match clause to be added to the existing route map configuration.

```
route-map static-to-eigrp permit 30
  match ip address 10.4.57.0/24
!
router eigrp 100
  redistribute static route-map static-to-eigrp
```

Step 5: Log in to the Cisco Nexus 5500 Series data center core switch-B, and then apply the corresponding configurations as just applied on switch-A.

```
vlan 157
  name VDI_Desktop
exit
!
interface port-channel 53-54
   switchport trunk allowed vlan add 157
exit
!
ip route 10.4.57.0/24 Vlan 153 10.4.53.126
!
route-map static-to-eigrp permit 30
  match ip address 10.4.57.0/24
!
router eigrp 100
  redistribute static route-map static-to-eigrp
```

Procedure 3 Configure the data center firewall

Network traffic entering and exiting the VDI VLAN in the data center transits the data center Cisco ASA firewall. The base firewall configuration is created as part of the *Cisco SBA—Data Center Deployment Guide*, and this procedure builds upon that configuration.

The following information is used in this procedure to configure the data center Cisco ASA firewall:

- Production port-channel interface—port-channel 10.157
- Interface name—DC-VDI_Desktop
- Firewall security level—75
- IP address—10.4.57.1/24
- Standby IP address—10.4.57.2

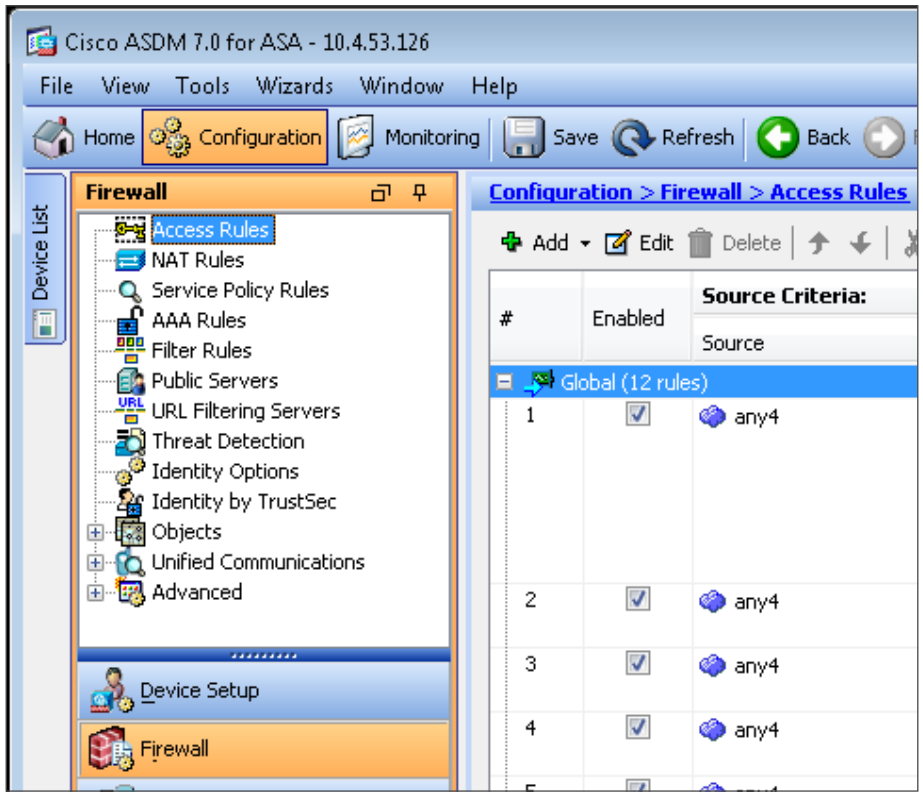
Step 1: Connect to the data center Cisco ASA firewall, and use the CLI to add VLAN 157 to production port-channel 10.

```
interface Port-channel10.157
description DC VDI_Desktop VLAN
vlan 157
nameif DC-VDI_Desktop
security-level 75
ip address 10.4.57.1 255.255.255.0 standby 10.4.57.2
no shutdown
```

Step 2: In a web browser, launch Cisco Adaptive Security Device Manager (ASDM). This is the Cisco ASA management GUI that allows you to configure firewall policies.

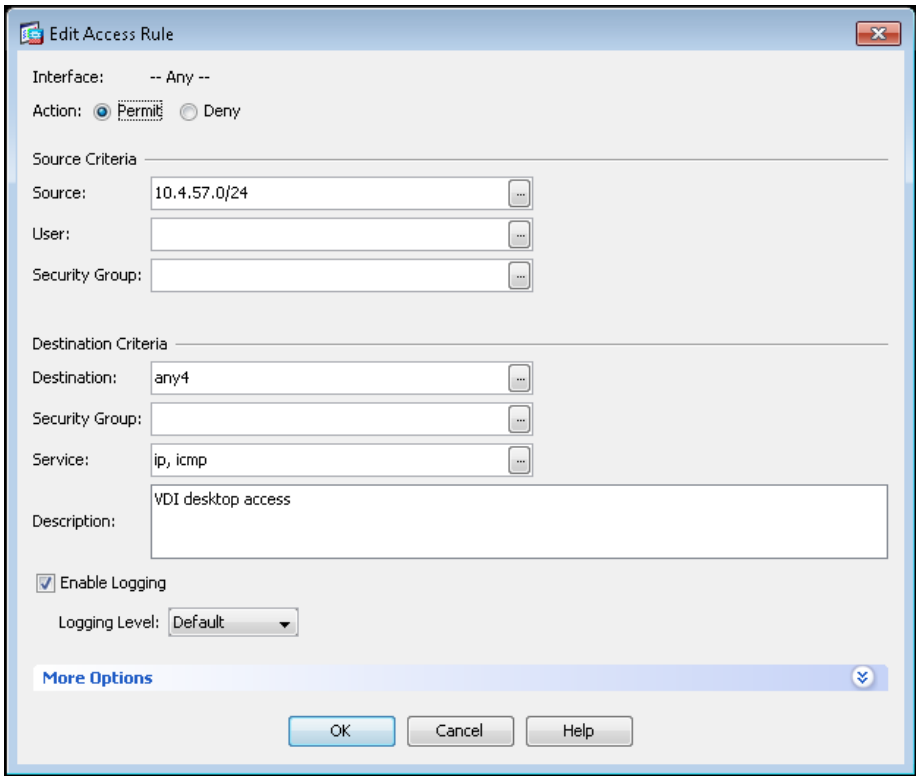
https://[Cisco ASDM IP address]/

Step 3: Select **Configuration**, click **Firewall**, and then click **Access Rules**. The running firewall access rules are displayed.

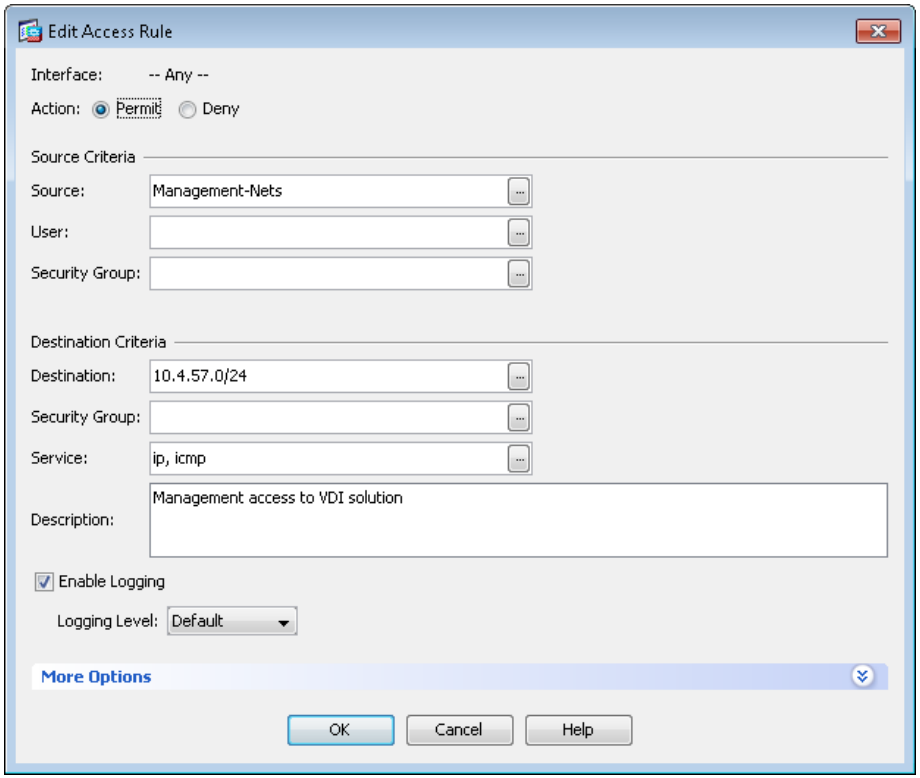


Next, you create firewall policies. The values used in this procedure are examples, and your organization may have different firewall policy requirements.

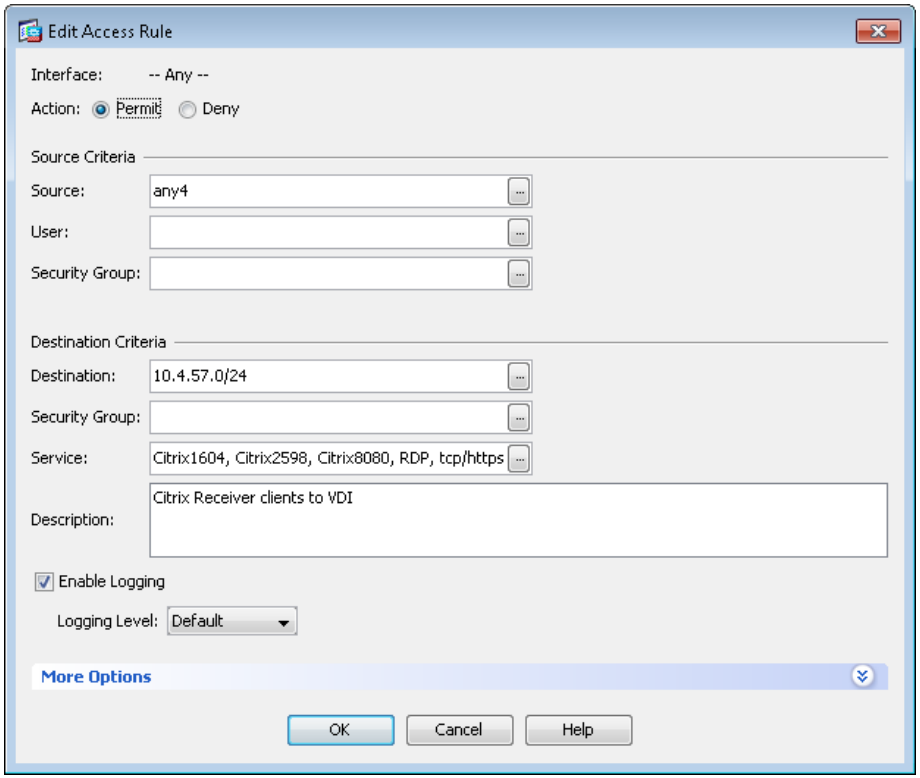
Step 4: Using the Access Rules configuration panel, add an access rule to enable a policy permitting VDI desktop traffic originating from the source DC-VDI_Desktop-network/24 object to access any network, and then click **OK**.



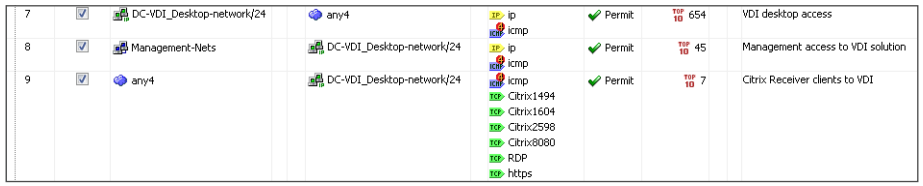
Step 5: Add an access rule to enable a policy allowing workstations to manage Citrix XenDesktop, PVS, and XenApp instances in the VDI VLAN destination DC-VDI_Desktop-network/24 object, and then click **OK**.



Step 6: Add an access rule to enable a policy allowing Citrix Receiver clients to access virtual desktops in the VDI VLAN destination DC-VDI_Desktop-network/24 object, and then click **OK**.



Step 7: At the display showing the inserted firewall access rules, click **Apply**. This enables the new rules.



The firewall now permits access inbound and outbound to the VDI VLAN.

Process

Installing and Configuring Citrix XenDesktop

1. Install XenDesktop
2. Install Citrix License Server VM
3. Configure the site
4. Prepare SQL database for remote access
5. Join additional XenDesktop VM into site

Citrix XenDesktop contains multiple components that you install on the server hardware designated for VDI infrastructure. The components include:

- XenDesktop Controller—also known as the *Desktop Delivery Controller (DDC)*
- Web Access—to broker connections for the virtual desktops
- Desktop Studio—to configure and manage your XenDesktop deployment
- Desktop Director—to monitor and maintain hosted virtual desktops
- License Server—to maintain Citrix licenses for this installation. This component is required if an available Citrix License Server does not already exist in the organization.

The installation of these components is included as part of the Citrix XenDesktop ISO installation image. The ISO also contains the Virtual Desktop Agent, which you do not install on Windows Server but do install into the operating system on the virtual desktops that are created for the users.

Procedure 1 Install XenDesktop

In this procedure, you create a primary VM and secondary VM that both operate Citrix XenDesktop, for high-availability purposes. Each installation of the Citrix XenDesktop software is installed into a Microsoft Windows Server 2008 R2 operating system. The details of a Windows Server installation vary by IT organization, and specific Windows installation details are not included in this guide.

Reader Tip

For more information about installing Windows Server 2008 R2, see the following:
http://technet.microsoft.com/en-us/library/dd379511.aspx

You install Microsoft Windows Server 2008 R2 virtual machine instances (including VMware Tools) on the Cisco UCS hardware designated for infrastructure services. The following information is used.

Table 1 - Citrix XenDesktop configuration values for Cisco UCS server 1

Component	Parameter	Cisco SBA value
H1: Cisco UCS server 1	Name in VMware vCenter	chas3-s1
	IP address	10.4.63.112
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
DDC virtual machine	Name in VMware vCenter	H1-DDC
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	DNS name	DDC
	IP address	10.4.57.4
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

For each Windows Server instance, ensure that:

- Network connectivity is configured and available
- Windows OS license is activated
- Windows Server patches are applied
- Microsoft Active Directory domain is joined (prerequisite for site-configuration step)

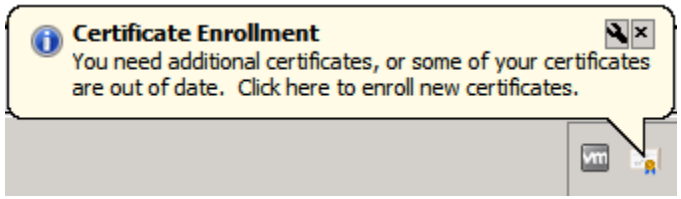
The following Windows Server prerequisites for the Citrix XenDesktop installation do not need to be installed at this time because the installation software detects that they are not installed and then automatically launches their installation:

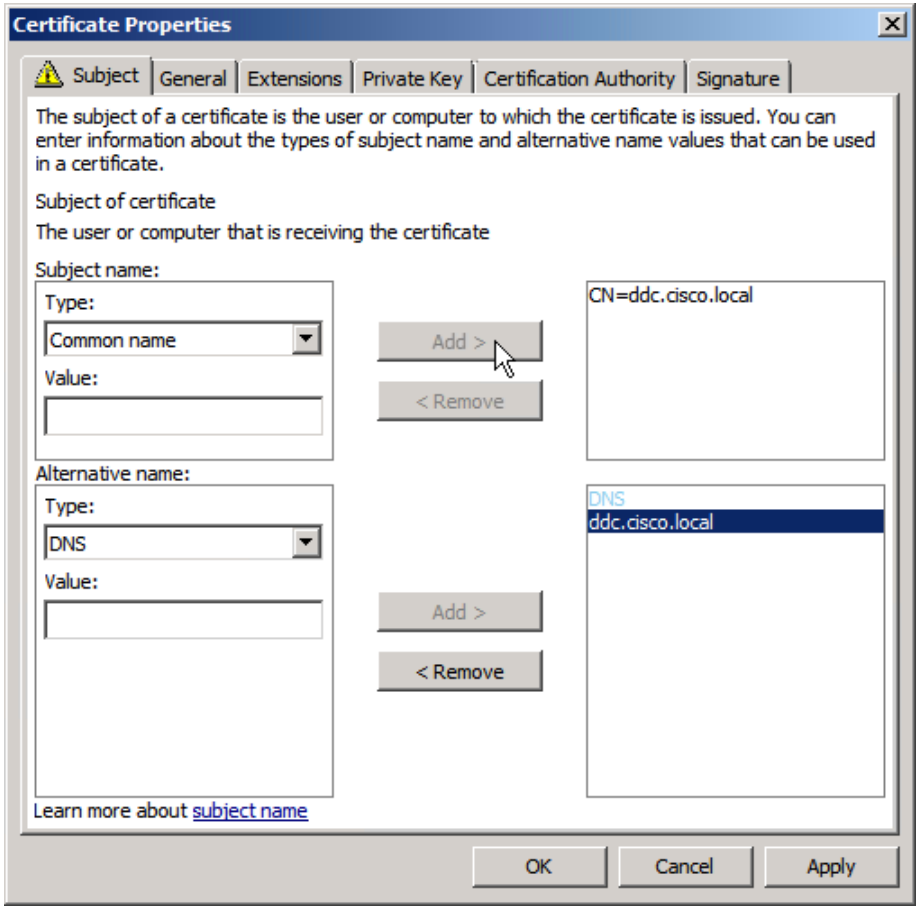
- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft Internet Information Services (IIS)
- Microsoft Visual J# 2.0 SE
- Microsoft SQL Server 2008 R2 Express

Step 1: On Cisco UCS server 1, install a Microsoft Windows Server 2008 R2 virtual machine instance and VMware Tools, configure network connectivity by using the values in Table 1, and then join the Active Directory domain. When joining the domain, you will be prompted to reload the VM. This is the virtual machine instance that runs the primary DDC installation.

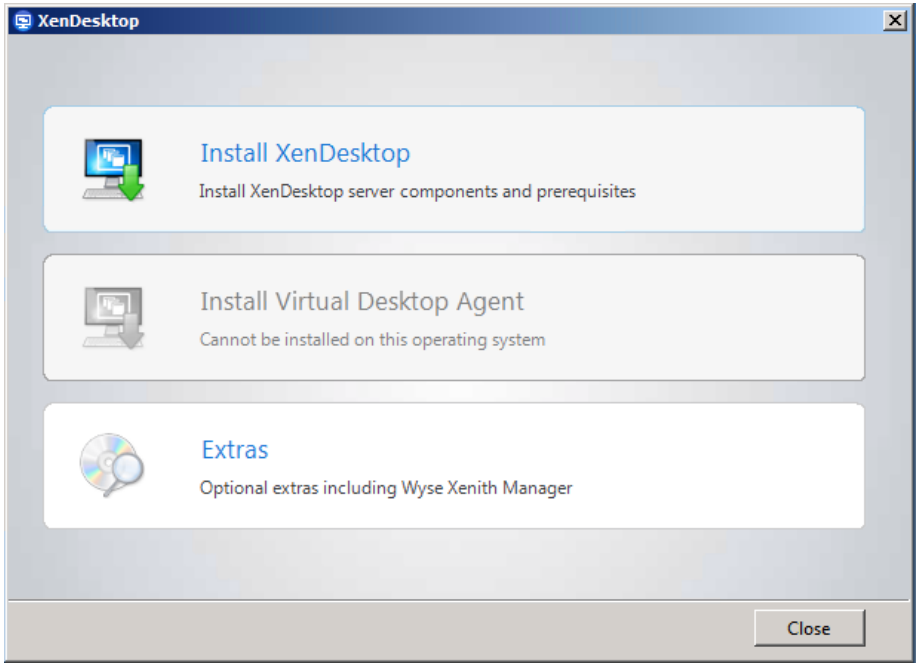
Step 2: After the reload for Active Directory changes is complete, return to the console and then log in to the Active Directory domain as a user with administrative privileges (Example: cisco.local\administrator).

Step 3: If the Active Directory domain requires setup of a certificate for the Simple Certificate Enrollment Protocol (SCEP) service, a message is displayed. Click the taskbar icon, and then complete the certificate enrollment. Use names that match the DNS names for the VM installation instance.





Step 4: In VMware vCenter, mount the Citrix XenDesktop ISO image to the created Windows Server virtual machine, and then allow the AutoPlay service to launch the Citrix AutoSelect.exe XenDesktop installer. The first XenDesktop installation wizard is displayed.



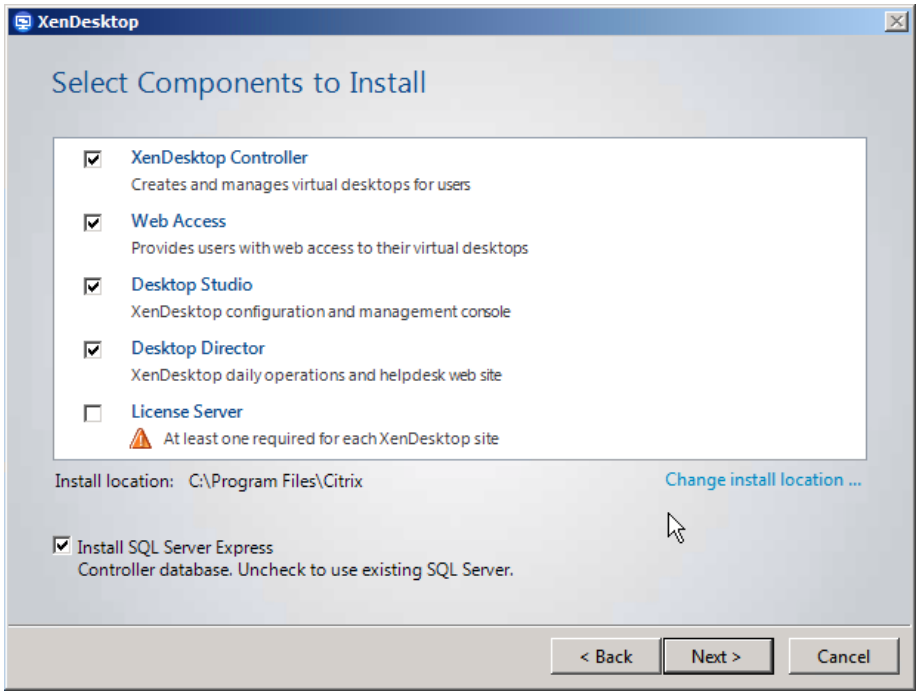
Step 5: Click **Install XenDesktop**.

Step 6: On the licensing page, accept the Citrix XenDesktop Licensing Agreement, and then click **Next**.

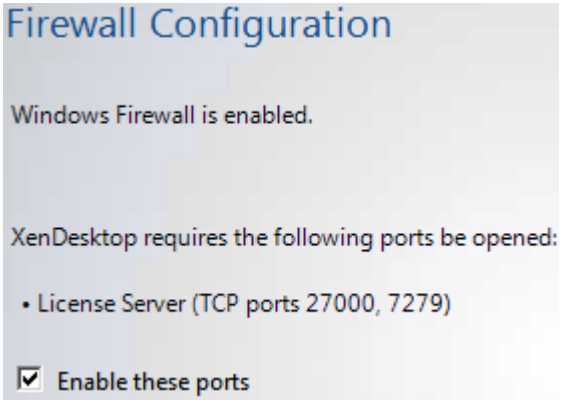
Step 7: On the Select Components to Install page, clear **License Server**.

If this installation is for an additional server for high availability or you have an alternative SQL database that you are using for the installation, clear **Install SQL Server Express**, and then click **Next**.

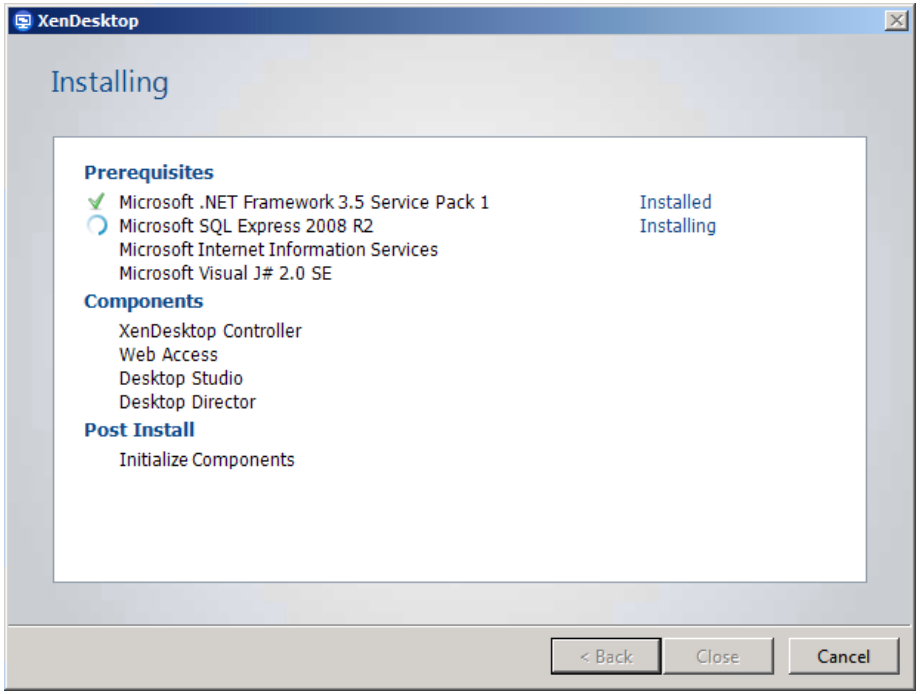
If this is the first Citrix XenDesktop installation (not an additional high-availability one) and you are not using an existing SQL database, verify **Install SQL Server Express** is selected, and then click **Next**.



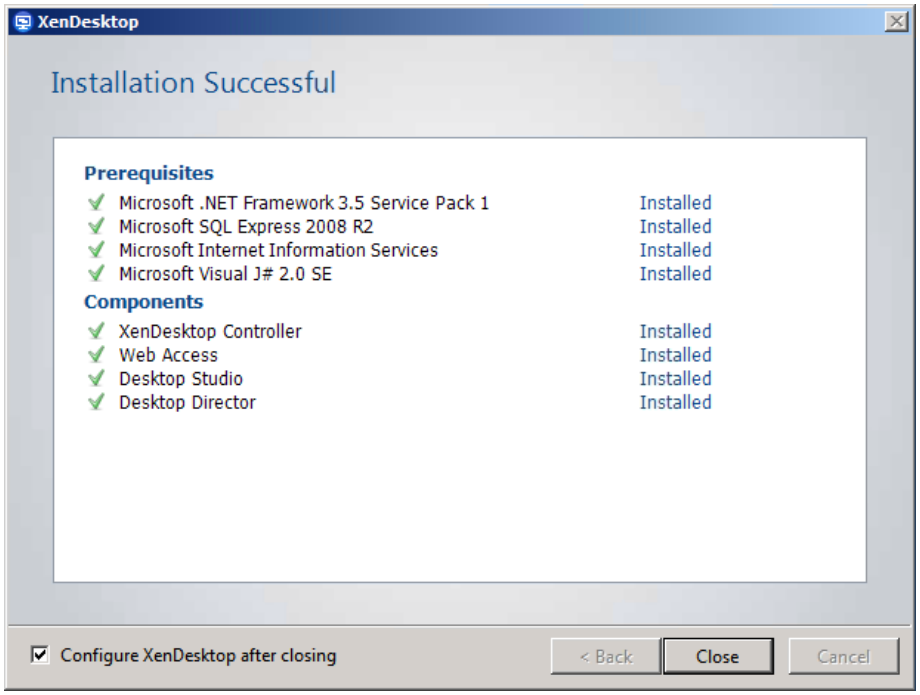
Step 8: If Windows Firewall is enabled, the Firewall Configuration page is displayed. Verify that **Enable these ports** is selected, and then click **Next**.



Step 9: On the Summary page, click **Install**. The installation begins. The Installing page appears and shows progress as the installation continues. The Microsoft SQL Express 2008 R2 prerequisite varies, depending on installation.



Once complete, Installation Successful is displayed.



Because this installation includes Desktop Studio and was launched on a server that is joined to Active Directory, the option to configure Citrix XenDesktop is displayed.

Step 10: On the Installation Successful page, verify **Configure XenDesktop after closing** is selected, and then click **Close**. The Citrix XenDesktop installation wizard completes, and the Citrix Desktop Studio snap-in to the Microsoft Management Console is launched.

Step 11: Close the Citrix Desktop Studio window. You complete this configuration in a later procedure.

Step 12: Launch Windows Update, apply any updates found, and then repeat the check for updates until no updates remain. Because the installation adds Windows components, those components should be updated with the latest patches, usually requiring at least one reboot of the virtual machine (VM).

On the server, in a web browser, navigate to the following URL: **http://localhost**

The Citrix XenDesktop logon screen displays in the web browser. This confirms the Citrix XenDesktop installation.

Step 13: On Cisco UCS server 2, which serves as the high-availability Citrix XenDesktop server, repeat this procedure and use the information in the following table.

Table 2 - DDCHA configuration values for Cisco UCS server 2

Component	Parameter	Cisco SBA value
H2: Cisco UCS server 2	Name in VMware vCenter	chas3-s2
	IP address	10.4.63.113
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
DDC high-availability virtual machine	Name in VMware vCenter	H2-DDCHA
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	DNS name	DDCHA
	IP address	10.4.57.5
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

Procedure 2 Install Citrix License Server VM

In this procedure, you create a new virtual machine on the primary Cisco UCS server. This virtual machine runs Citrix License Server, which is operated by a web-based License Administration Console and used to validate Citrix licenses.

The following information is used for the installation of Citrix License Server.

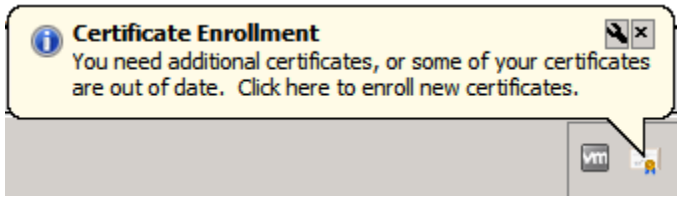
Table 3 - LicenseServer configuration values for Cisco UCS server 1

Component	Parameter	Cisco SBA value
H1: Cisco UCS server 1	Name in VMware vCenter	chas3-s1
	IP address	10.4.63.112
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
LicenseServer virtual machine	Name in VMware vCenter	H1-LicenseServer
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	DNS name	LicenseServer
	IP address	10.4.57.6
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

Step 1: On Cisco UCS server 1, install an additional Microsoft Windows Server 2008 R2 virtual machine instance for Citrix License Server, configure network connectivity, and then join the Active Directory domain. When joining the domain, you will be prompted to reload the VM.

Step 2: After the reload for Active Directory changes is complete, return to the console, and then log in to the Active Directory domain as a user with administrative privileges (Example: cisco.local\administrator).

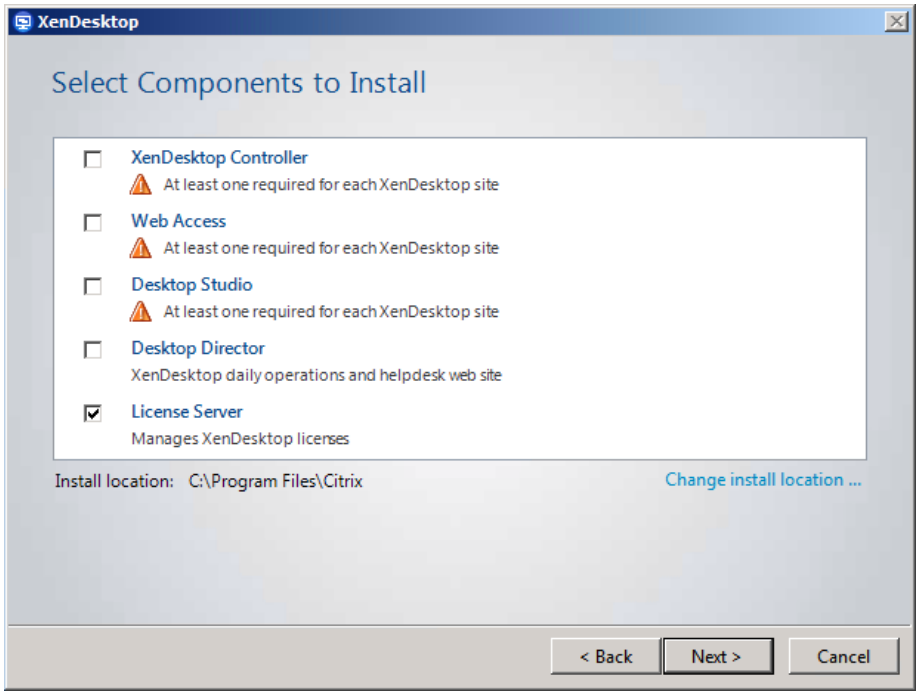
Step 3: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click the taskbar icon, and then complete the certificate enrollment.



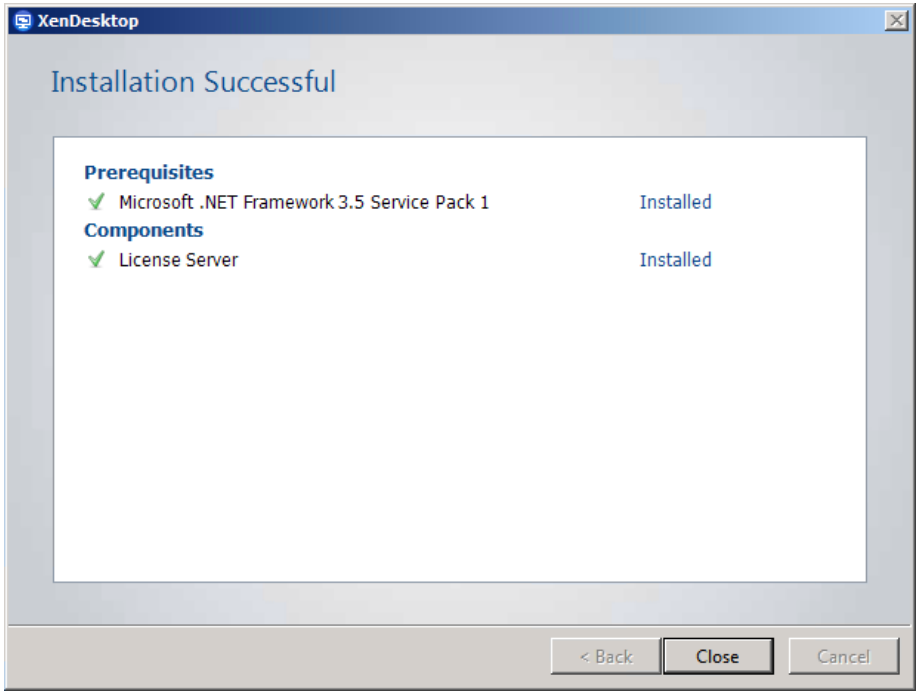
Step 4: In VMware vCenter, mount the Citrix XenDesktop ISO image to the created Windows Server virtual machine for the H1-LicenseServer VM, and then allow the AutoPlay service to launch the XenDesktop installer. The first XenDesktop installation wizard is displayed.

Step 5: Complete the XenDesktop installation wizard, and note the following:

- Click **Install XenDesktop**.
- On the licensing page, accept the Citrix XenDesktop Licensing Agreement, and then click **Next**.
- On the Select Components to Install page, clear all the check boxes except **License Server**, and then click **Next**.



- If Windows Firewall is enabled, then the Firewall Configuration page is displayed. Verify that **Enable these ports** is selected, and then click **Next**.
- Complete the wizard, and then click **Close**.



The Citrix License Server software is now installed. Because the installation adds Windows components, those components should be updated with the latest patches.

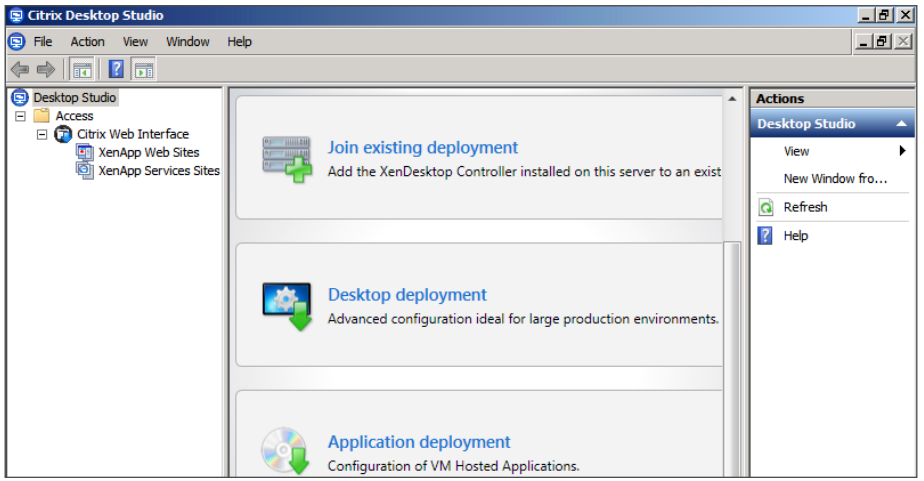
Step 6: Check for Windows updates, and apply any found.

Procedure 3 Configure the site

In this procedure, you use Citrix Desktop Studio in order to configure the desktop deployment site.

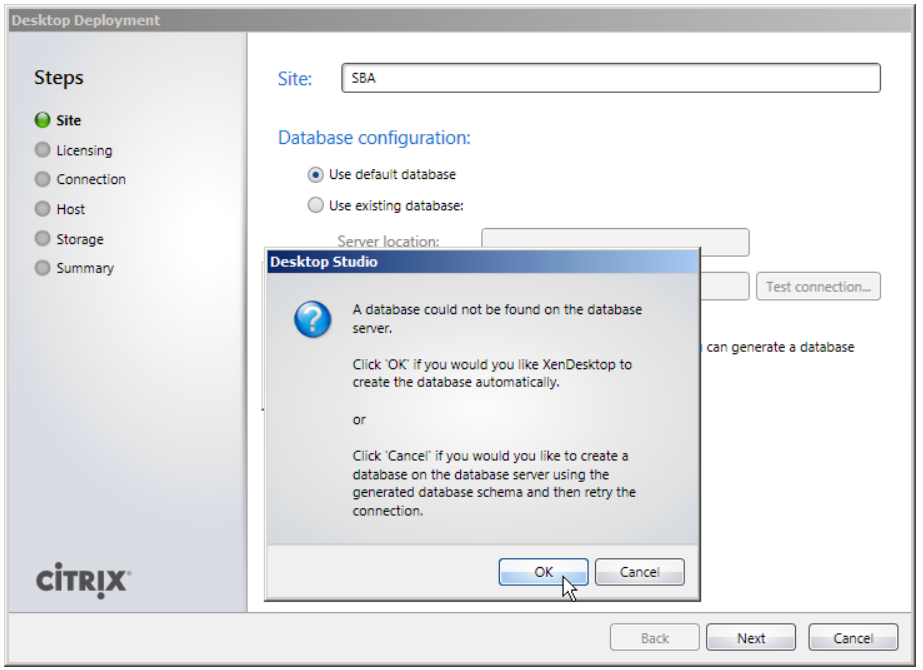
Step 1: Log in to the console of the H1-DDC VM (Example: DDC.cisco.local) as an administrative user in the Active Directory domain (Example: cisco.local\administrator).

Step 2: Click **Start** > **All Programs** > **Citrix**, and then click **Desktop Studio**. Citrix Desktop Studio launches.



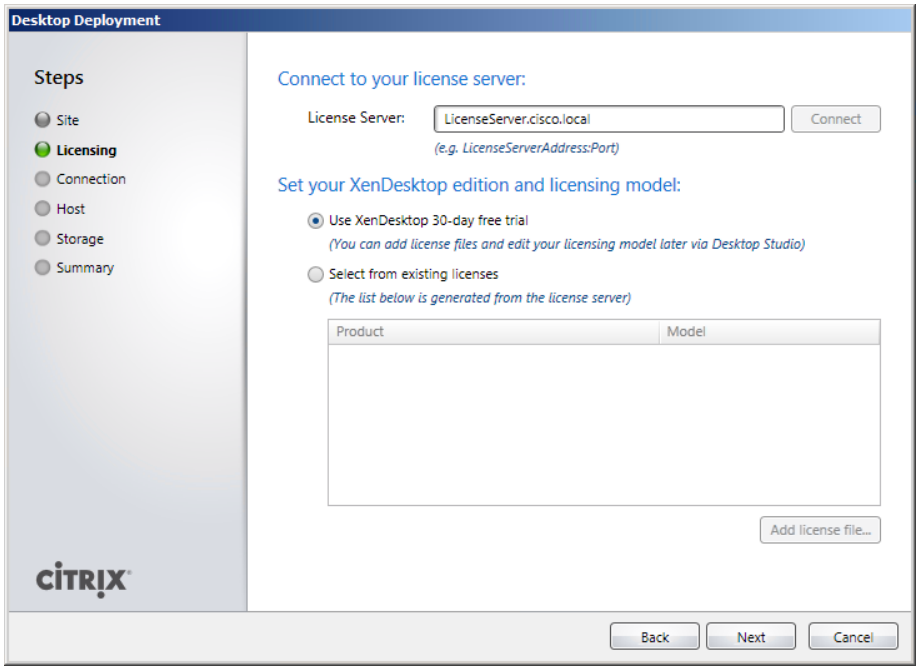
Step 3: Click **Desktop deployment**. The Desktop Deployment wizard launches.

Step 4: On the Site page, name the site SBA, select **Use default database**, and then click **Next**.



Step 5: On the "A database could not be found on the database server" message, click **OK**. Automated configuration of the database starts.

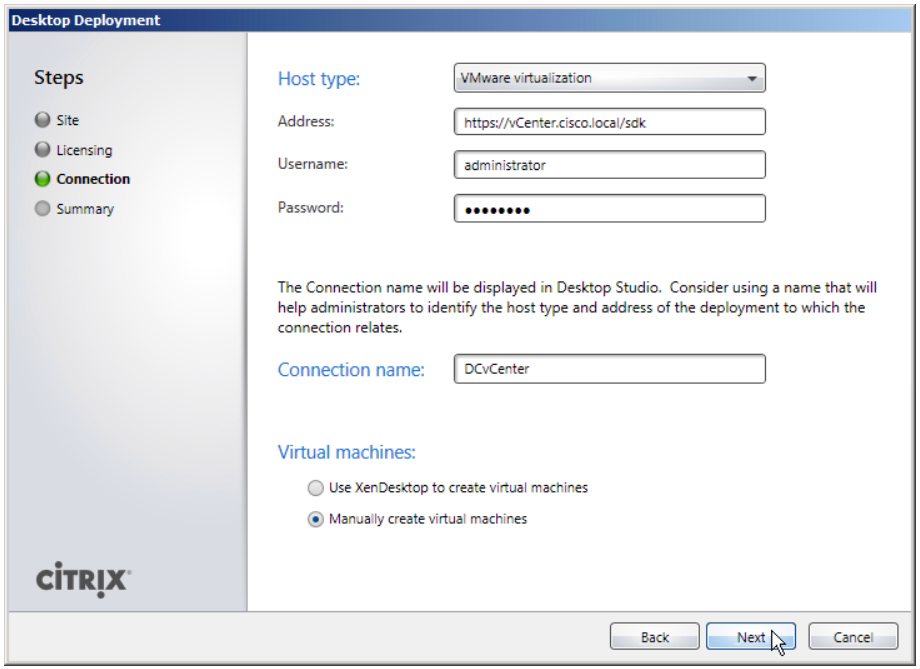
Step 6: On the Licensing page, in the **License Server** box, enter LicenseServer.cisco.local, and then click **Connect**. Ensure **Use XenDesktop 30-day free trial** is selected, and then click **Next**.



Step 7: On the connection page, enter the following values, and then click **Next**:

- Host type—**VMware virtualization**
- Address—http://vCenter.cisco.local/sdk
- Username—administrator
- Password—[password]
- Connection name—DCvCenter
- Virtual machines—**Manually create virtual machines**

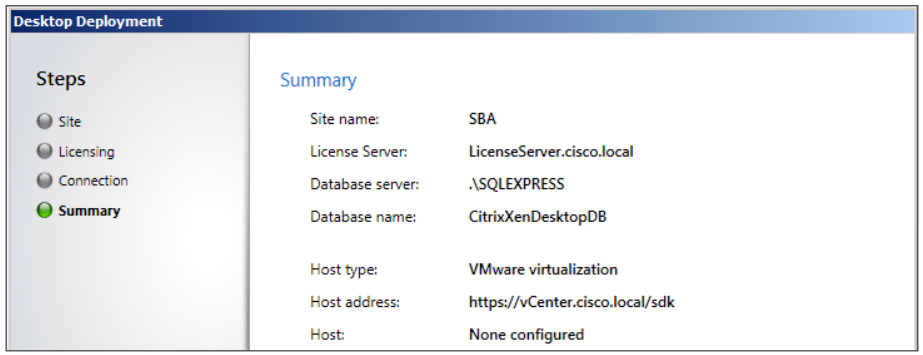
The manual option is the optimal way to configure when solely using Citrix PVS for machine creation, as the alternative requires more options in order to configure Machine Creation Services (MCS) before proceeding.



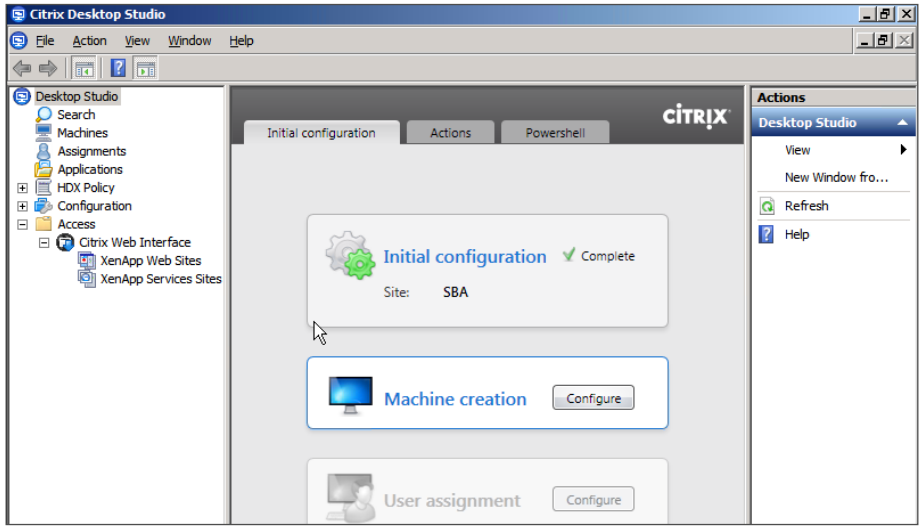
Tech Tip

For Citrix Desktop Studio Secure Sockets Layer (SSL) communication to VMware vCenter to be successful using HTTPS, an appropriate certificate trust relationship must be created. If vCenter is not using a trusted root certificate authority (CA), but instead uses a self-signed certificate, you can point a web browser to vCenter, such as https://vCenter.cisco.local, and accept the untrusted certificate. Then view the certificate and manually install it into the certificate physical stores, under **Trusted People** > **Local Computer**.

Step 8: On the Summary page, click **Finish**.



Desktop Studio completes the installation and displays the newly created site.



The base Citrix XenDesktop software installation is complete.

Procedure 4 Prepare SQL database for remote access

Step 1: Log in to the H1-DDC virtual machine console (Example: DDC.cisco.local), and then navigate to **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager**. SQL Server Configuration Manager opens.

Step 2: In the tree, navigate to **SQL Server Network Configuration > Protocols for SQLEXPRESS**.

Step 3: Double-click **Named Pipes**.

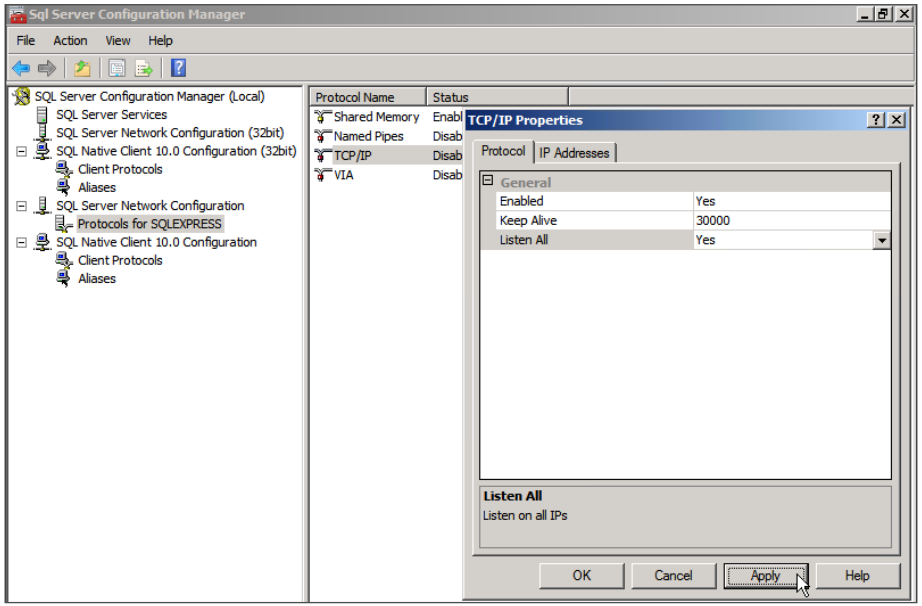
Step 4: On the Named Pipes Properties dialog box, next to Enabled, select **Yes**, and then click **Apply**.

Step 5: On the message about the changes made, click **OK**, and then click **OK** to close the dialog box.

Step 6: In the tree, navigate to **SQL Server Network Configuration > Protocols for SQLEXPRESS**.

Step 7: Double-click **TCP/IP**.

Step 8: On the TCP/IP Properties dialog box, on the Protocol tab, next to Enabled, select **Yes**, next to Listen All, choose **No**, click **Apply**.



Step 9: On the message about the changes made, click **OK**.

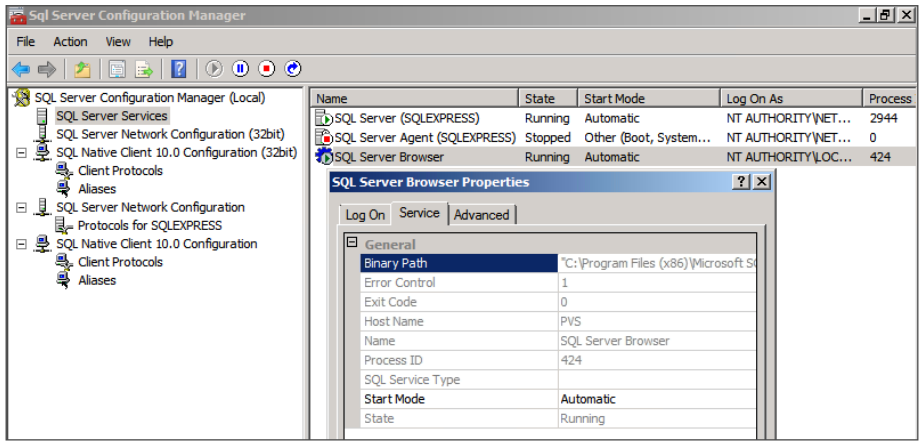
Step 10: Click the **IP Addresses** tab, locate the adapter with the active IP address, clear the **TCP Dynamic Port** box, in the **TCP Port** box, enter **1433**, and then click **OK**.

Step 11: On the message about the changes made, click **OK**, and then click **OK** to close the dialog box.

Step 12: In the tree, navigate to **SQL Server Services**, in the pane on the right side right-click **SQL Server**, and then click **Restart**. The SQL server restarts.

Step 13: In the tree, click **SQL Server Services**, right-click **SQL Server Browser**, and then choose **Properties**.

Step 14: On the SQL Server Browser Properties dialog box, click the **Service** tab, next to Start Mode, choose **Automatic**, and then click **OK**.



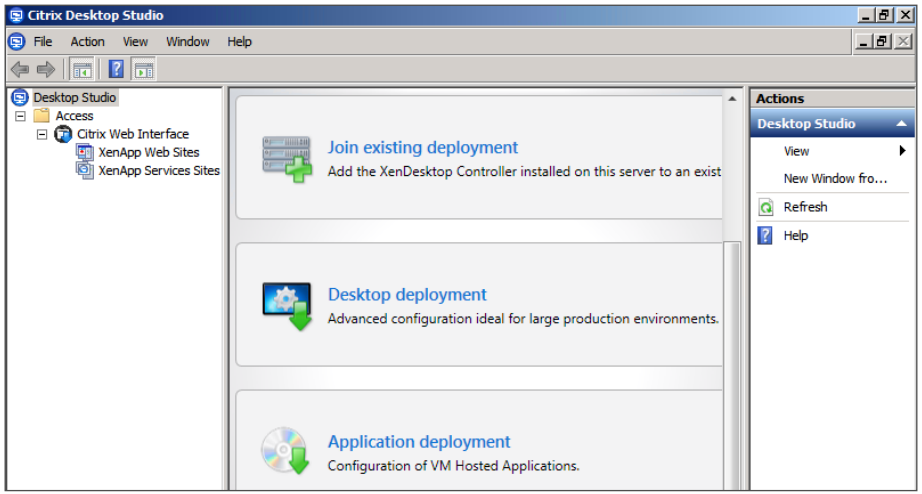
Step 15: Right-click **SQL Server Browser**, and then choose **Start**.

Step 16: On the H1-DDC VM console, using the Windows Control Panel, disable Windows Firewall. Once connectivity is demonstrated, you can enable and customize the firewall for your environment.

Procedure 5 Join additional XenDesktop VM into site

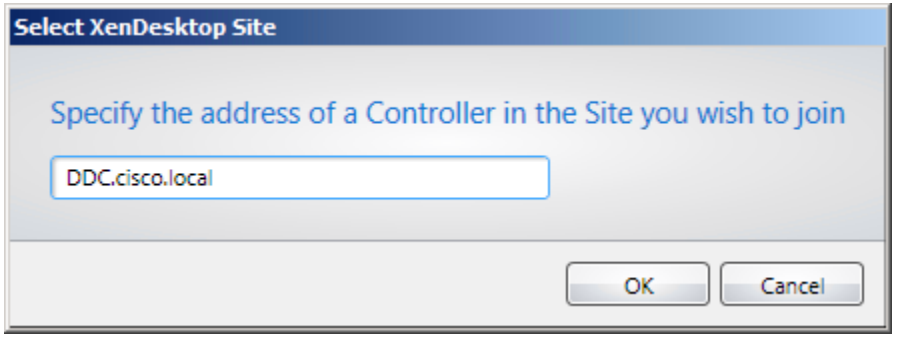
Step 1: Log in to the console of the H2-DDCHA VM as an administrative user in the domain (Example: cisco.local\administrator).

Step 2: Click **Start** > **All Programs** > **Citrix**, and then click **Desktop Studio**. Citrix Desktop Studio is launched.

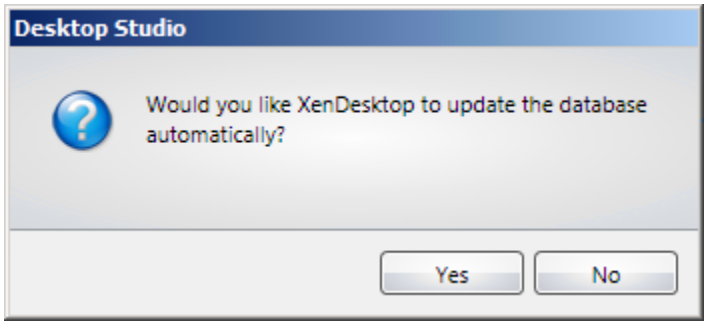


Step 3: Click **Join existing deployment**. The Desktop Deployment wizard launches.

Step 4: On the Select XenDesktop Site dialog box, enter DDC.cisco.local, and then click **OK**.

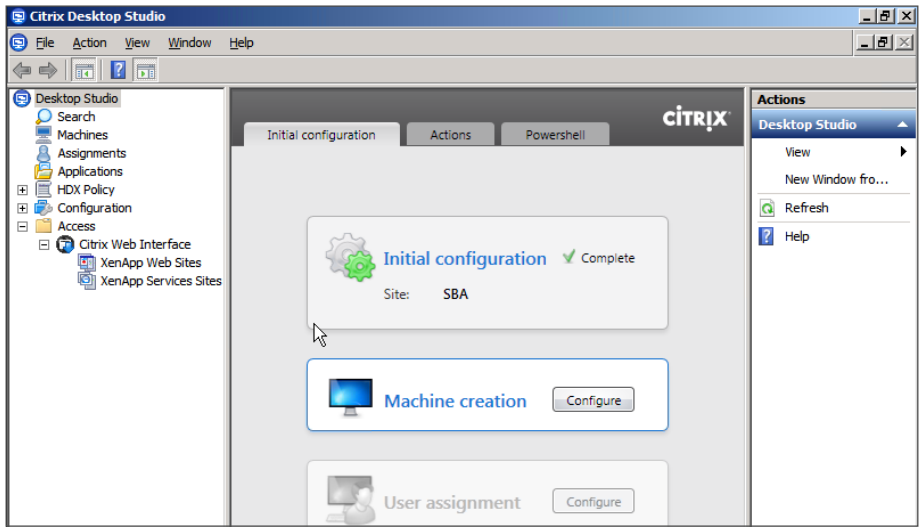


Step 5: On the "Would you like XenDesktop to update the database automatically" message, click **Yes**. Citrix XenDesktop begins to update the database.



If the wizard returns any errors, the database may not be remotely accessible. If the wizard asks for credentials, then the database may have been installed while not logged into the domain, or the current user may not be logged into the domain with credentials that can access the database. If these scenarios occur, you must correct them and restart the configuration procedure.

Citrix Desktop Studio completes the installation and displays the newly created site, showing the same view as available from the H1-DDC VM.



The base Citrix XenDesktop software installation for the high availability server is complete.

Process

Deploying Citrix Provisioning Services (PVS)

1. Install Citrix Provisioning Services VM
2. Configure Provisioning Services
3. Create a master Windows 7 desktop
4. Install Virtual Desktop Agent (VDA)
5. Install Citrix PVS Target Device Software
6. Remove any ghost network interfaces
7. Create and acquire master target vDisk
8. Install additional Citrix PVS VM
9. Configure additional Citrix PVS VM
10. Create streamed VM collection
11. Create catalog in Citrix Desktop Studio
12. Test connectivity to virtual desktops

Citrix XenDesktop has a built-in virtual desktop provisioning service called Machine Creation Services (MCS). To improve scalability, Citrix Provisioning Services (PVS) is used as an alternative to MCS. PVS achieves greater scalability by using the SAN for delivery of a common virtual disk (vDisk) to multiple users, whereas MCS does not require SAN but requires more RAM I/O operations as the performance trade-off.

In this process, you install a primary Citrix PVS VM and one or more additional PVS VMs for high availability and increased scalability. After installation, you configure the PVS instances.

Procedure 1 Install Citrix Provisioning Services VM

Each installation of the Citrix Provisioning Services (PVS) software is installed into a Microsoft Windows Server 2008 R2 operating system. The details of a Windows Server installation vary by IT organization, and specific Windows installation details are not included here.

Reader Tip

For more information about installing Windows Server 2008 R2, see the following:
http://technet.microsoft.com/en-us/library/dd379511.aspx

You install Microsoft Windows Server 2008 R2 virtual machine instances (including VMware Tools) on the Cisco UCS hardware designated for infrastructure services. The following information is used:

Table 4 - Citrix PVS configuration values for Cisco UCS server 1

Component	Parameter	Cisco SBA value
H1: Cisco UCS server 1	Name in VMware vCenter	chas3-s1
PVS virtual machine	Name in VMware vCenter	H1-PVS
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:\ drive)
	Hard disk 2	Virtual disk with default 40 GB drive (E:\ drive)
	DNS name	PVS
	IP address	10.4.57.7
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

For each Windows Server instance, ensure that:

- Network connectivity is configured and available
- Windows OS license is activated
- Windows Server patches are applied
- Microsoft Active Directory domain is joined

The following Windows Server prerequisite for the Citrix Provisioning Services installation needs to be installed, before Citrix PVS installation:

- Microsoft .NET Framework 3.5 Service Pack 1

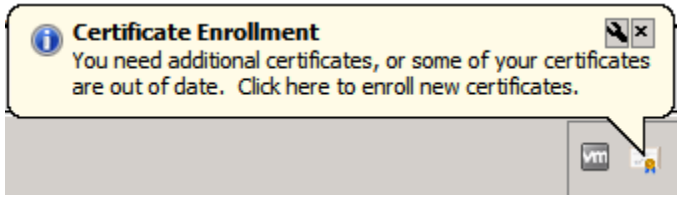
Step 1: On Cisco UCS server 1, install a Microsoft Windows Server 2008 R2 virtual machine instance and VMware Tools, configure network connectivity by using the values in Table 4, activate Windows, and then join the Active Directory domain. When joining the domain, you will be prompted to reload the VM. This is the primary virtual machine instance that runs Citrix PVS.

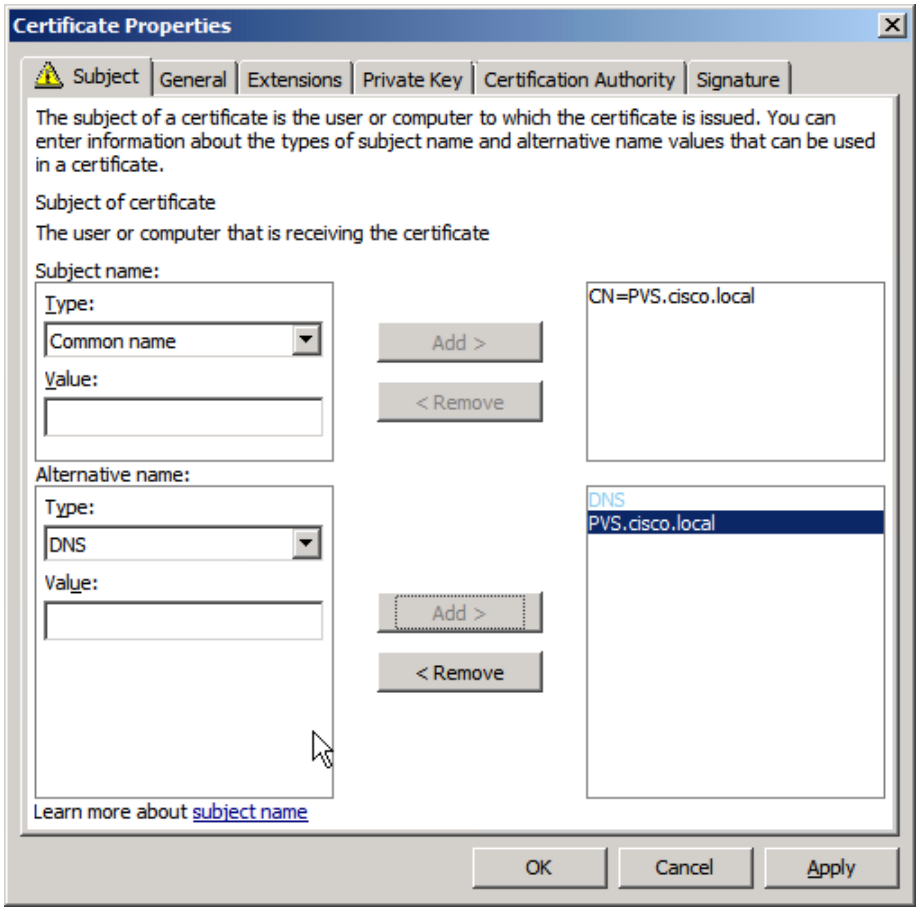
Step 2: After the reload for Active Directory changes is complete, log into the Active Directory cisco.local domain, with an account that has local administrator privileges.

Caution

Installing Citrix PVS while not logged in as a user in a domain can cause setup issues.

Step 3: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click on the taskbar icon, and then complete the certificate enrollment.





Step 4: Click **Start**, in the search box, enter **server manager**, and then click **Server Manager**.

Step 5: In Server Manager, click **Features > Add Features**, select **.NET Framework 3.5.1 Features**, and then at the prompt, click **Add Required Role Services**.

Step 6: In the wizard, use the default values, and then on the last page, click **Install**. When prompted, confirm the installation.

Step 7: When the installation is complete, close the installation wizard.

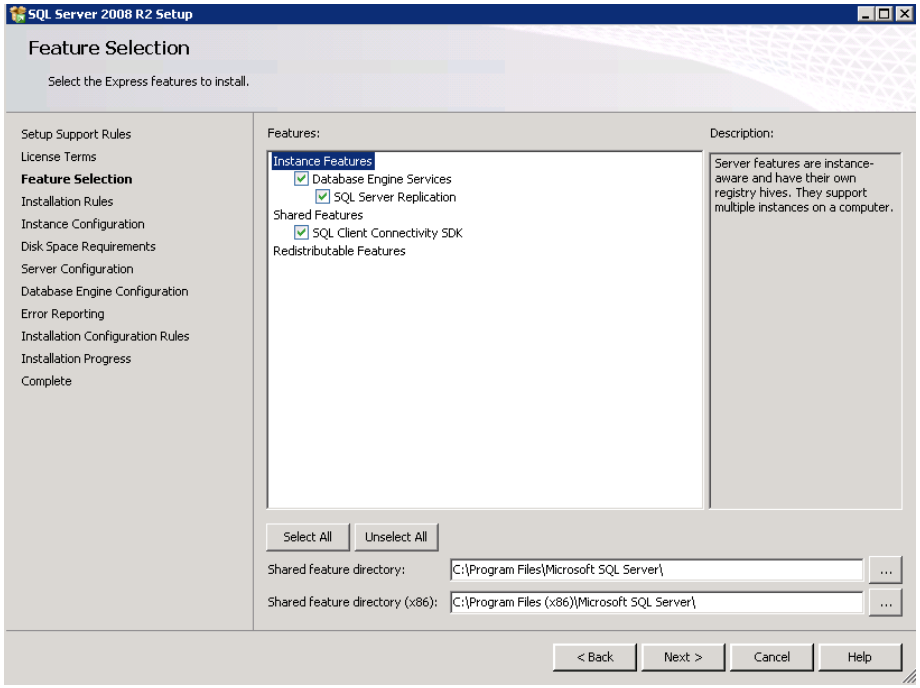
If you plan to integrate with an existing production SQL database, skip to Step 26. As previously described, for this deployment you use a local SQL Express database. The installation for Citrix PVS is available from the Citrix XenDesktop ISO image.

Step 8: In VMware vCenter, connect the Citrix XenDesktop installation ISO (not the PVS ISO) to the H1-PVS VM.

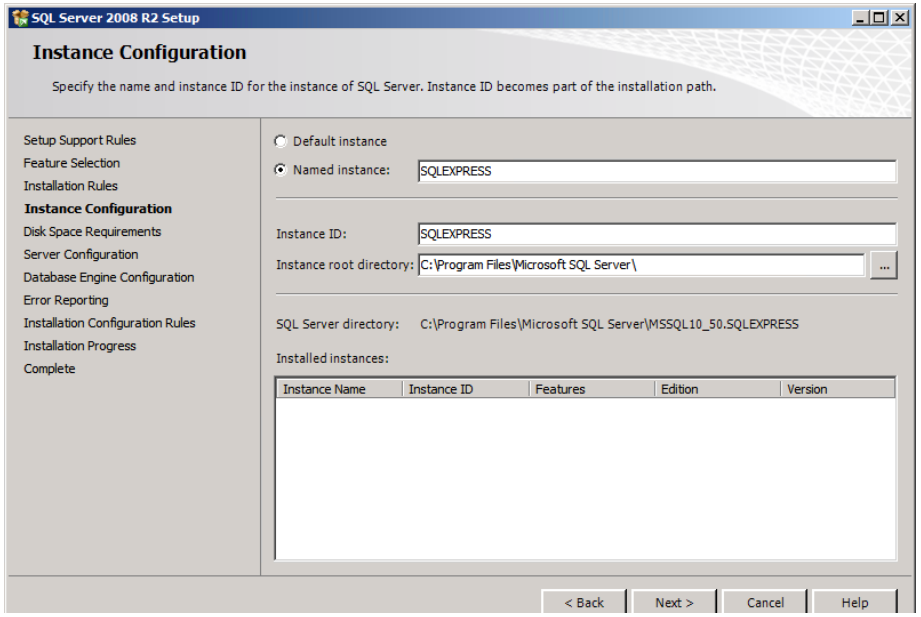
Step 9: From the VM console, cancel the installation by the AutoPlay service, navigate to the **D:\Support\SQLExpress2008R2\x64** folder on the ISO image, and then double-click the setup icon. The SQL Server 2008 R2 Setup wizard is displayed.

Step 10: Complete the SQL Server 2008 R2 Setup wizard. Note the following:

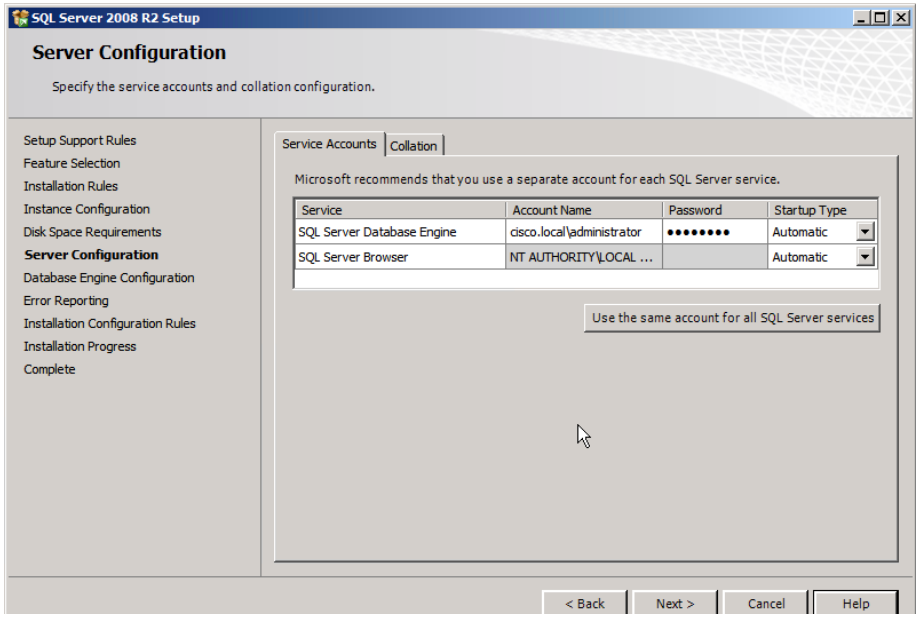
- On the License Terms page, accept the license terms, and then click **Next**.
- On the Feature Selection page, select all features, and then click **Next**.



- On the Instance Configuration page, verify **Named instance** is selected, keep the remaining SQL Express defaults, and then click **Next**.



- On the Server Configuration page, for both services, in the **Startup Type** list, choose **Automatic**, and then for the SQL Server Database Engine service, in the **Account Name** box, enter **cisco.local\administrator**.



- Complete the wizard by accepting the default values.

Step 11: Click **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **Configuration Tools** > **SQL Server Configuration Manager**. SQL Server Configuration Manager launches.

Step 12: In the tree, navigate to **SQL Server Network Configuration** > **Protocols for SQLEXPRESS**.

Step 13: Double-click **Named Pipes**.

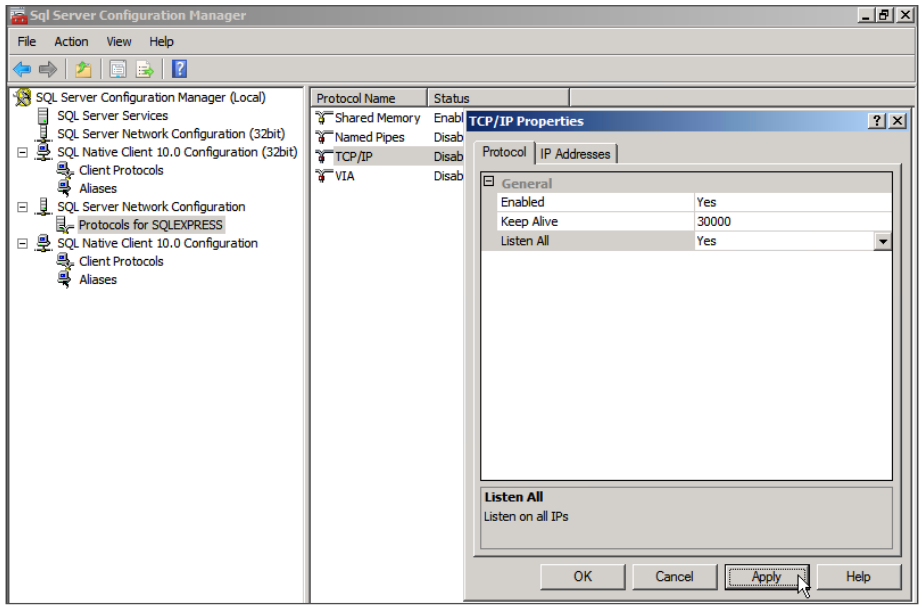
Step 14: On the Named Pipes Properties dialog box, next to Enabled, select **Yes**, and then click **Apply**.

Step 15: On the message about the changes made, click **OK**, and then click **OK** to close the dialog box.

Step 16: In the tree, navigate to **SQL Server Network Configuration** > **Protocols for SQLEXPRESS**.

Step 17: Double-click **TCP/IP**.

Step 18: On the TCP/IP Properties dialog box, on the Protocol tab, next to Enabled, select **Yes**, next to Listen All, choose **No**, click **Apply**.



Step 19: On the message about the changes made, click **OK**.

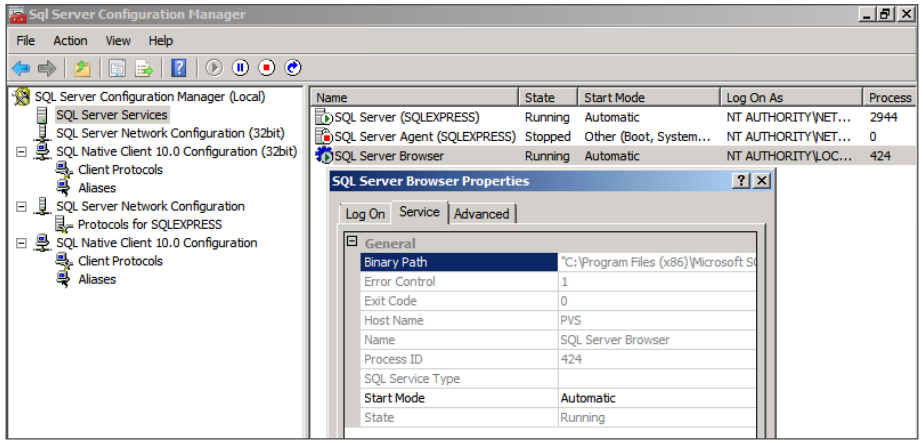
Step 20: Click the **IP Addresses** tab, locate the adapter with the active IP address, clear the **TCP Dynamic Port** box, in the **TCP Port** box, enter **1433**, and then click **OK**.

Step 21: On the message about the changes made, click **OK**, and then click **OK** to close the dialog box.

Step 22: In the tree, navigate to **SQL Server Services**, in the pane on the right side right-click **SQL Server**, and then click **Restart**. The SQL server restarts.

Step 23: In the tree, click **SQL Server Services**, right-click **SQL Server Browser**, and then choose **Properties**.

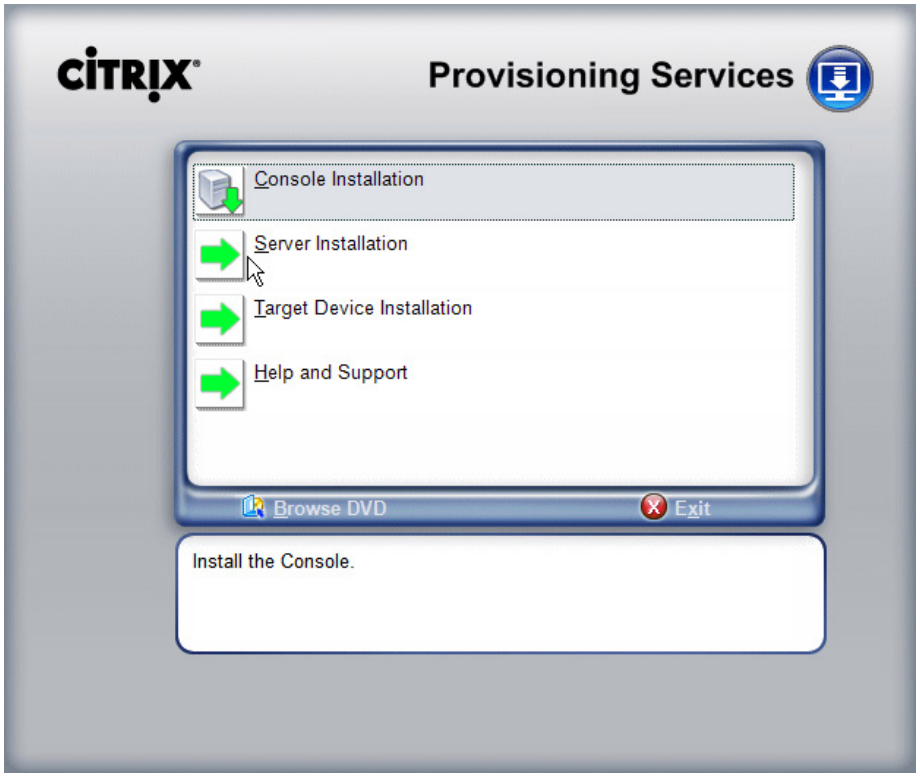
Step 24: On the SQL Server Browser Properties dialog box, click the **Service** tab, next to Start Mode, choose **Automatic**, and then click **OK**.



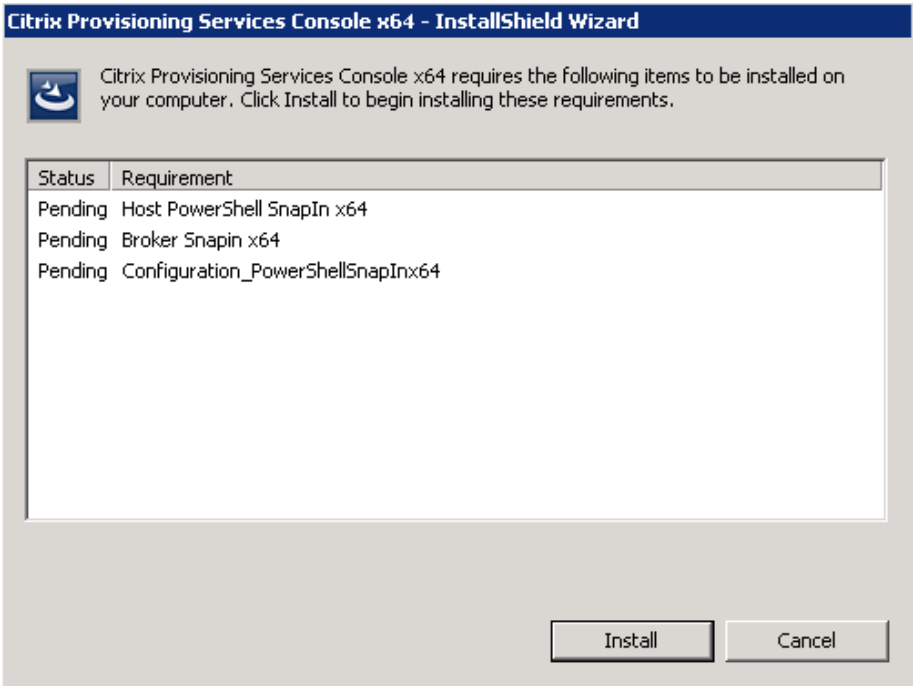
Step 25: Right-click **SQL Server Browser**, and then choose **Start**.

Step 26: Launch Windows Update, apply any updates found, and then repeat the check for updates until no updates remain. Because the installation adds Windows components, those components should be updated with the latest patches, usually requiring at least one reboot of the VM.

Step 27: In VMware vCenter, mount the Citrix PVS ISO image to the created H1-PVS virtual machine, and then allow the AutoPlay service to launch the installation. The Provisioning Services installation wizard is displayed.



Step 28: Select **Console Installation**, and then on the InstallShield Wizard dialog box, click **Install**.



Step 29: Complete the next three installation wizards for the Host PowerShell, Broker, and Configuration Snap-Ins, and note the following for each:

- Select **I accept the terms of the License Agreement**.
- Click **Install**.
- When the module installation is complete, click **Next**.

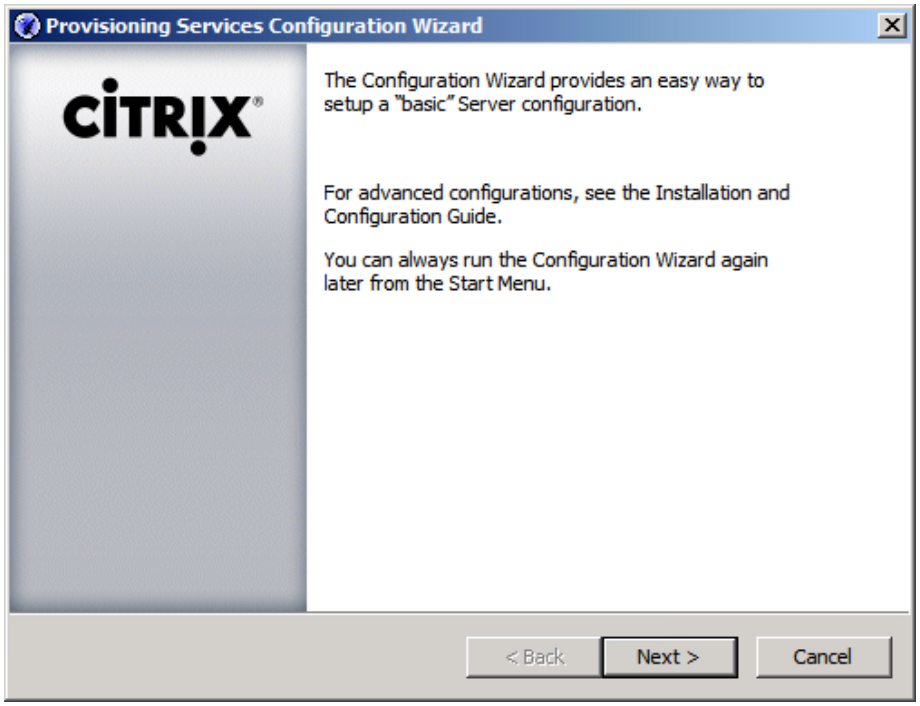
Step 30: At the prompt for Customer Information, in the **User Name** box, enter Administrator, and in the **Organization** box, enter SBA, and then click **Next**.

Step 31: Use all of the defaults in order to finish the installation of Provisioning Services Console.

Step 32: In the Provisioning Services installation wizard, select **Server Installation**, and then click **Install Server**.

Step 33: Accept all the default settings and prompts, accept the licensing agreement, in the **User Name** box, enter **Administrator**, and in the **Organization** box, enter **SBA**, and then complete the Provisioning Services server installation.

The Provisioning Services Configuration Wizard automatically launches.



Procedure 2 Configure Provisioning Services

Step 1: Open the console of the **H1-PVS** VM (Example: PVS.cisco.local). The Provisioning Services Configuration Wizard should be open.

If the Provisioning Services Configuration Wizard has been closed, restart it by selecting **Start > All Programs > Citrix, Provisioning Services > Provisioning Services Configuration Wizard**.

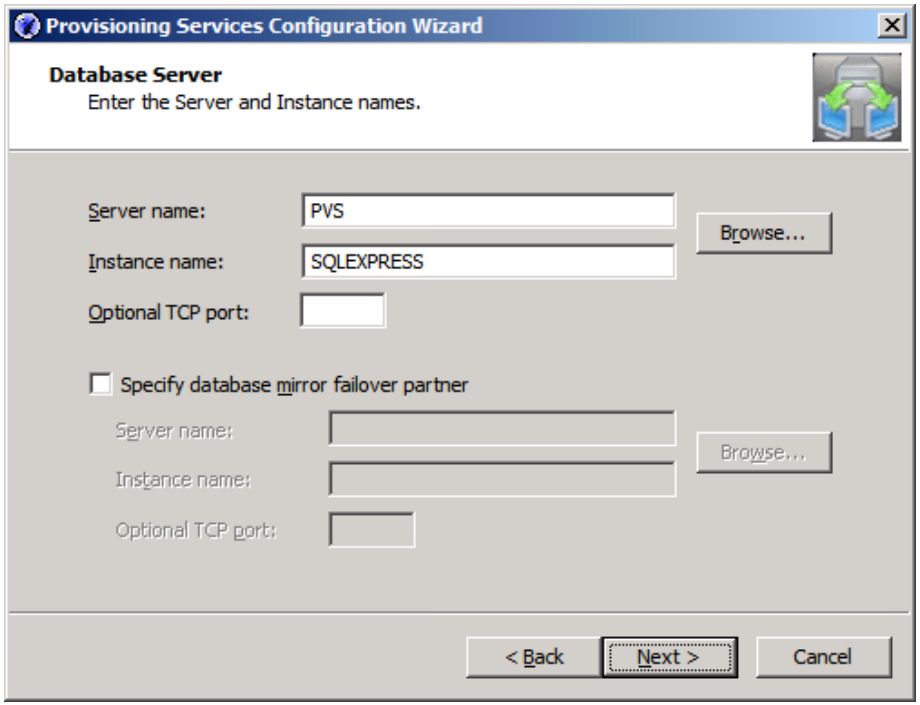
Step 2: On the introduction page, click **Next**.

Step 3: On the DHCP Services page, select **The service that runs on another computer**, and then click **Next**.

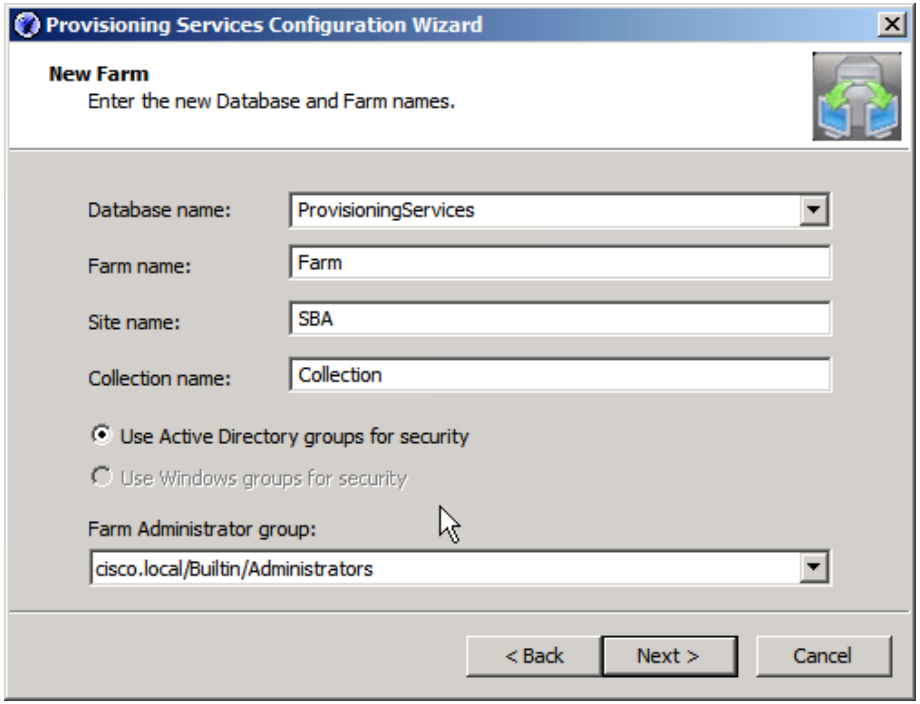
Step 4: On the PXE Services page, select **The service that runs on this computer**, select **Provisioning Services PXE service**, and then click **Next**.

Step 5: On the Farm Configuration page, select **Create farm**, and then click **Next**.

Step 6: On the Database Server page, in the **Server name** box, enter **PVS**, in the **Instance name** box, enter **SQLEXPRESS**, and then click **Next**.

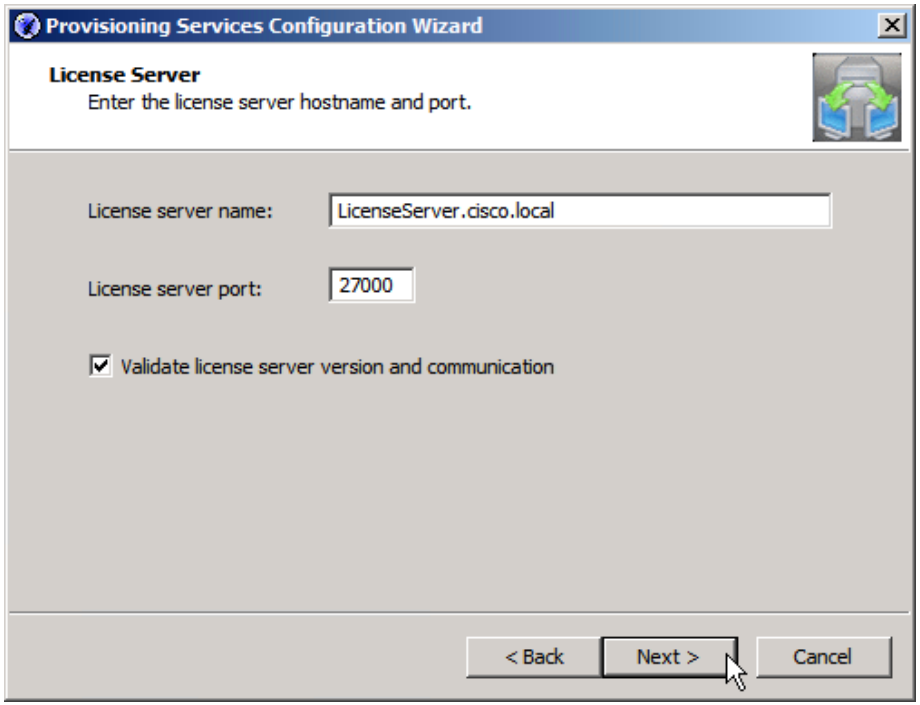


Step 7: On the New Farm page, in the **Site name** box, enter SBA, in the **Farm Administrator group** list, enter an Active Directory account with administration privileges (Example: cisco.local/Builtin/Administrators), and then click **Next**.

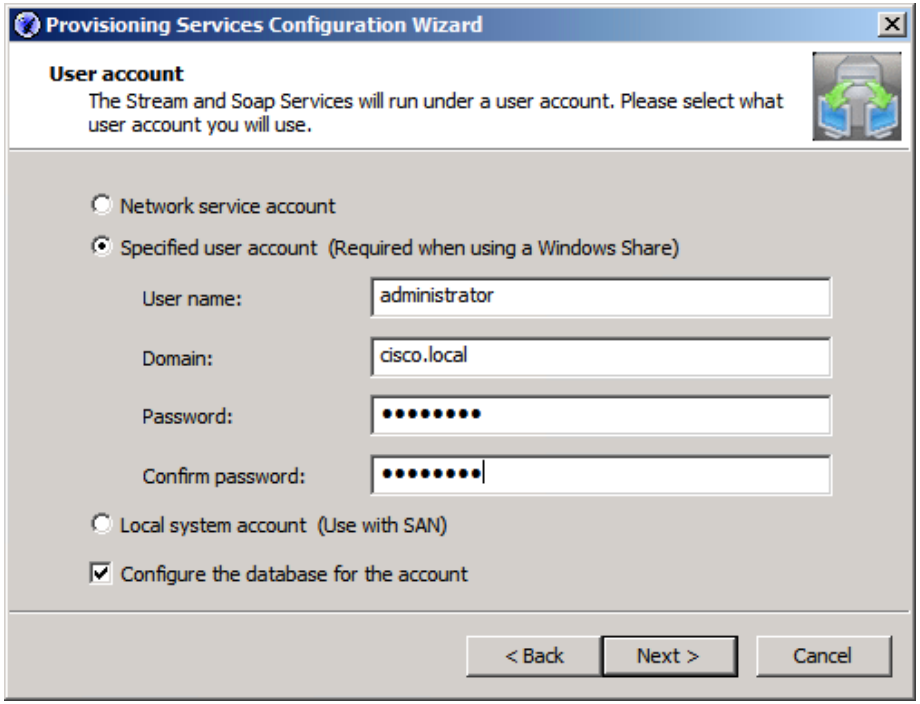


Step 8: On the New Store page, keep the default store name, use the **Browse** button to define and select a store that uses the second non-OS drive (Example: E:\Store), and then click **Next**.

Step 9: On the License Server page, in the **License Server Name** box, enter LicenseServer.cisco.local, select **Validate license server version and communication**, and then click **Next**.



Step 10: On the User account page, select **Specified user account (Required when using a Windows Share)**, enter the administrator username, domain, and password, select **Configure the database for the account**, and then click **Next**.

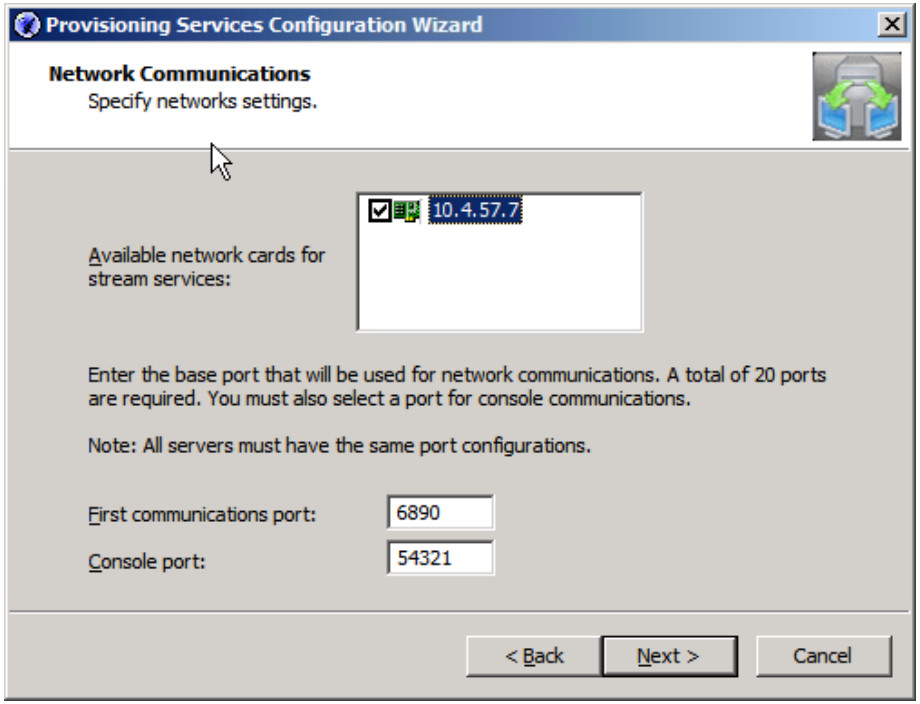


Tech Tip

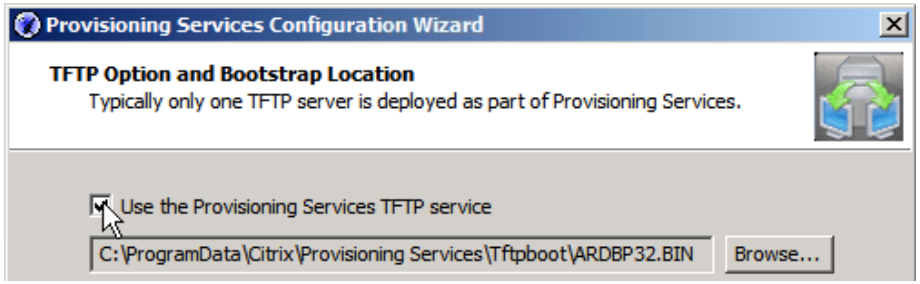
The account used in this step needs to have Active Directory creation privileges, or Citrix PVS is unable to create accounts to be associated with provisioned VMs, causing future procedures to fail.

Step 11: On the Active Directory Computer Account Password page, keep the default values, and then click **Next**.

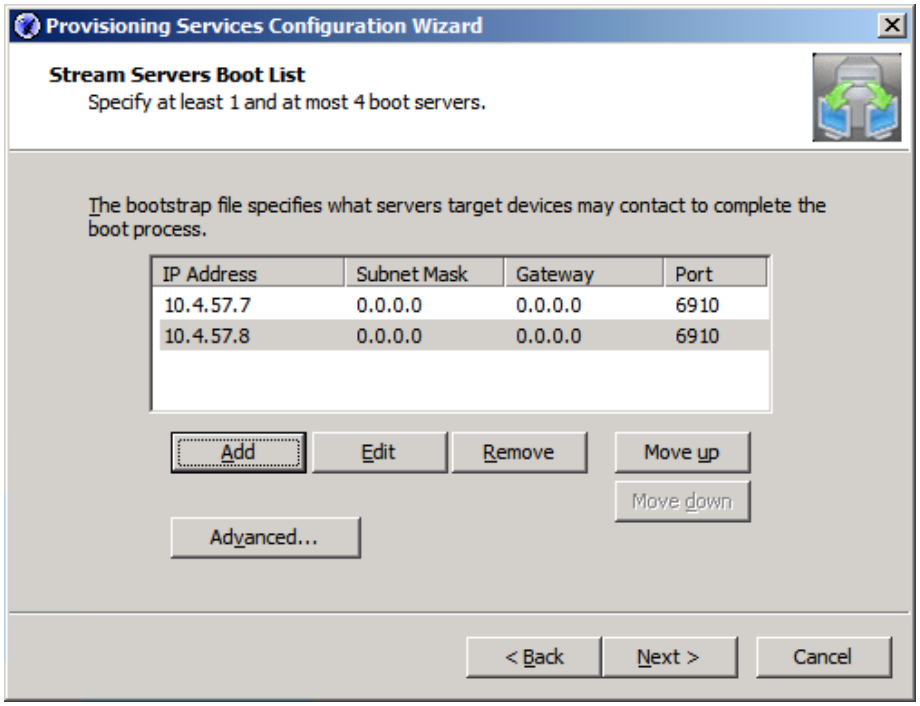
Step 12: On the Network Communications page, accept the default settings, and then click **Next**.



Step 13: On the TFTP Option and Bootstrap Location page, select **Use the Provisioning Services TFTP Service**, and then click **Next**.

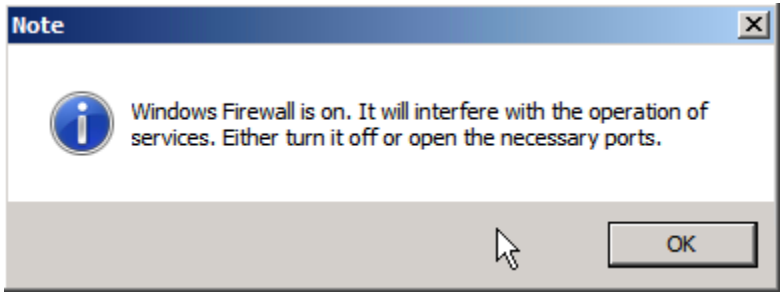


Step 14: On the Stream Servers Boot List page, click **Add**, update with 10.4.57.8, confirm the update, and then click **Next**. The Finish page is displayed.



Step 15: If you have Windows Firewall enabled, a "Windows Firewall is on" message appears. Do not select **OK**.

If you do not have Windows Firewall enabled and the message does not appear, skip to Step 17.



Step 16: In the Control Panel, open Windows Firewall, and then disable it for configuration and testing.

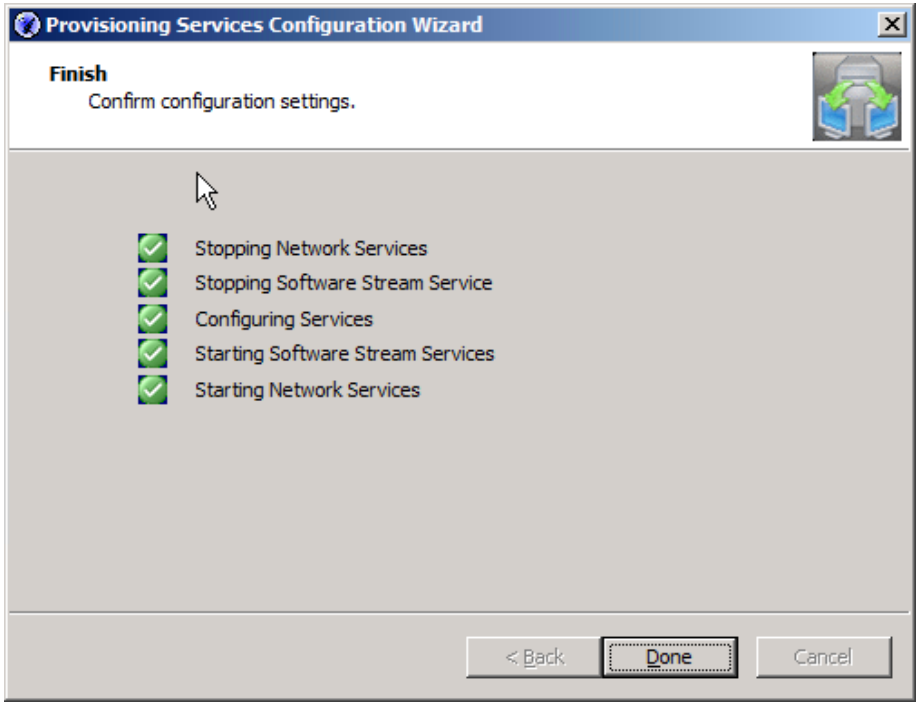
Tech Tip

Your deployment has specific firewall requirements for communications, which depends on features enabled. For more information, see the communications information at the Citrix website: https://support.citrix.com/servlet/KbServlet/download/2389-102-654859/CitrixPorts_by_Port_1103.pdf

Step 17: Return to the Provisioning Services Configuration Wizard, and if the Windows Firewall warning is still displayed, click **OK**.

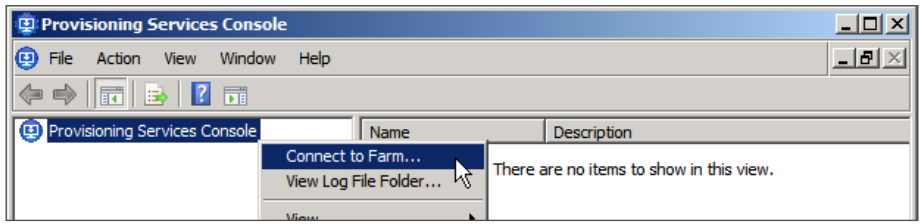
Step 18: On the Finish page, click **Finish**. A configuration status dialog box is displayed while the configuration wizard completes configuration tasks.

Step 19: When the configuration is complete, click **Done**.

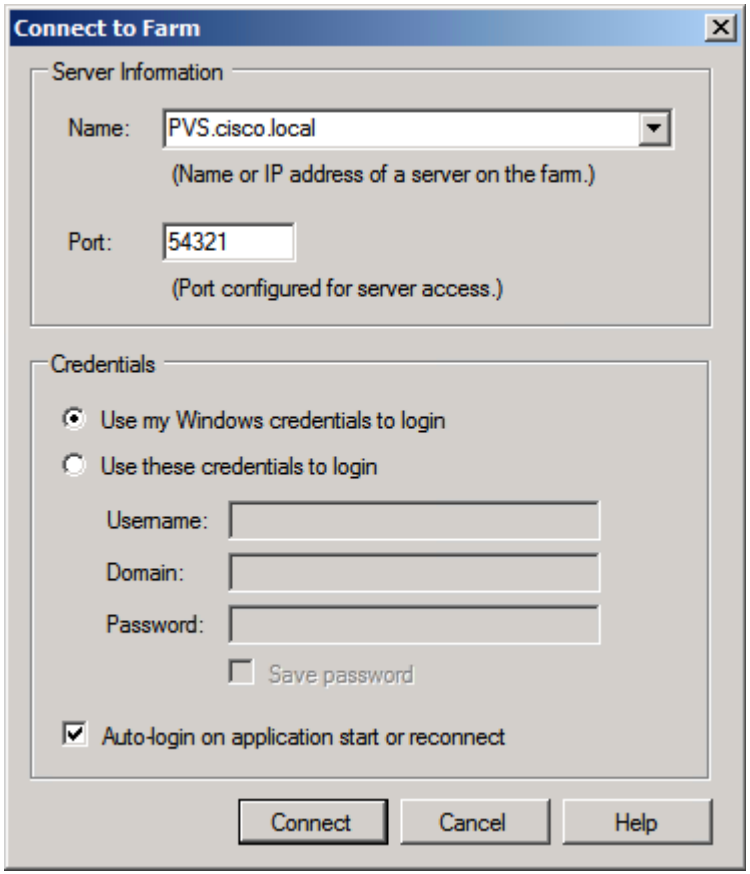


Step 20: Click **Start**, and then open the Provisioning Services Console.

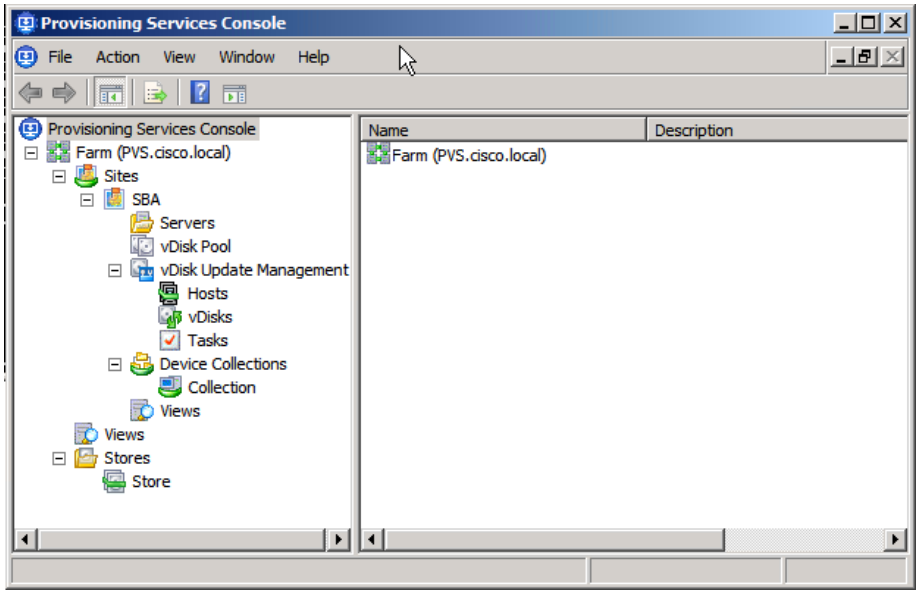
Step 21: In the tree, right-click on the **Provisioning Services Console** icon, and then choose **Connect to Farm**.



Step 22: On the Connect to Farm dialog box, in the **Name** box, enter PVS.cisco.local, keep the other default settings, select **Auto-login on application start or reconnect**, and then click **Connect**.



The newly created farm is displayed.



Procedure 3 Create a master Windows 7 desktop

Before you deploy and use Citrix PVS, a master Windows 7 desktop virtual machine is created on a host hypervisor in VMware vCenter, to be used as the source to create a vDisk and additional virtual desktops.

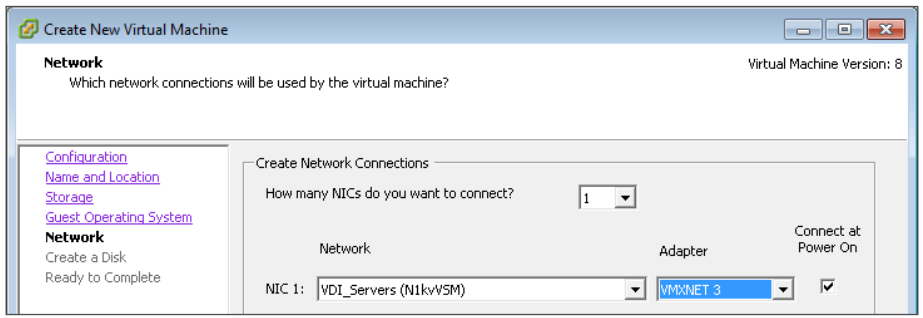
A Microsoft Windows 7 64-bit installation ISO must be available for mapping in the VMware vCenter management console in order to use the following steps successfully.

Step 1: Connect to VMware vCenter, and create a new Windows 7 64-bit master virtual machine by using the parameters in the following table.

Table 5 - Master Windows 7 configuration values for Cisco UCS server 3

Component	Parameter	Cisco SBA value
H3: Cisco UCS server 3	Name in VMware vCenter	chas3-s3
	IP address	10.4.63.113
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
Master Windows 7 64-bit VM	Name in VMware vCenter	H3-DesktopMaster
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	IP and DNS configuration	DHCP assigned
	DNS and Active Directory domain	cisco.local

It is important to configure the NIC with the VMXNET 3 option, as shown below, because the E1000 is unsupported with Citrix PVS on VMware vSphere 5.



Step 2: In VMware vCenter, in the H3-DesktopMaster virtual machine console, click **Edit Settings**, configure CD/DVD Drive 1 to be associated with the Windows 7 64-bit installation ISO image, select **Connect at power on**, and then click **Close**.

Step 3: Power on the virtual machine. The Install Windows wizard starts, and you can observe it in the VMware vCenter console window for the VM.

Step 4: Complete the installation wizard. Step-by-step details for the Windows installation are not covered, leaving installation options open for customization by the administrator.

After completing the new installation, the Windows desktop on the new guest VM is displayed.

Step 5: In VMware vCenter, right-click H3-DesktopMaster VM, choose **Guest**, and then click **Install/Upgrade VMware Tools**. The installation ISO image launches on the VM.

Step 6: Start the setup, take all defaults, run the installation program to completion, and allow rebooting of the server. VMware Tools are now installed, and the VM can now be fully managed from VMware vCenter.

Because VMware Tools applied the VXMNET 3 driver, the VM is now able to boot with a DHCP address, and you can update and configure it in order to join the Microsoft Active Directory domain.

Step 7: In the VM console, click **Start**, and in the search box, enter Windows Update, and then when **Windows Update** appears, press **Enter**.

Step 8: Apply all Windows updates available.

Step 9: If a reboot is required, reboot, and then check again for any Windows updates that are available. Repeat as needed until all important updates are applied.

Caution

Not applying the latest Windows patches may keep the VM from fully booting, and missing patches may cause other unexpected behavior.

Step 10: In the VM console, click **Start**, and in the search box, enter **domain**, and then when **Join a domain** appears, press **Enter**. The System Properties window is displayed.

Step 11: In the **Computer Description** box, enter VirtualDesk, and then click **Change**.

Step 12: Select **Domain**, enter cisco.local, and then click **More**.

Step 13: In the **Primary DNS Suffix** box, enter cisco.local, click **OK**, and then click **OK** again. Windows Security prompts for credentials for computer name or domain changes.

Step 14: For the cisco.local domain, in the **User name** box, enter administrator, enter the password, and then click **OK**. After the VM supplies the correct credentials and communicates with the Active Directory server, the "Welcome to the cisco.local domain" message is displayed.

Step 15: On the message, click **OK**. The VM is now joined to the cisco.local domain.

Step 16: Follow the instructions for applying the domain change and restarting the VM.

Step 17: Once the machine reboot is complete, in the H3-DesktopMaster VM console, log in, click **Start**, right-click **Computer**, choose **Properties**, click **Change product key**, and then enter your Windows group activation key. The Activate Windows window is displayed.

Step 18: Complete the information in order to activate Windows. You need to apply a Microsoft Volume Activation key to the VM, because duplicate keys exist on all replicated virtual machines.

Step 19: Install and configure any additional applications your organization desires to be available on the virtual desktop machines.

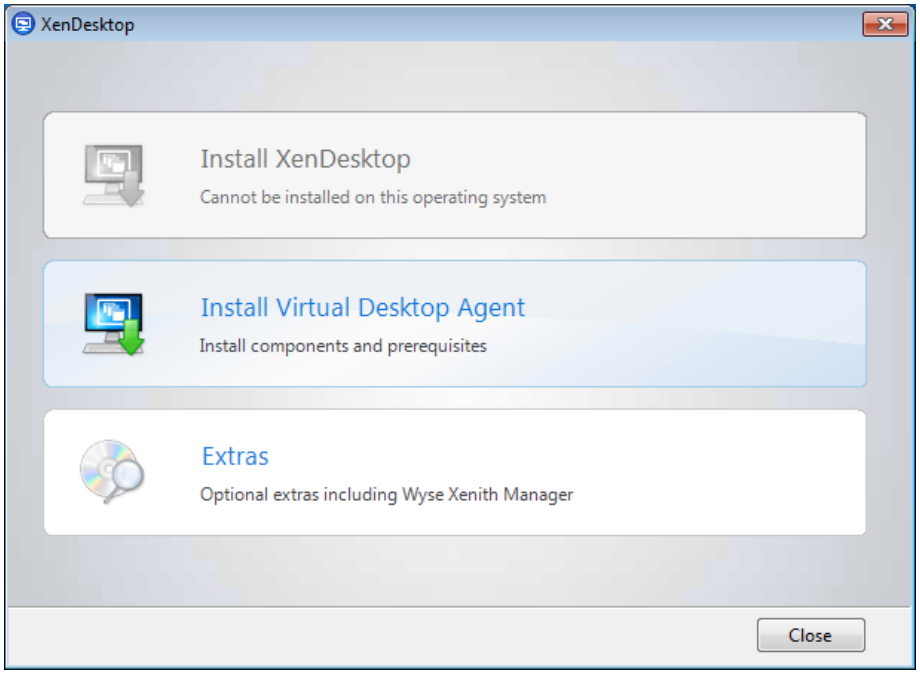
Step 20: It is not required that you manually configure Windows Firewall settings because they are addressed by the Citrix PVS installation.

Procedure 4 Install Virtual Desktop Agent (VDA)

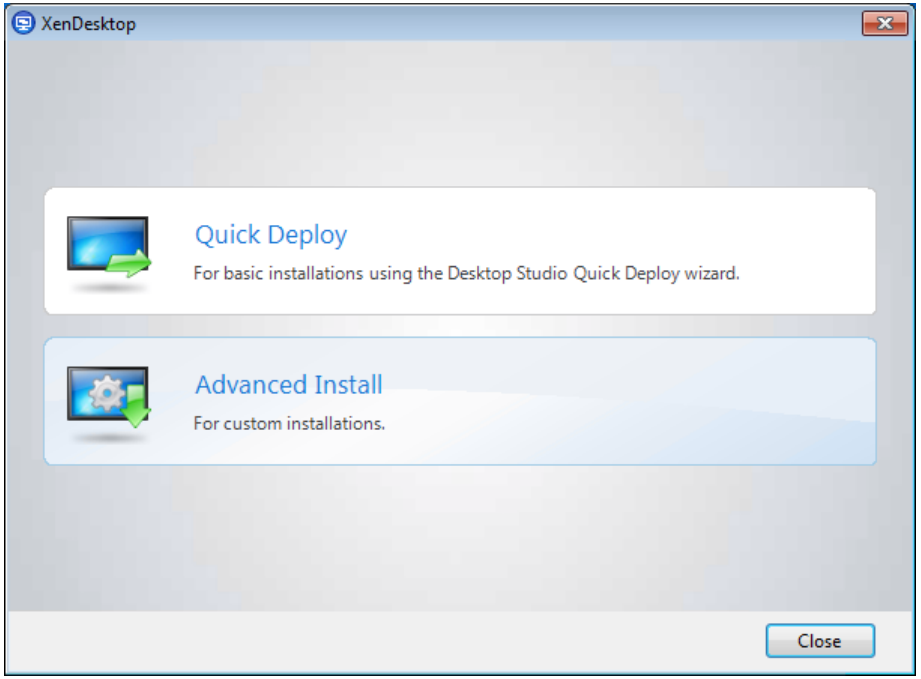
Citrix XenDesktop must be able to communicate with each VM that it controls, and the Virtual Desktop Agent tools must be a part of the Citrix PVS vDisk in order to enable the management functionality. You install the tools before the machine image is captured.

Step 1: In VMware vCenter, mount the Citrix XenDesktop ISO image to the H3-DesktopMaster VM, and then within the VM console, allow the AutoPlay service to launch the XenDesktop installer. The XenDesktop installation wizard opens.

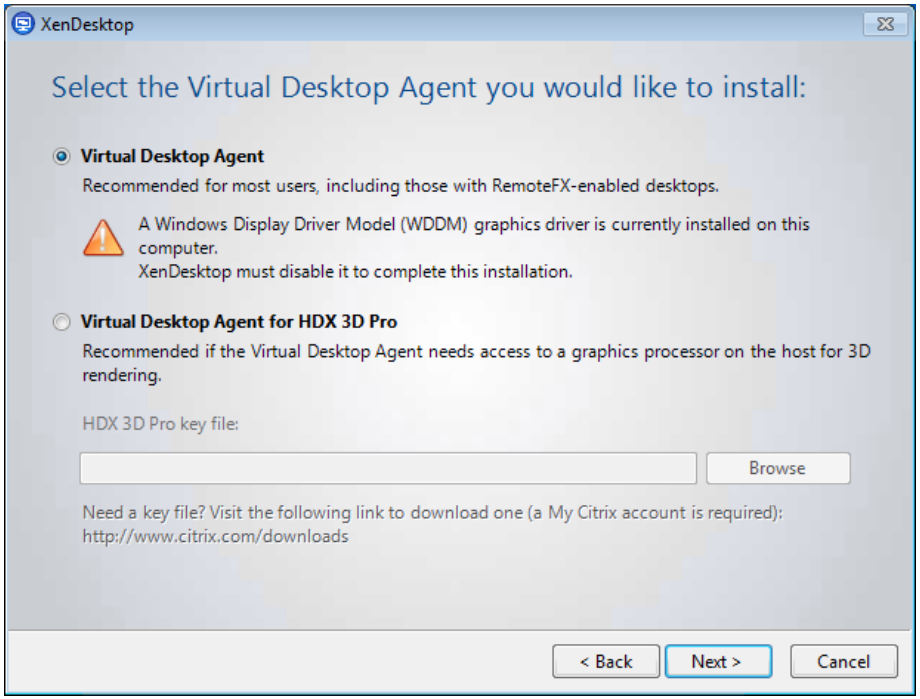
Step 2: Click **Install Virtual Desktop Agent**.



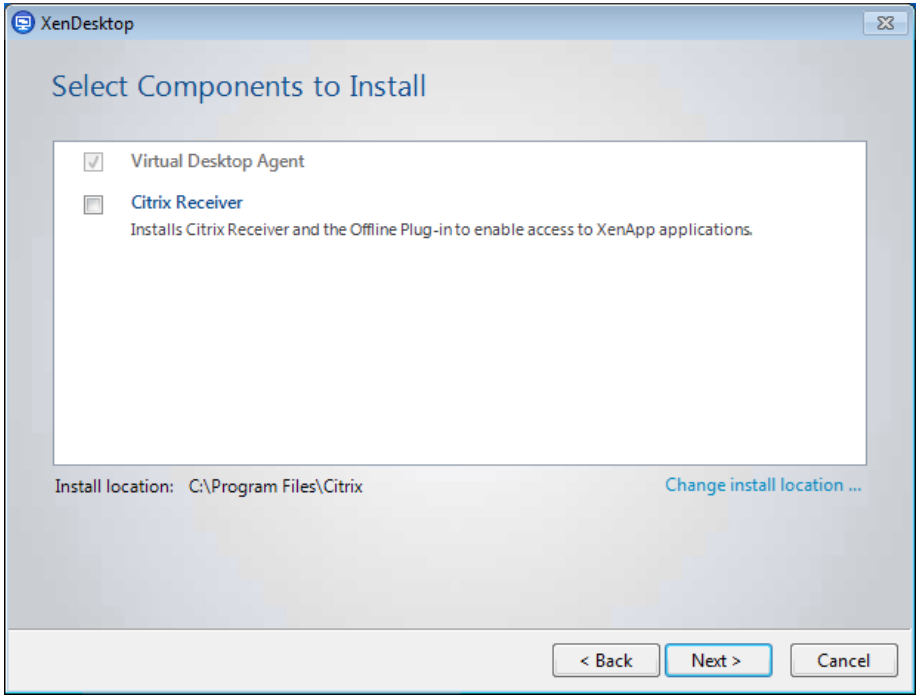
Step 3: Click **Advanced Install**, accept the license agreement, and then click **Next**.



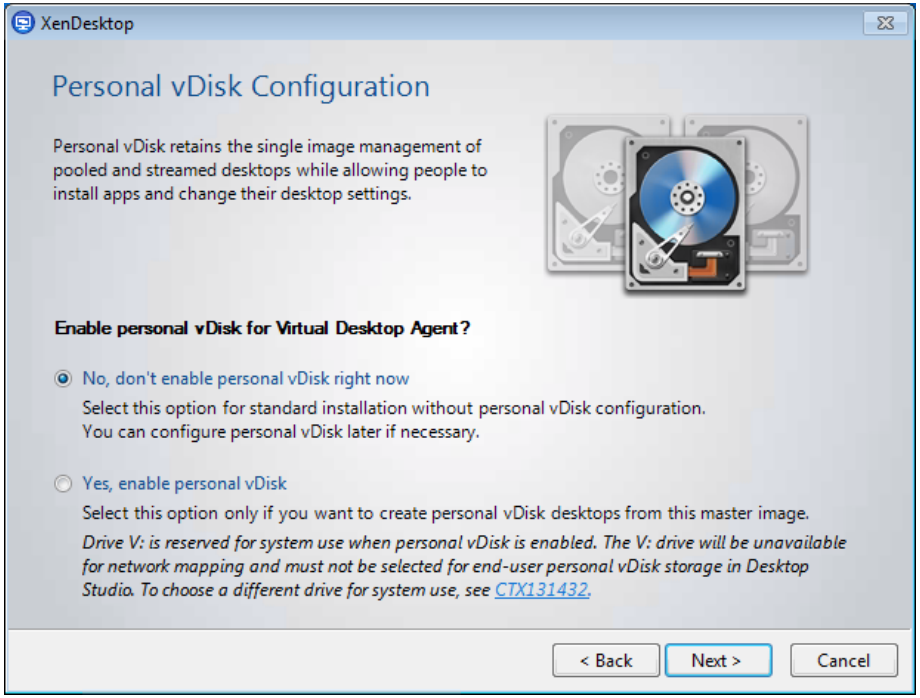
Step 4: On the Select the Virtual Desktop Agent you would like to install page, keep the default selection of **Virtual Desktop Agent**, and then click **Next**.



Step 5: On the Select Components to Install page, clear **Citrix Receiver**, and then click **Next**. If your deployment uses streamed applications to virtual desktops, the Citrix Receiver is used on the VM, and you can add the functionality when it is needed.

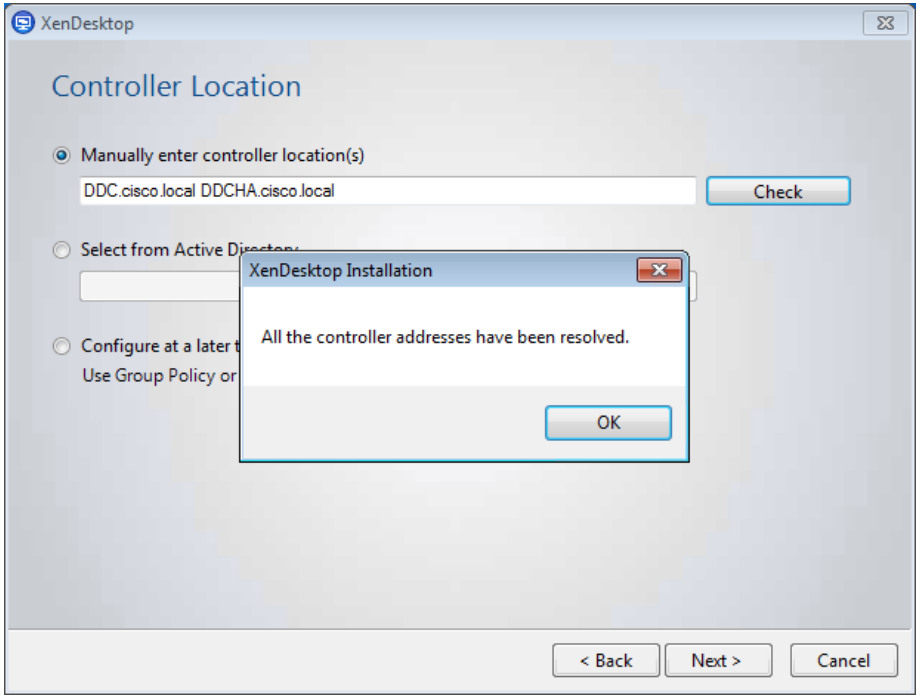


Step 6: On the Personal vDisk Configuration page, select **No, don't enable personal vDisk right now**, and then click **Next**.

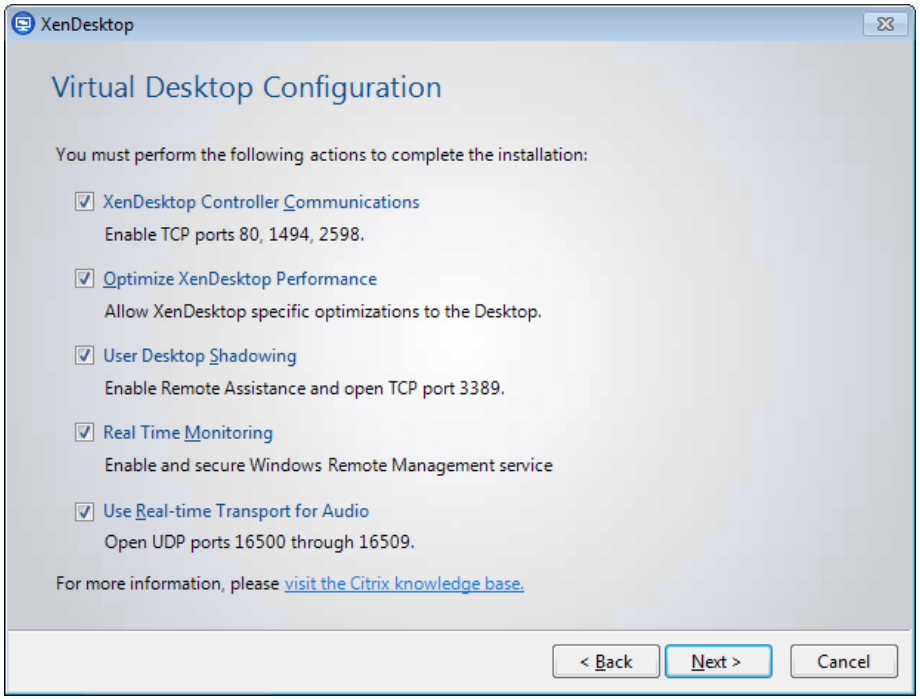


Step 7: On the Controller Location page, select **Manually enter controller location(s)**, enter the DNS names of the two Citrix XenDesktop servers, separated by a space (Example: DDC.cisco.local DDCHA.cisco.local), and then click **Check**.

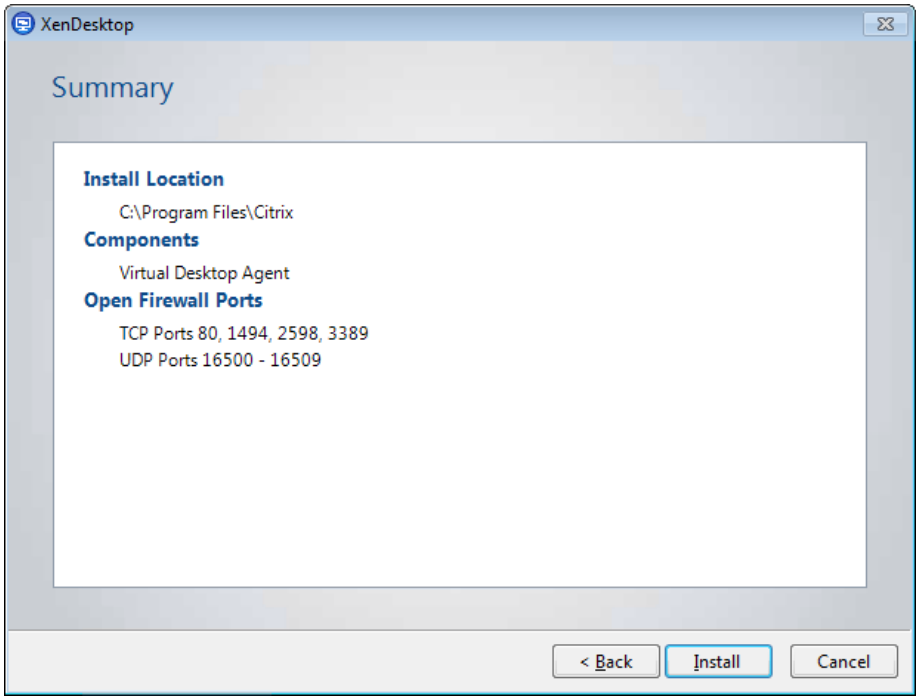
Step 8: On the "All the controller addresses have been resolved" message, click **OK**, and then on the Controller Location page, click **Next**.



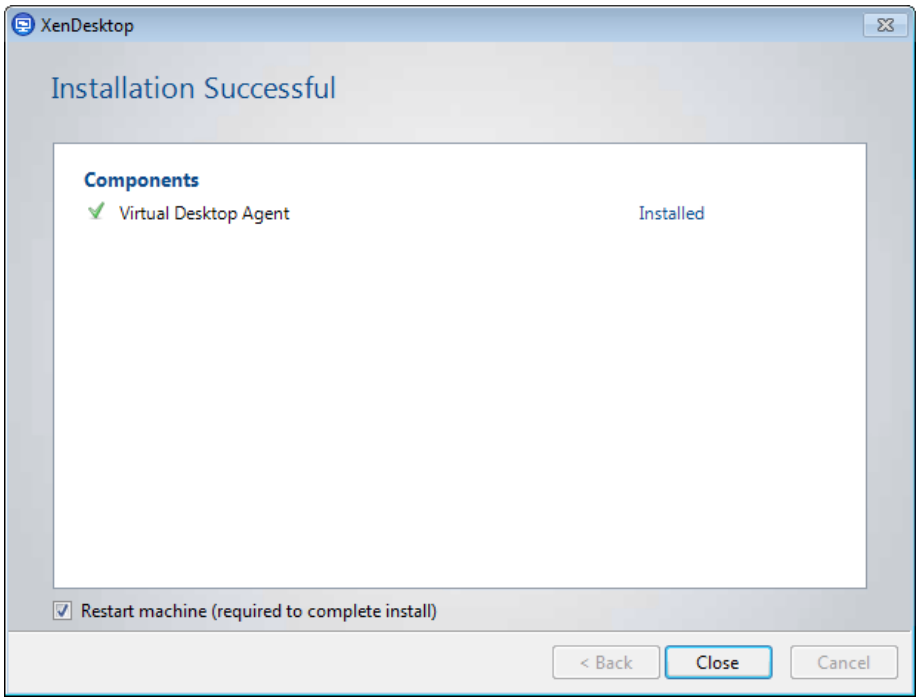
Step 9: On the Virtual Desktop Configuration page, click **Next**.



Step 10: On the Summary page, click **Install**.



Step 11: When the installation completes, click **Close**. H3-DesktopMaster restarts.

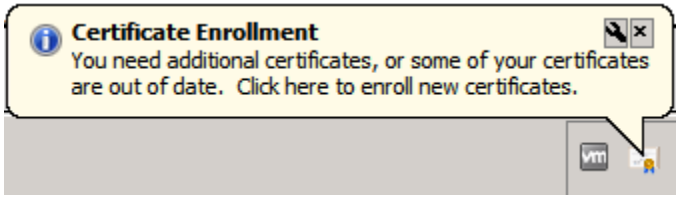


Procedure 5 Install Citrix PVS Target Device Software

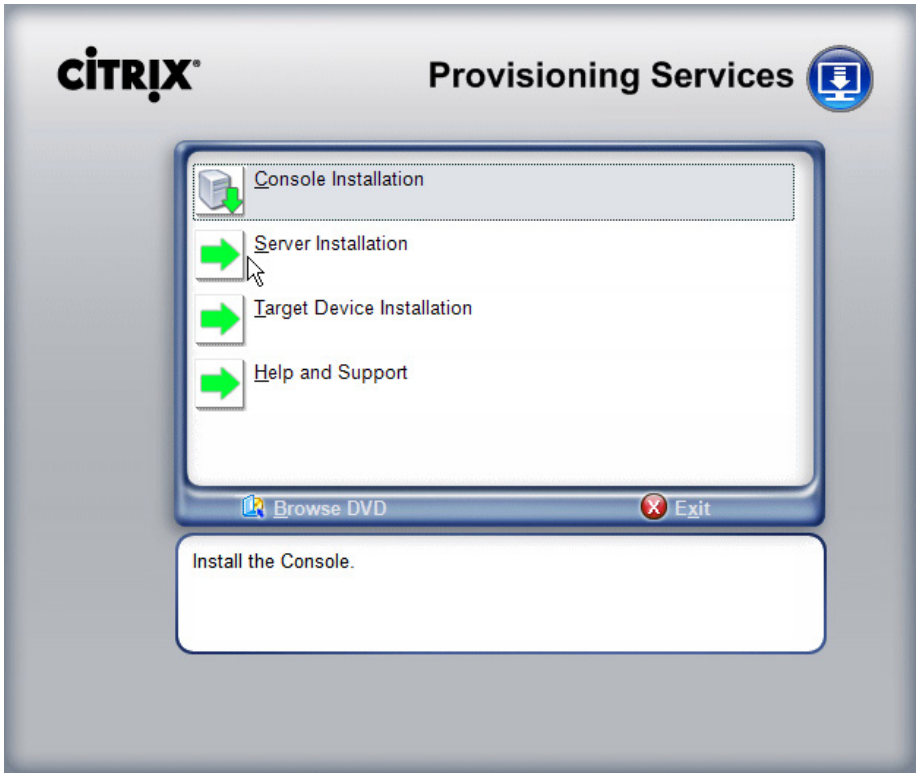
This deployment demonstrates streaming and access on a single network interface. For additional performance and scale, dual NICs can be created, allowing for segmentation of vDisk streaming on a non-routed VLAN, separate from the VLAN used for standard work communication with the VM.

Step 1: In VMware vCenter, using a domain account with administrator privileges (Example: cisco.local\administrator), log in to the console of H3-DesktopMaster VM.

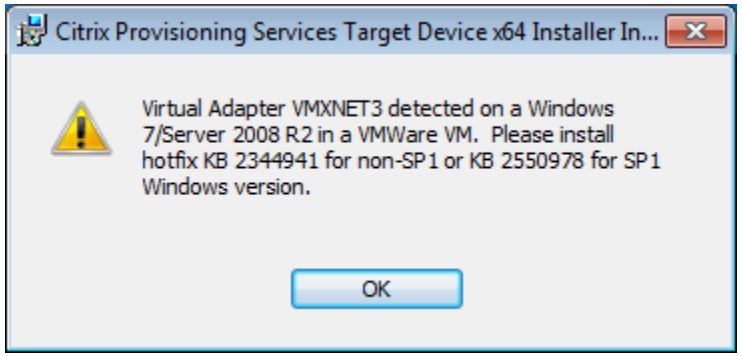
Step 2: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click the taskbar icon, and then complete the certificate enrollment.



Step 3: In VMware vCenter, connect the Citrix PVS ISO image to the H3-DesktopMaster virtual machine on Cisco UCS server 3, and then allow the AutoPlay service to launch the installation. The Provisioning Services installation wizard opens.



Step 4: Click **Target Device Installation**, and then on the new window that is displayed, click **Target Device Installation**. The installation launches, and then a message appears.



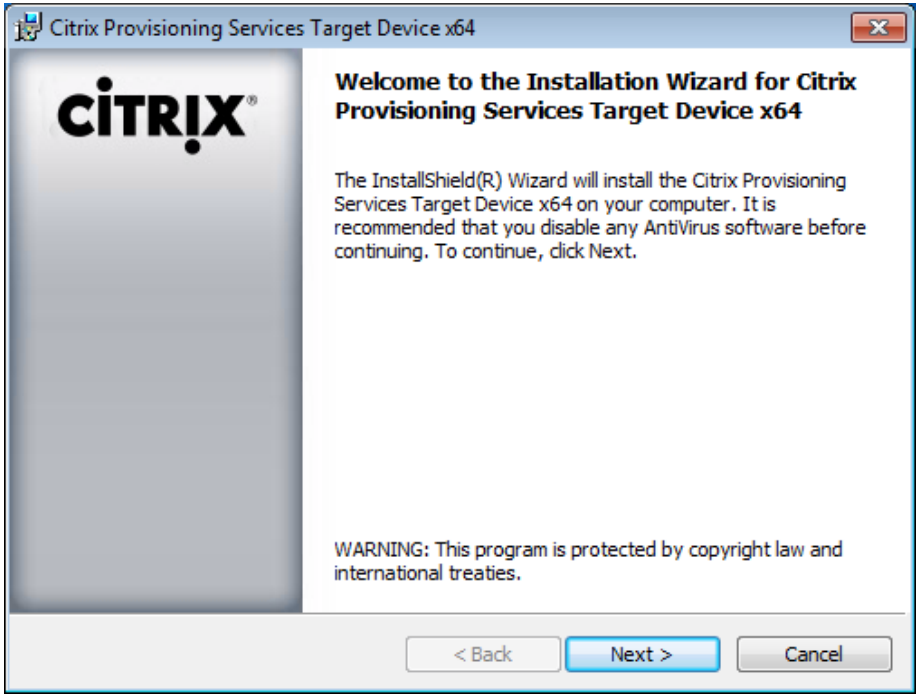
Step 5: Acquire the appropriate update from Microsoft (Example: 433809_intl_x64_zip.exe), and then apply the update, which may require temporarily enabling the Windows Update service. After applying, the VM restarts in order to finish applying the patch.

Step 6: In VMware vCenter, using a domain account with administrator privileges (Example: cisco.local\administrator), log in to the console of the H3-DesktopMaster VM.

Step 7: In VMware vCenter, reconnect the Citrix PVS ISO image to the H3-DesktopMaster on Cisco UCS server 3, and then allow the AutoPlay service to launch the installation. The Provisioning Services installation wizard is displayed.

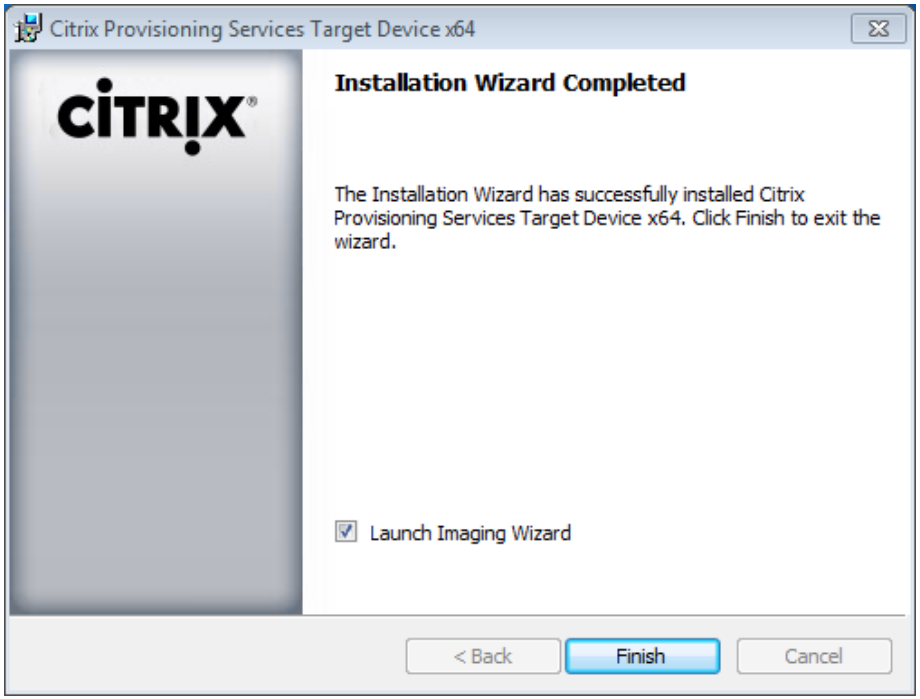
Step 8: Click **Target Device Installation**, and then on the new window that is displayed, click **Target Device Installation**.

With the Microsoft VMXNET 3 fix applied, the Installation Wizard for Citrix Provisioning Services Target Device automatically launches.



Step 9: Complete the wizard as follows:

- On the Welcome page, click **Next**.
- On the License Agreement page, accept the license.
- On the Customer Information page, click **Next**.
- On the Ready to Install the Program page, click **Install**.
- On the Installation Wizard Completed page, click **Finish**.



The Provisioning Services Imaging Wizard launches.

Do not continue with the Provisioning Services Imaging Wizard until you have completed Procedure 6.

Procedure 6 Remove any ghost network interfaces

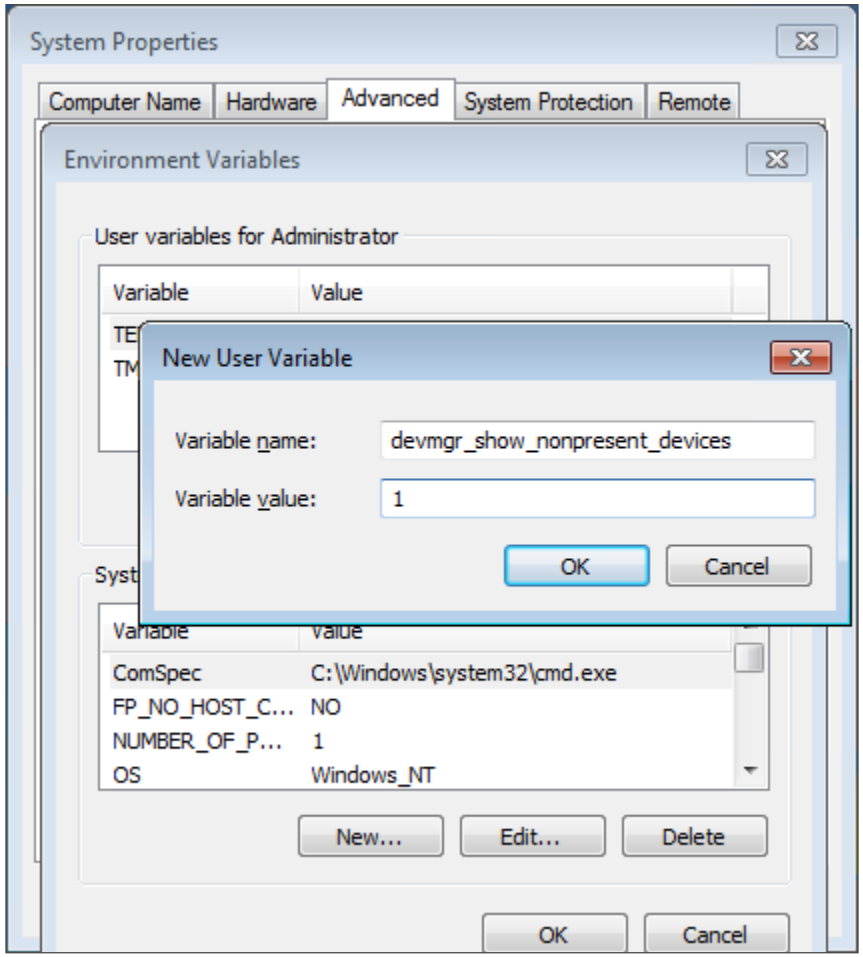
Depending on version of the Citrix PVS Target Device Software, the Provisioning Services Imaging Wizard may bind the vDisk created in the next procedure to a "ghost" network interface, if one exists. If this happens, you will not be able to successfully complete the vDisk creation. This procedure checks for any ghost drivers first, and it removes them if they exist in order to ensure successful vDisk creation.

Step 1: While logged into the H3-DesktopMaster VM with administrator credentials, click the Windows Start button, in the search box, enter **advanced system**, and then when the **View advanced system properties** option appears, press **Enter**.

Step 2: On the System Properties dialog box, on the Advanced tab, click **Environment Variables**.

Step 3: On the Environment Variables dialog box, under User Variables, click **New**.

Step 4: In the **Variable name** box, enter devmgr_show_nonpresent_devices, and in the **Variable value** box, enter 1, and then click **OK**.

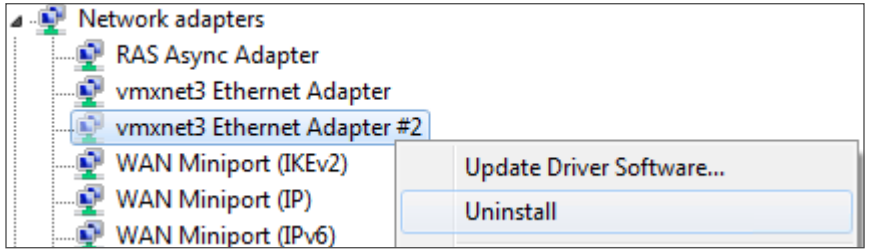


Step 5: On the Environment Variables dialog box, click **OK**, and then on the System Properties dialog box, click **OK**.

Step 6: Click the Windows **Start** button, in the search, enter **Device Manager**, and then when Device Manager appears, press **Enter**.

Step 7: From the **View** menu, choose **Show hidden devices**, then in the navigation tree, expand **Network adapters**.

Step 8: If any Ethernet adapter appears grayed out, signifying that it is not present, right-click the adapter, choose **Uninstall**, and then complete the device removal. Repeat for all Ethernet interface hardware that is not present.



Once no ghost Ethernet network interfaces exist, continue to the next procedure.

Procedure 7 Create and acquire master target vDisk

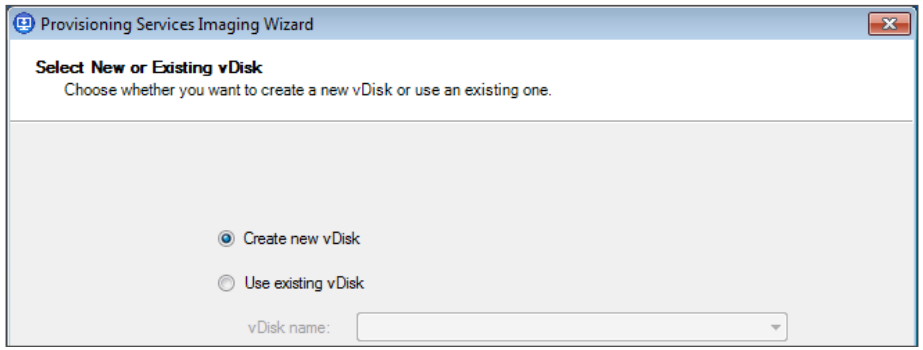
The H3-DesktopMaster VM is now enabled in order to begin the first stage of vDisk creation.

Step 1: If the Provisioning Services Imaging Wizard is not open, navigate to **Start** > **All Programs** > **Citrix** > **Imaging Wizard**.

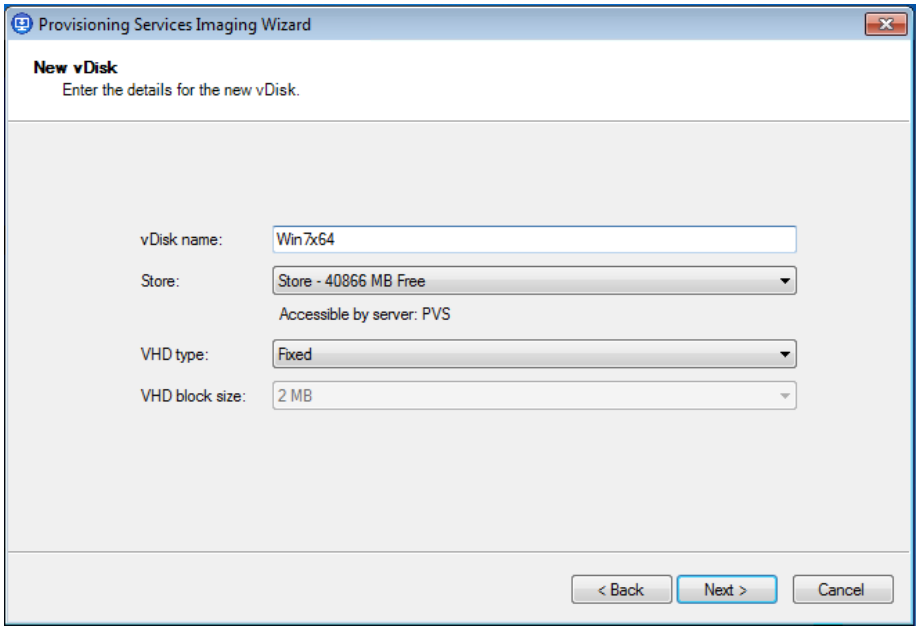
Step 2: On the Welcome page, click **Next**. Information for connecting to the farm is requested.

Step 3: On the Connect to Farm page, in the **Server** box, enter PVS, select **Use my Windows credentials**, and then click **Next**.

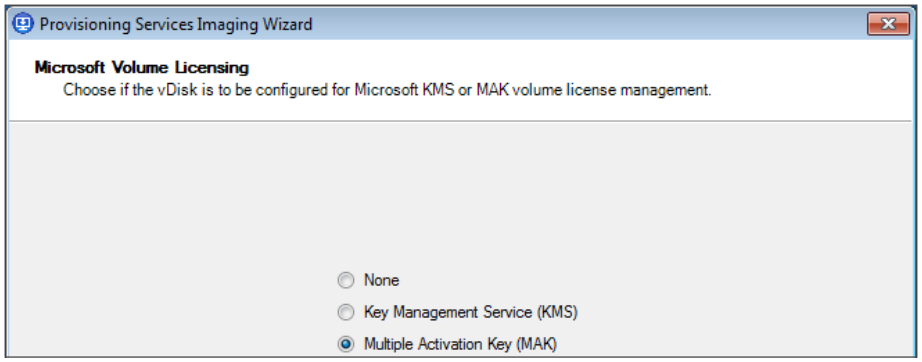
Step 4: On the Select New or Existing vDisk page, select **Create new vDisk**, and then click **Next**.



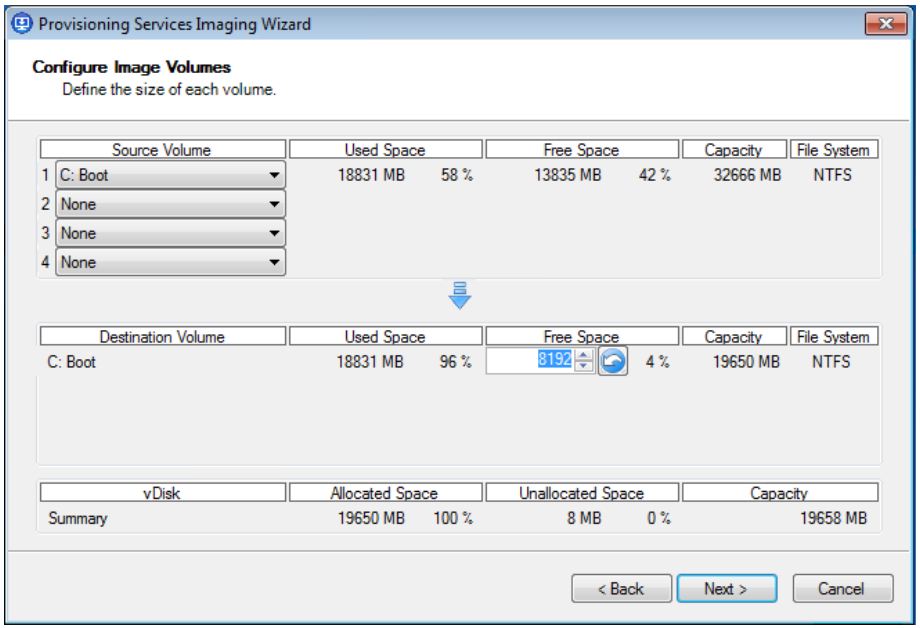
Step 5: On the New vDisk page, in the **vDisk name** box, enter Win7x64, keep the default value in the **Store** list, and in the **VHD type** list, choose **Fixed**, and then click **Next**.



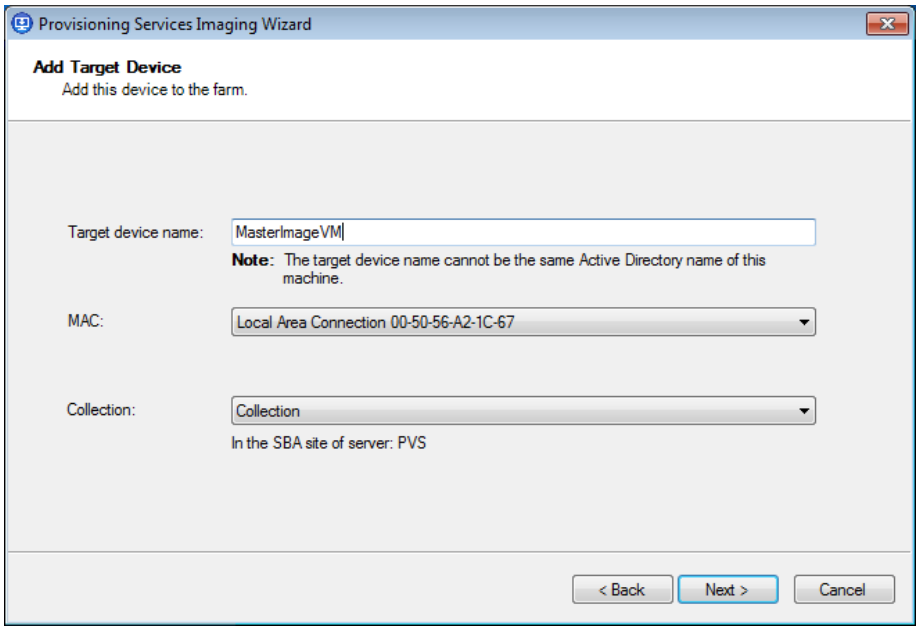
Step 6: On the Microsoft Volume Licensing page, select **Multiple Activation Key (MAK)**, and then click **Next**.



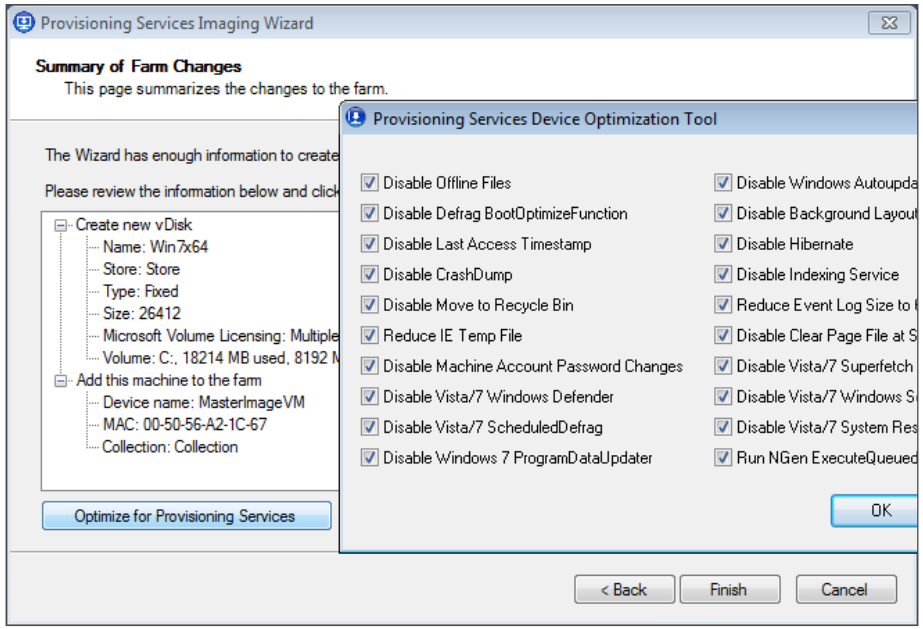
Step 7: On the Configure Image Volumes page, in the **Free Space** box, enter approximately 8192 MB, keep the other values, and then click **Next**.



Step 8: On the Add Target Device page, in the **Target device name** box, enter MasterImageVM, leave the other default values, and then click **Next**.

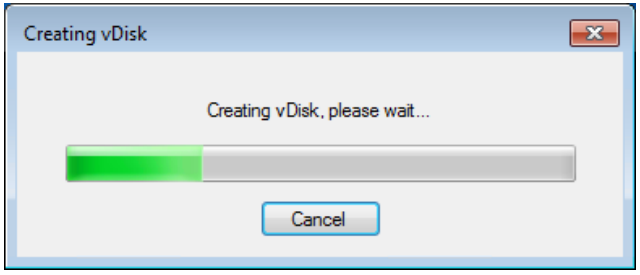


Step 9: On the Summary of Farm Changes page, click **Optimize for Provisioning Services**, and then on the Provisioning Services Device Optimization Tool dialog box, click **OK**.

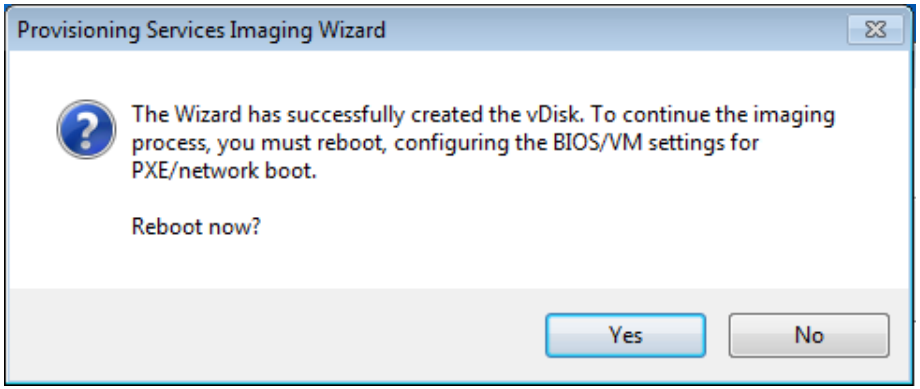


The wizard optimizes the Windows setup and then returns to the Summary of Farm Changes page.

Step 10: Click **Finish**. The Creating vDisk dialog box displays the status of the configuration.



When the image creation is complete, a reboot request message appears.

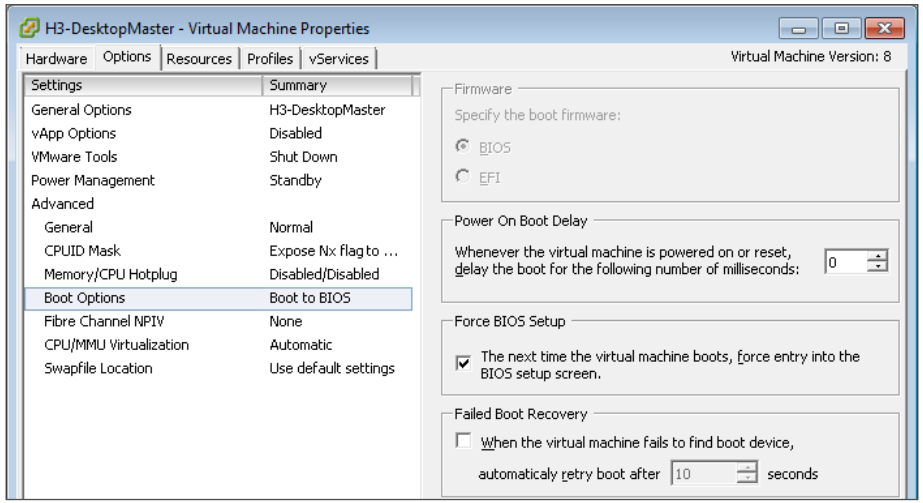


Do not make a selection yet. Before you continue, be aware that during the reboot process, it is necessary to reconfigure the VM BIOS to boot from the network by using PXE boot services. To change the BIOS, you use VMware vCenter in order to force booting into the BIOS configuration utility.

Step 11: In VMware vCenter, right-click the H3-DesktopMaster VM, and then choose **Edit Settings**.

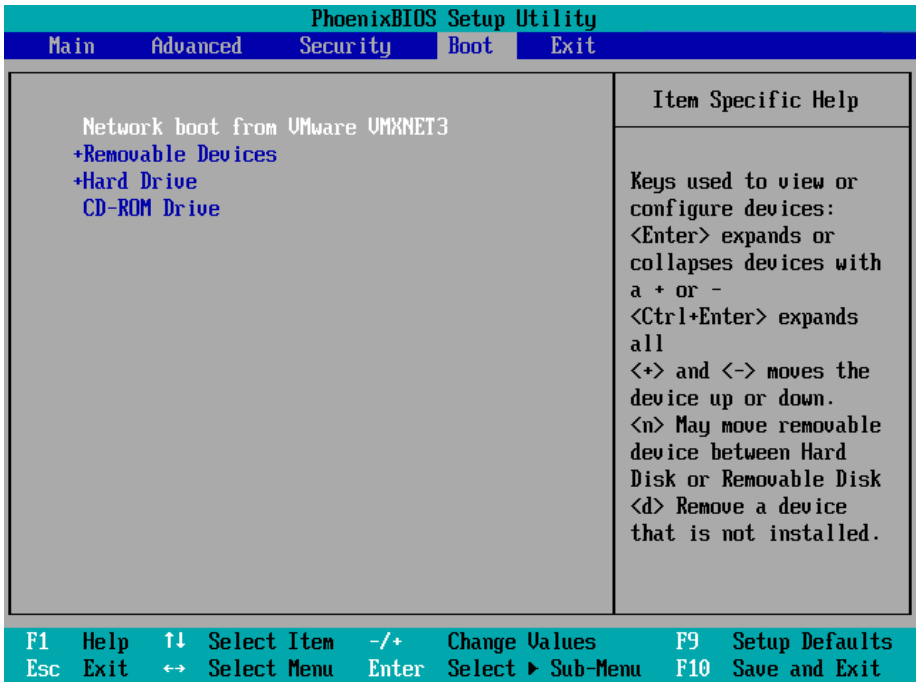
Step 12: On the H3-DesktopMaster - Virtual Machine Properties dialog box, on the Hardware tab, for **CD/DVD drive 1**, clear **Connected**.

Step 13: Click the **Options** tab, under the Advanced category, select **Boot Options**, and in the Force BIOS Setup pane, select **The next time the virtual machine boots, force entry into the BIOS setup screen**, and then click **OK**.



Step 14: Return to the H3-DesktopMaster VM console, and then on the "Reboot now" message, click **Yes**. The VM reboots and enters the PhoenixBIOS Setup Utility.

Step 15: Navigate to the **Boot** tab, move **Network boot from VMware VMXNET3** to the top of the list, and then press **F10**.



Step 16: Press **Enter**. This confirms and saves the changes. The virtual machine reboots from the network, with access to the vDisk for creating the initial vDisk image.

```
Network boot from VMware VMXNET3
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 50 56 A2 1C 67  GUID: 4222F569-413F-53C7-2C9C-56053F9043B2
CLIENT IP: 10.4.57.64  MASK: 255.255.255.0  DHCP IP: 10.4.48.10
GATEWAY IP: 10.4.57.1
```

Tech Tip

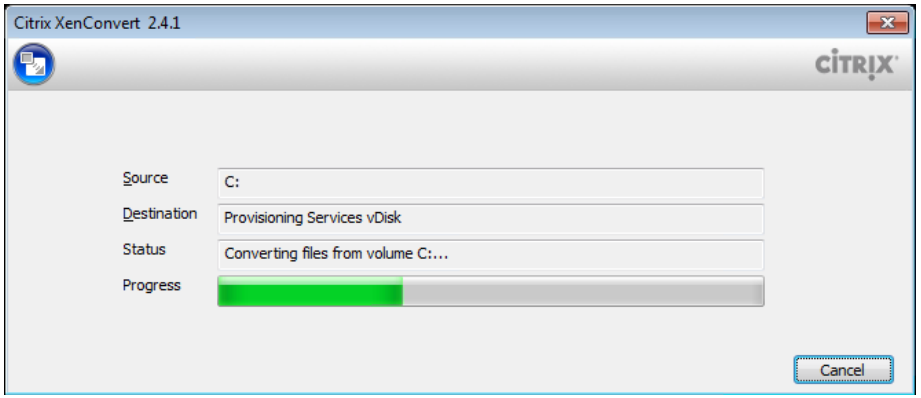
If the virtual desktops are on a different broadcast domain from the Citrix PVS servers that are running the BNPXE.exe PXE boot service, then a network boot is possible by updating the DHCP server servicing the VDI VLAN with the following two options:

Option 66, **Boot Server Host Name** = 10.4.57.7

Option 67, **Bootfile Name** = ARDBP32.BIN

These options allow the booting VM in the DHCP scope to find a boot server beyond the local subnet. You can also use a DNS host name and then configure DNS round-robin with multiple IP addresses for additional resiliency. There are other alternatives, but none are required if the virtual desktops share the broadcast domain with the Citrix PVS servers, any of which can service the boot requests with resilient service.

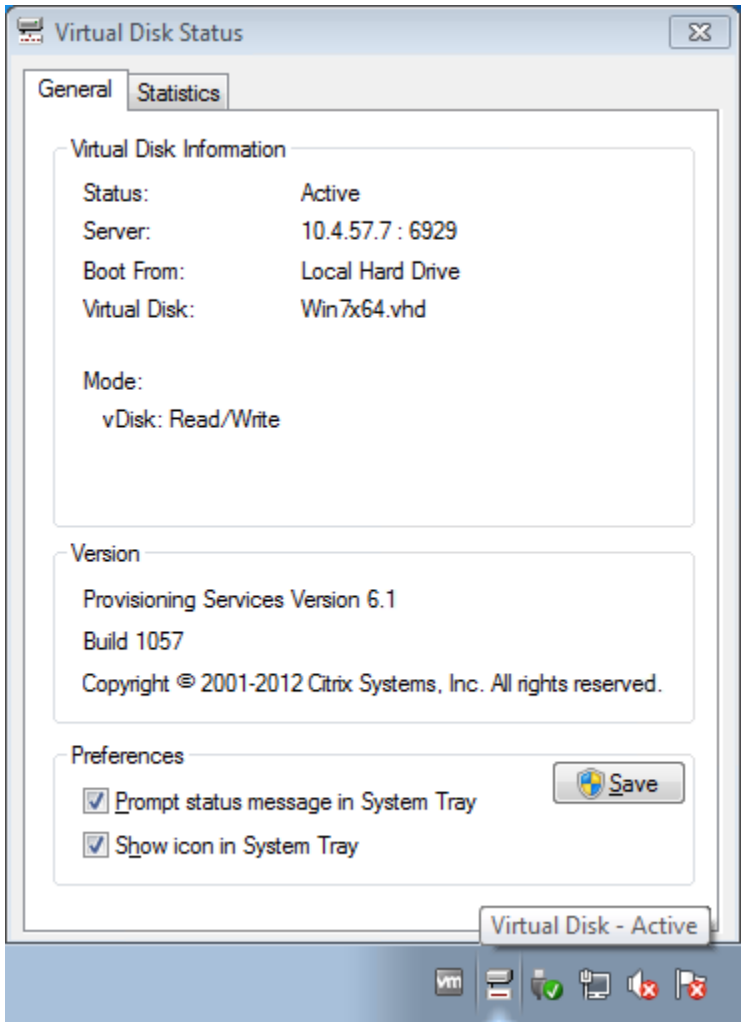
Step 17: After booting of the H3-DesktopMaster VM is complete, log in using domain administrator credentials. Because the virtual machine is network-booted, connectivity to the H1-PVS VM for vDisk creation is available, and the XenConvert utility automatically launches upon login, initiating the second stage of vDisk creation.



The conversion of the OS and all files on the VM C: drive into a Citrix PVS vDisk takes place. This process takes many minutes to complete.

Step 18: When complete, click **Finish**. The XenConvert utility closes.

Step 19: In the taskbar, click the Virtual Disk icon. Validate H3-DesktopMaster has an active vDisk.



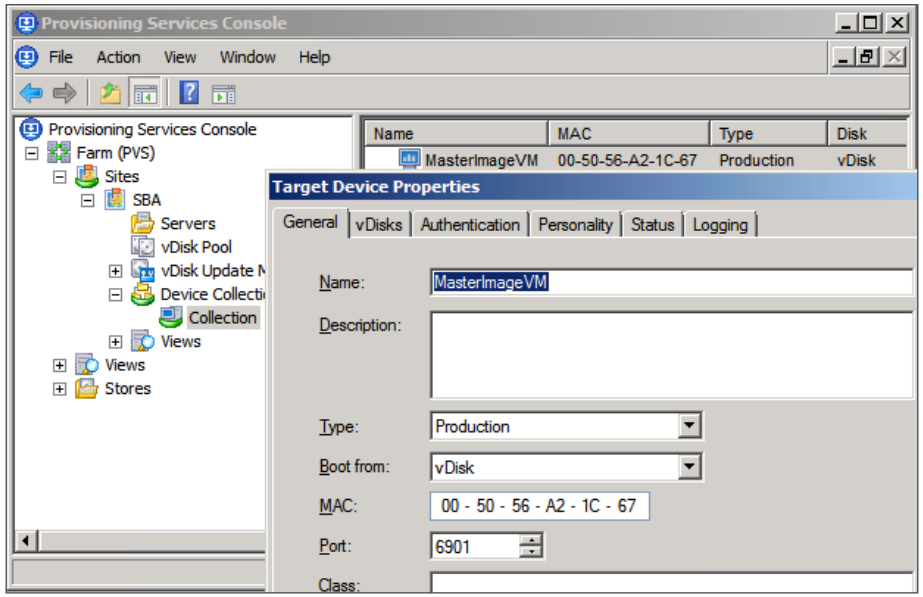
Step 20: Start a proper shutdown of the H3-DesktopMaster VM. The shutdown releases the lock that is engaged on the vDisk while the VM is running.

Step 21: Return to the console of the H1-PVS VM, open the Provisioning Services Console, navigate to **Farm** > **Sites** > **SBA** > **Device Collection** > **Collection**.

Step 22: From the **Action** menu, choose **Refresh**.

Step 23: Select the newly created virtual machine that appears (Example: MasterImageVM), right-click the virtual machine, and then choose **Properties**.

Step 24: On the Target Device Properties dialog box, in the **Boot from** list, choose **vDisk**, and then click **OK**.

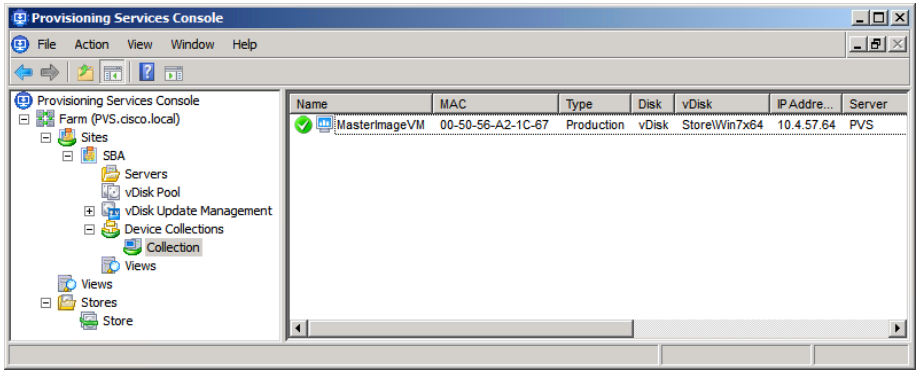


The PVS service on the H1-PVS VM directs the H3-DesktopMaster VM to boot from the vDisk instead of the C:\ drive on the H3-DesktopMaster VM. This configuration is used as an initial test of functionality.

Step 25: In VMware vCenter, power on the H3-DesktopMaster VM. From the VM console, observe that the VM completes a network boot and the OS now loads from the vDisk assigned by the H1-PVS VM to the H3-DesktopMaster VM by its MAC address.

Step 26: Return to the H1-PVS VM, and within the Provisioning Services Console navigate to **Farm** > **Sites** > **SBA** > **Device Collections** > **Collection**.

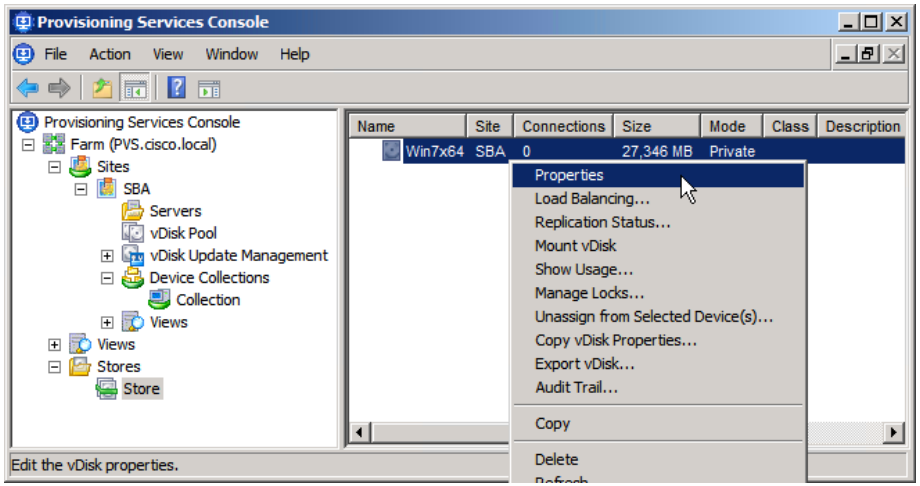
Step 27: From the **Action** menu, choose **Refresh**. The Provisioning Services Console shows the MasterImageVM VM within **Collection** as in use.



The vDisk generated for the master image is now available in the collection, but it is in private mode by default, which means that it cannot be shared with additional VMs.

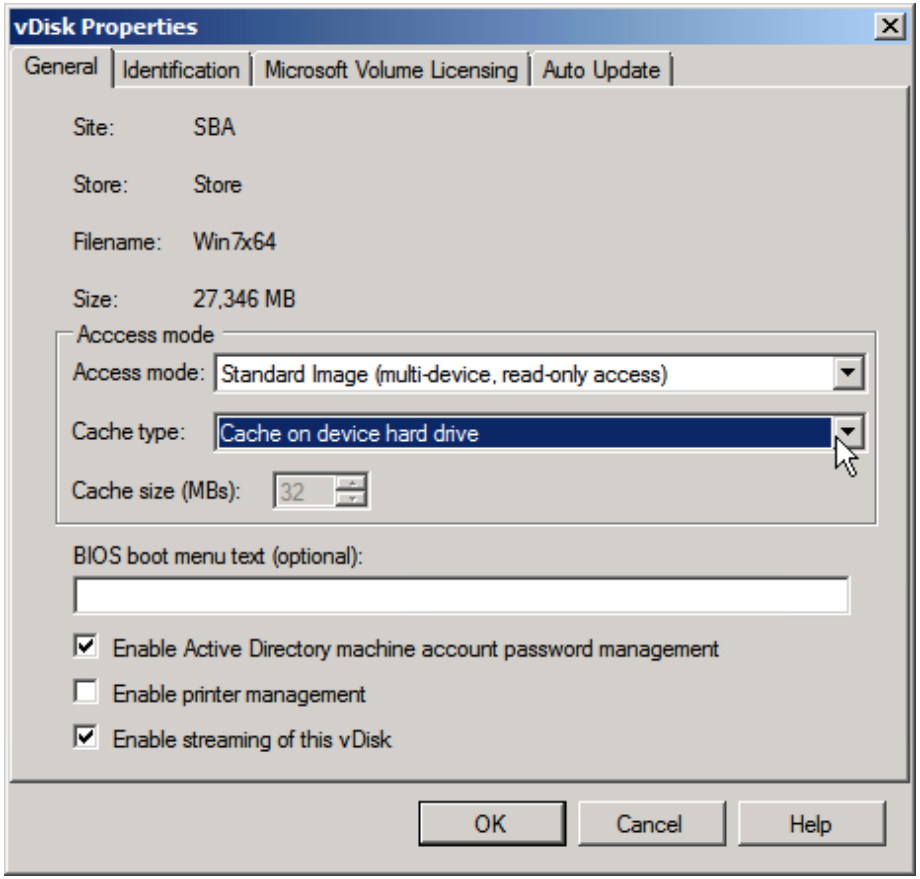
Step 28: Start a proper shutdown of the H3-DesktopMaster VM. The shutdown releases the lock that is engaged on the vDisk while the VM is running, which gives you permission to change the mode.

Step 29: Once the shutdown is complete, in the Provisioning Services Console, navigate to **Farm > Stores > Store**, select the **Win7x64** vDisk, right-click it, and then choose **Properties**.



The vDisk Properties dialog box appears. To be able to use the vDisk across multiple Windows VMs, you must change the image mode to Standard Image mode and change the write cache.

Step 30: In the **Access mode** list, choose **Standard Image (multi-device, read-only access)**, and in the **Cache type** list, choose **Cache on device hard drive**, leave the other default settings, and then click **OK**.



The mode of the vDisk is now changed.

Tech Tip

The storage device hard drive selected for the write cache is used for information that is cleared upon VM reboot. Because this is volatile information, an organization's policies may allow for cost savings by moving this cache off of the highly resilient SAN storage and onto storage that is locally attached to the server blade on the Cisco UCS system. Available solid state drives with high I/O performance are well suited for use as a volatile write cache.

Step 31: In VMware vCenter, right-click the H3-DesktopMaster VM, choose **Template > Convert to Template**. A template is created from the selected VM, and you can use this template in order to create additional VMs.

Procedure 8 Install additional Citrix PVS VM

Table 6 - Citrix PVS configuration values for Cisco UCS server 2

Component	Parameter	Cisco SBA value
H2: Cisco UCS server 2	Name in VMware vCenter	chas3-s2
PVS high-availability virtual machine	Name in VMware vCenter	H2-PVS2
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:\ drive)
	Hard disk 2	Virtual disk with default 40 GB drive (E:\ drive)
	DNS name	PVS2
	IP address	10.4.57.8
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

Additional Citrix PVS servers use the existing SQL database, making it unnecessary to install those components.

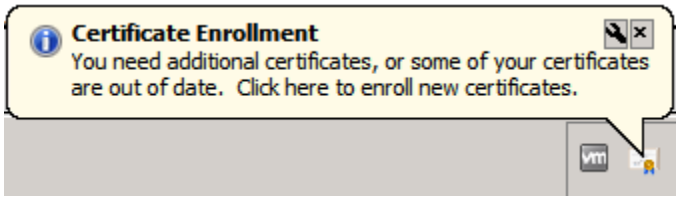
Step 1: On Cisco UCS server 2, install a Microsoft Windows Server 2008 R2 virtual machine instance and VMware Tools, configure network connectivity by using the values in Table 6, activate Windows, and then join the Active Directory domain. When joining the domain, you will be prompted to reload the VM. This is the virtual machine instance that runs the high-availability Citrix PVS installation.

Step 2: After the reload for Active Directory changes is complete, log in to the cisco.local domain, with an account that has local administrator privileges.

Caution

Installing Citrix PVS while not logged in as a domain administrator can cause setup issues resulting from incorrect domain permissions.

Step 3: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click on the taskbar icon, and then complete the certificate enrollment.



Step 4: Click **Start**, in the search box, enter **server manager**, and then click **Server Manager**.

Step 5: In Server Manager, click **Features > Add Features**, select **.NET Framework 3.5.1 Features**, and then at the prompt, click **Add Required Role Services**.

Step 6: In the wizard, use the default values, and then on the last page, click **Install**. When prompted, confirm the installation.

Step 7: When the installation is complete, close the installation wizard.

Step 8: Launch Windows Update, apply any updates found, and then repeat the check for updates until no updates remain. Because the installation adds Windows components, those components should be updated with the latest patches, usually requiring at least one reboot of the VM.

Step 9: In VMware vCenter, mount the Citrix PVS ISO image to the created Windows Server virtual machine, and then allow the AutoPlay service to launch the installation. The Provisioning Services installation wizard is displayed.

Step 10: Select **Console Installation**, and then click **Install**.

Step 11: Complete the next three installation wizards for the Host PowerShell, Broker, and Configuration Snap-Ins, and note the following for each:

- Select **I accept the terms of the License Agreement**.
- Click **Install**.
- When the module installation is complete, click **Next**.

Step 12: At the prompt for Customer Information, in the **User Name** box, enter Administrator, and in the **Organization** box, enter SBA, and then click **Next**.

Step 13: Use all of the defaults in order to finish the installation of Provisioning Services Console.

Step 14: In the Provisioning Services installation wizard, select **Server Installation**, and then click **Install Server**.

Step 15: Accept all the default settings and prompts, accept the licensing agreement, in the **User Name** box, enter Administrator, and in the **Organization** box, enter SBA, and then complete the Provisioning Services server installation.

The Provisioning Services Configuration Wizard is automatically launched.

Procedure 9 Configure additional Citrix PVS VM

Step 1: Open the console of the H2-PVS2 VM (Example: PVS2.cisco.local). The Provisioning Services Configuration Wizard should be open.

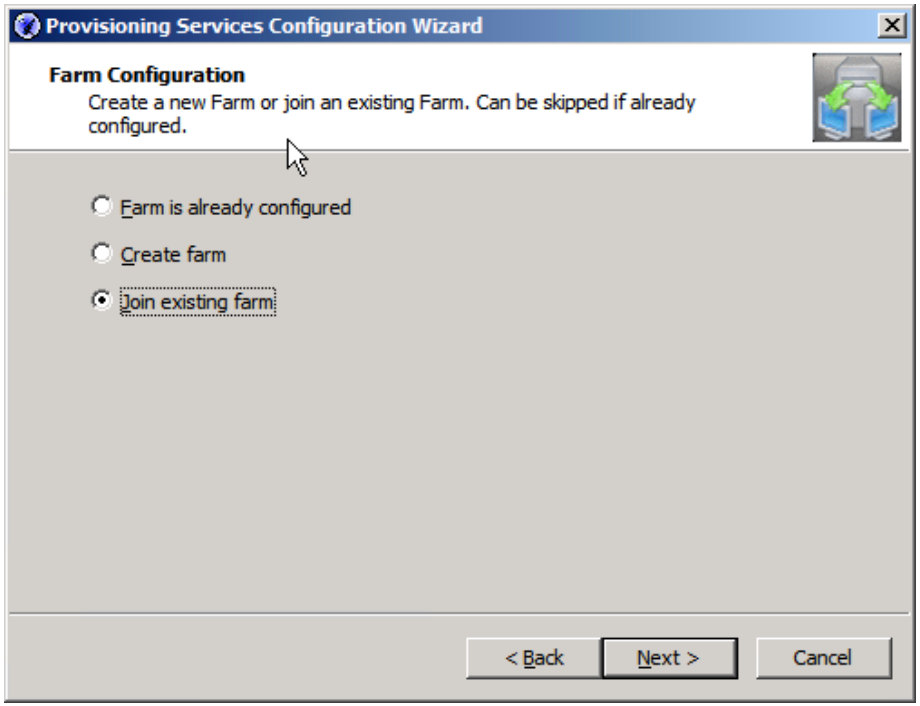
If the Provisioning Services Configuration Wizard has been closed, restart it by selecting **Start > All Programs > Citrix, Provisioning Services > Provisioning Services Configuration Wizard**.

Step 2: On the introduction page, click **Next**.

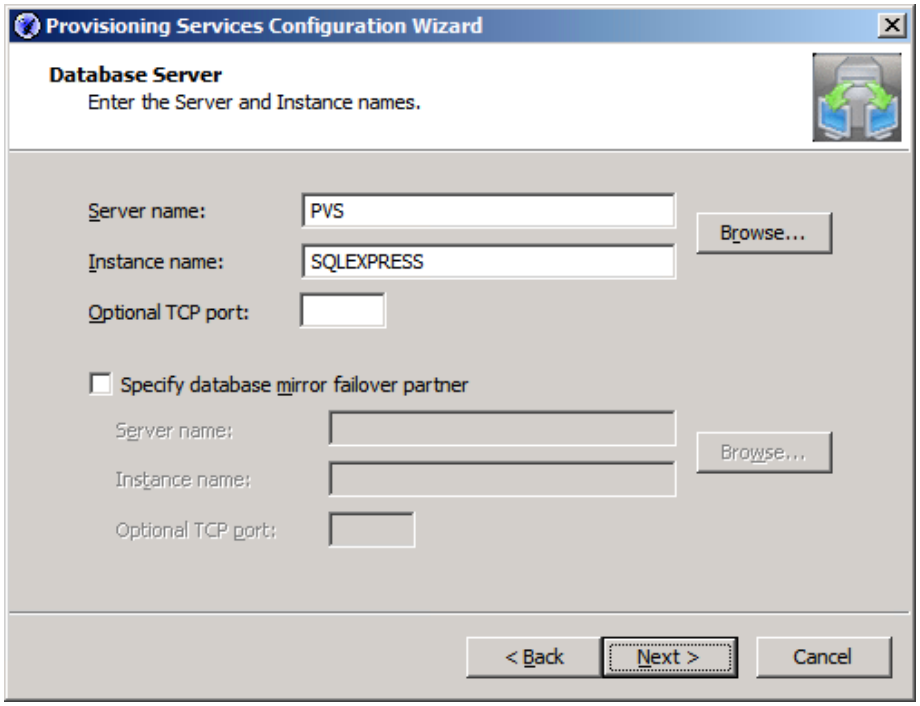
Step 3: On the DHCP Services page, select **The service that runs on another computer**, and then click **Next**.

Step 4: On the PXE Services page, select **The service that runs on this computer**, select **Provisioning Services PXE service**, and then click **Next**.

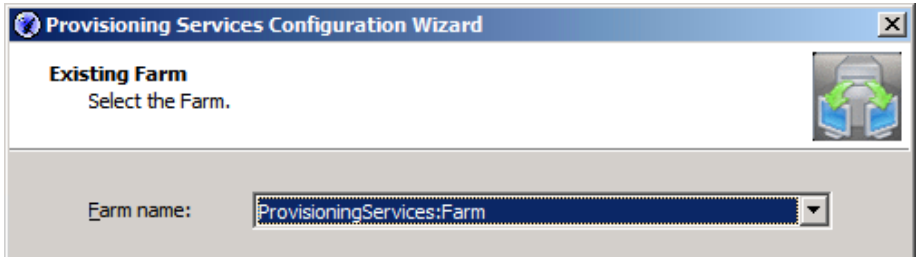
Step 5: On the Farm Configuration page, select **Join existing farm**, and then click **Next**.



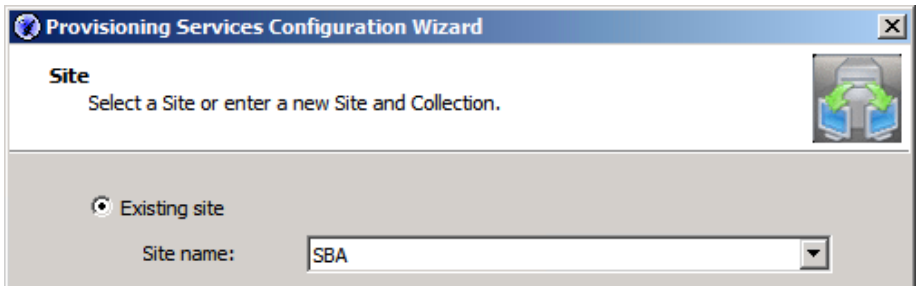
Step 6: On the Database Server page, in the **Server name** box, enter the Active Directory name of the H1-PVS VM (Example: PVS), in the **Instance name** box, enter **SQLEXPRESS**, and then click **Next**.



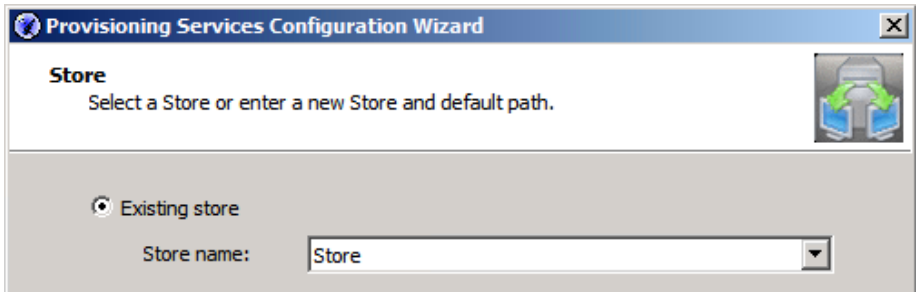
Step 7: On the Existing Farm page, in the **Farm name** list, choose the farm on the H1-PVS VM (Example: ProvisioningServices:Farm), and then click **Next**.



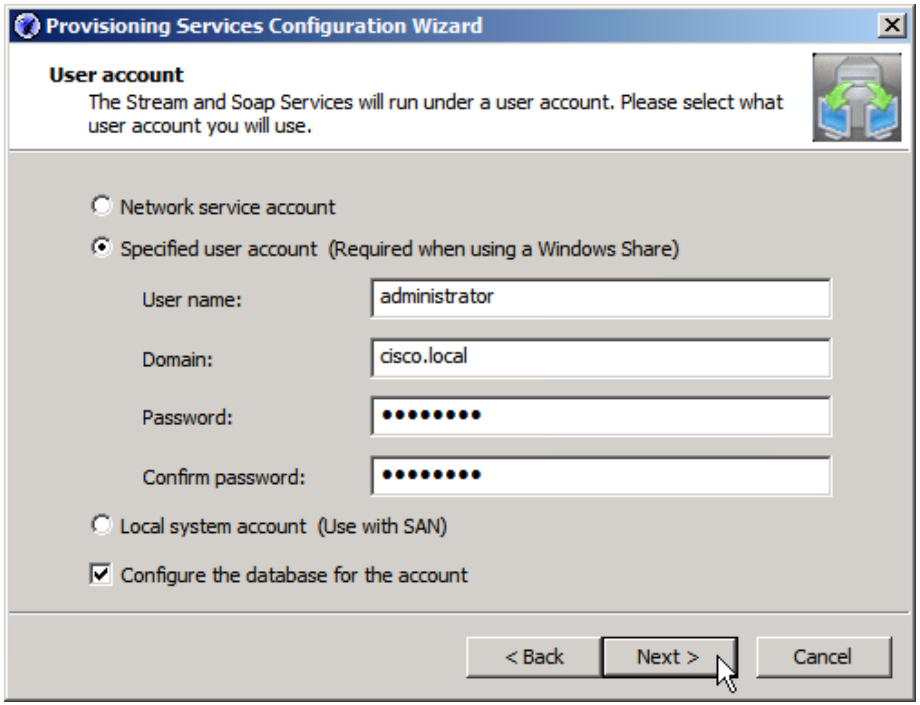
Step 8: On the Site page, ensure the value in the **Site Name** list is **SBA**, and then click **Next**.



Step 9: On the Store page, ensure the value in the **Store Name** list is **Store**, and click **Next**.

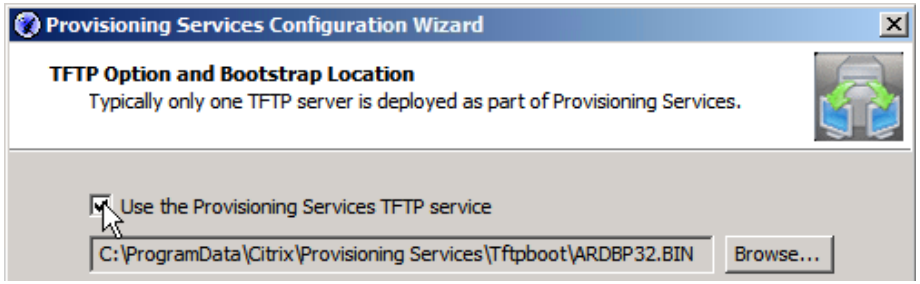


Step 10: On the User account page, select **Specified user account (Required when using a Windows Share)**, in the **User name** box, enter administrator, in the **Domain** box, enter cisco.local, and in the **Password** and **Confirm password** boxes, enter the administrator password. Select **Configure the database for the account**, and then click **Next**.

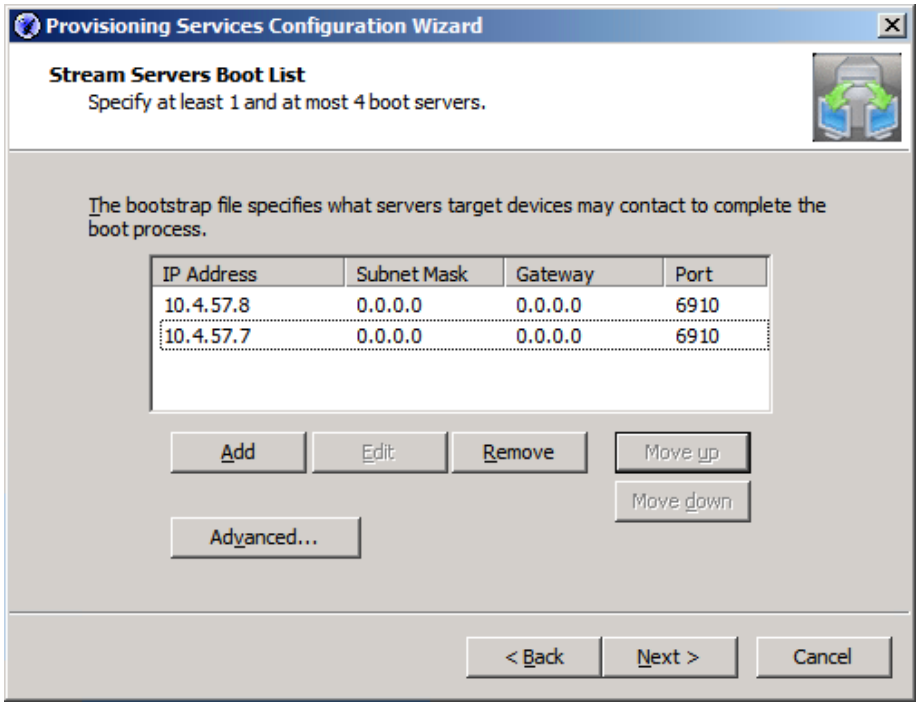


Step 11: On the next two pages, accept the defaults, and then click **Next**.

Step 12: On the TFTP Option and Bootstrap Location page, select **Use the Provisioning Services TFTP Service**, and then click **Next**.

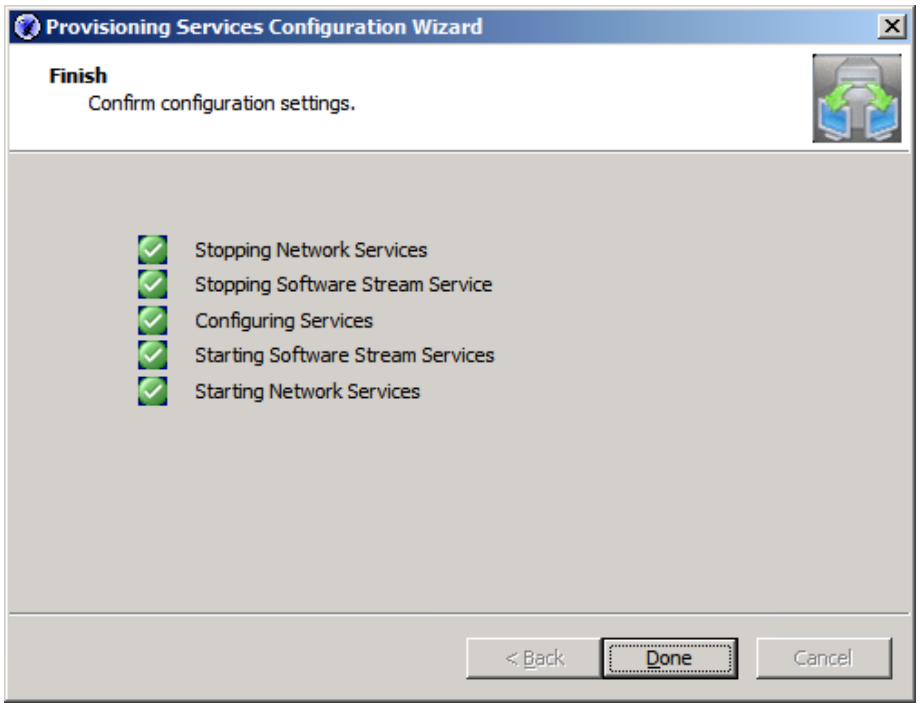


Step 13: On the Stream Servers Boot List page, click **Add**, enter the IP address of the H1-PVS VM (Example: 10.4.57.7), confirm the update, and then click **Next**.



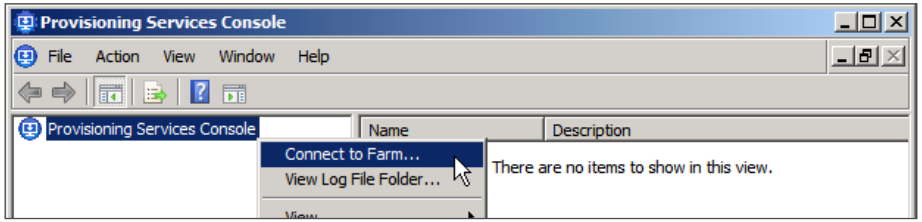
Step 14: On the Finish page, click **Finish**. The configuration is confirmed, and the status is displayed as the Citrix PVS services start.

Step 15: When the configuration is complete, click **Done**. Configuration of the H2-PVS2 VM with the configuration wizard is complete.

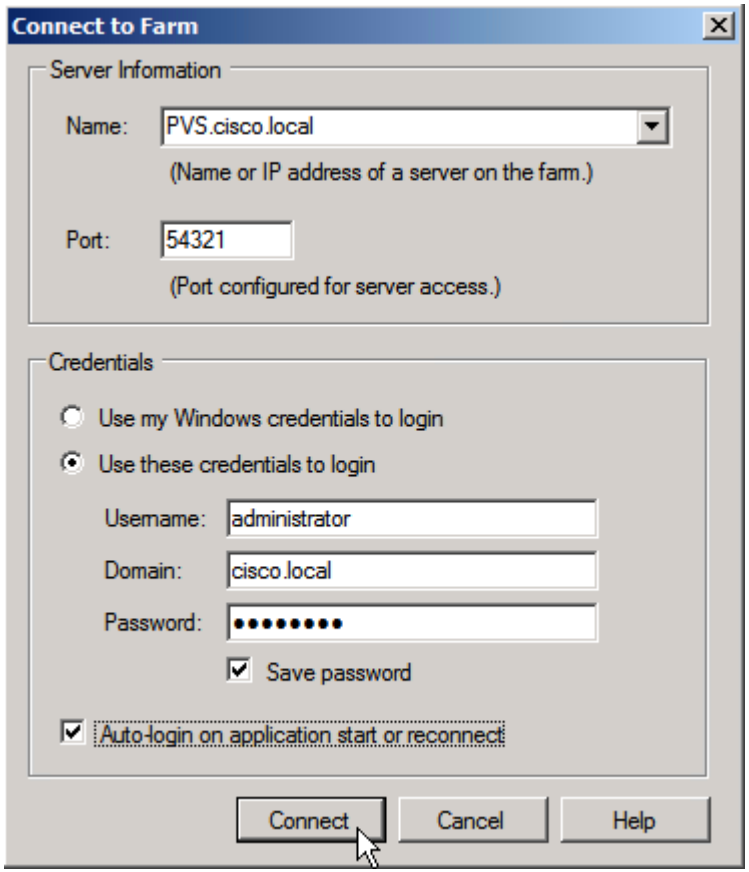


Step 16: Click **Start**, and then open the Provisioning Services Console.

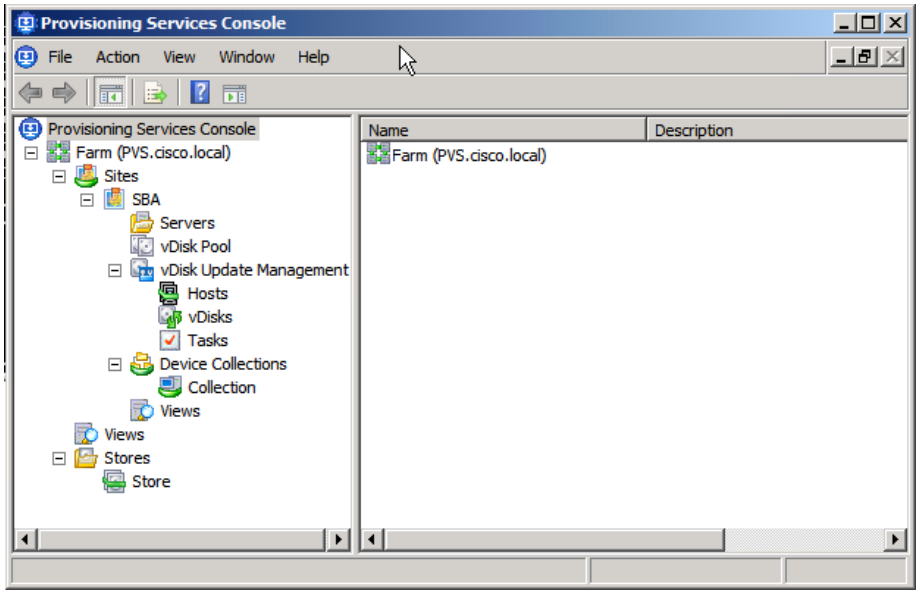
Step 17: In the tree, right-click **Provisioning Services Console**, and then choose **Connect to Farm**.



Step 18: On the Connect to Farm dialog box, in the **Name** box, enter PVS.cisco.local, keep the other default settings, select **Auto-login on application start or reconnect**, and then click **Connect**.



The created farm is displayed.

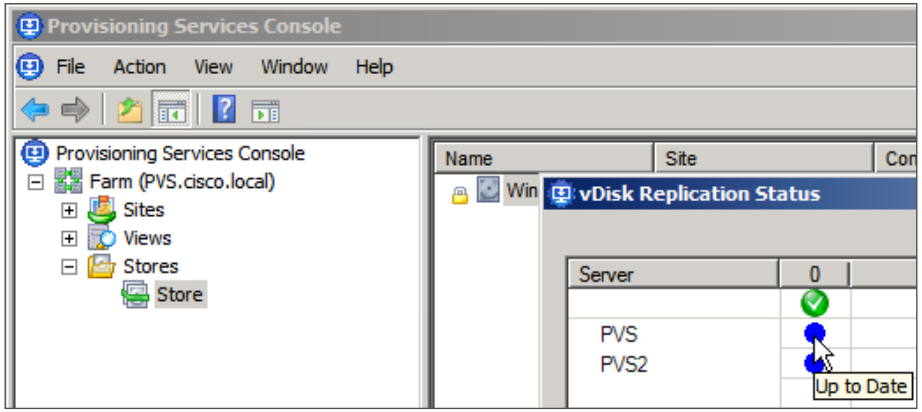


To allow the H2-PVS2 VM to serve the same Standard Image mode vDisk as that is on the H1-PVS VM, you must copy the E:\Store directory to the H2-PVS2 VM.

Step 19: From your management machine, share the H1-PVS E:\ drive and the H2-PVS2 E:\ drive, and copy all files with names ending in .vhd, .avhd, and .pvp within the Store directory from the H1-PVS VM to the H2-PVS2 VM. Do not copy any files with names ending in .lok.

After the file copy is complete, you can validate the replication status.

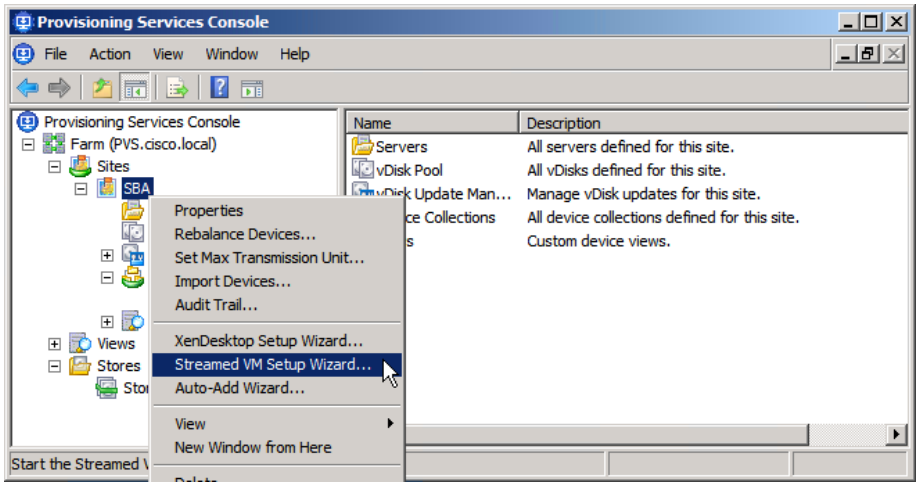
Step 20: In the provisioning services console, navigate to **Farm** > **Store** > **Stores**, in the right pane right-click the Win7x64 vDisk, and then select **Replication Status**. Hovering the mouse pointer over the circles will reveal the current status for vDisk replication.



Procedure 10 Create streamed VM collection

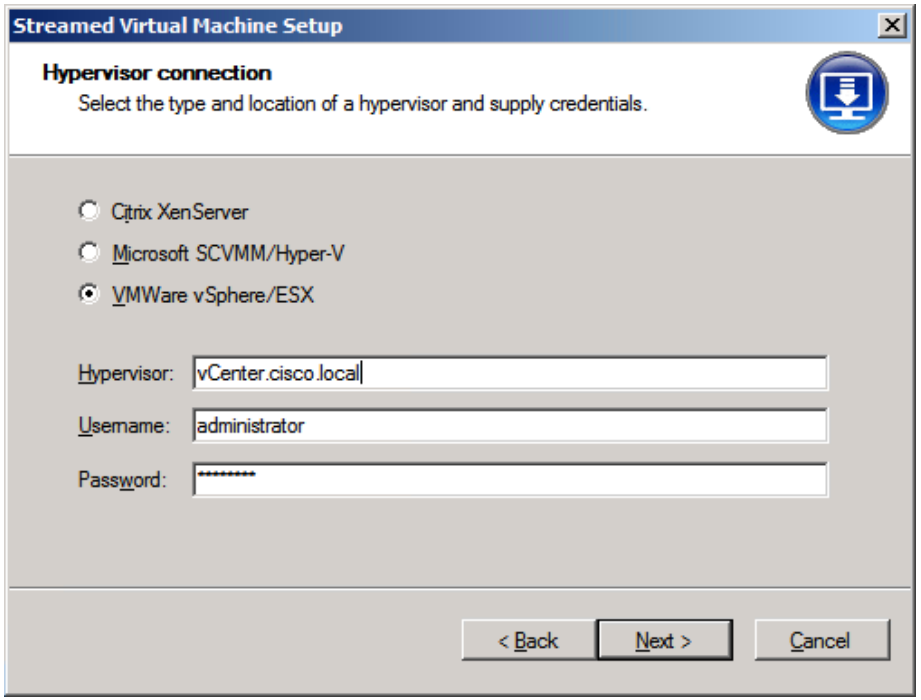
The Streamed VM Setup Wizard automates the creation of VMs managed by Citrix XenDesktop, integrating vDisk streaming from Provisioning Services and creating Microsoft Active Directory accounts for the VMs. The required number of VMs is automatically cloned in VMware vCenter by using the template previously created, and the VMs are made available in the catalog. In order for any Provisioning Services VM to update Active Directory, it must have permissions on the Active Directory server to do so.

Step 1: On the H1-PVS VM, in the Provisioning Services Console, navigate to Farm > Sites > SBA, right-click SBA, and then choose Streamed VM Setup Wizard.

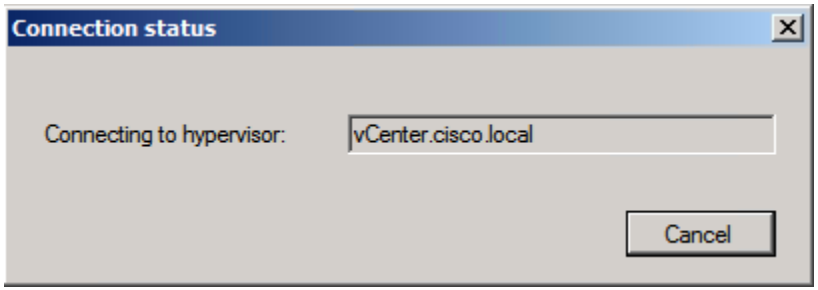


Step 2: In the Streamed Virtual Machine Setup wizard, on the Welcome page, click Next.

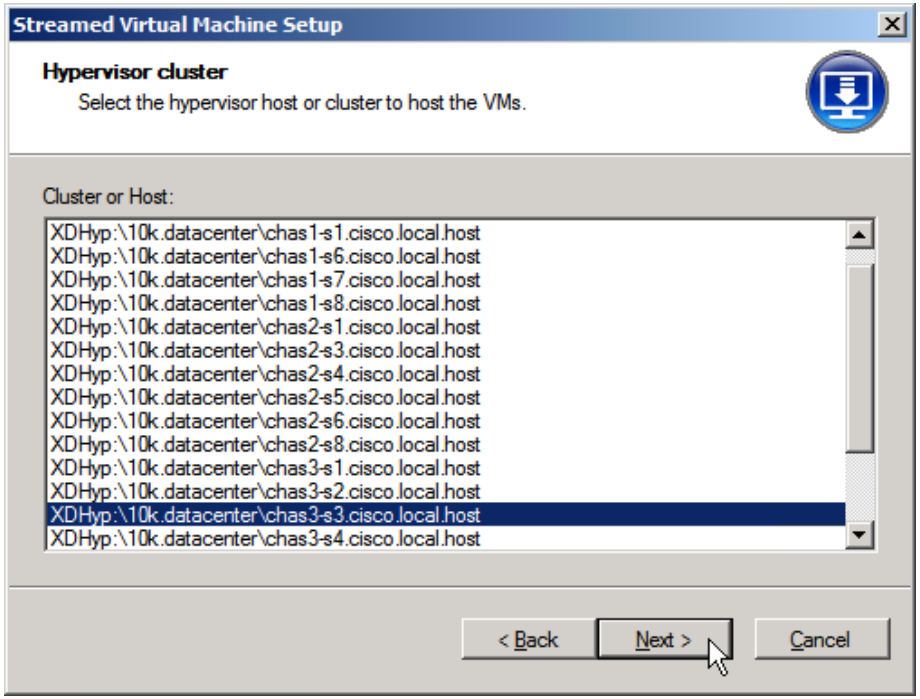
Step 3: On the Hypervisor connection page, select VMWare vSphere/ESX, in the Hypervisor box, enter vCenter.cisco.local, enter the administrator credentials, and then click Next.



A Connection status dialog box displays. It may take a few minutes before the connection is complete.



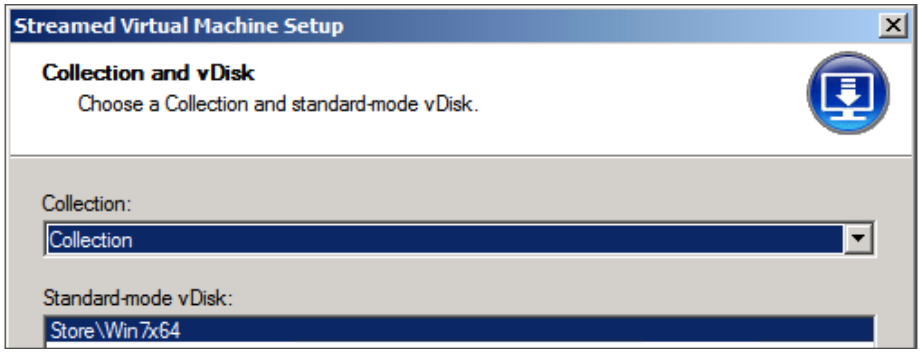
Step 4: On the Hypervisor cluster page, select the Cisco UCS server 3 hypervisor host (Example: chas3-s3.cisco.local), and then click **Next**.



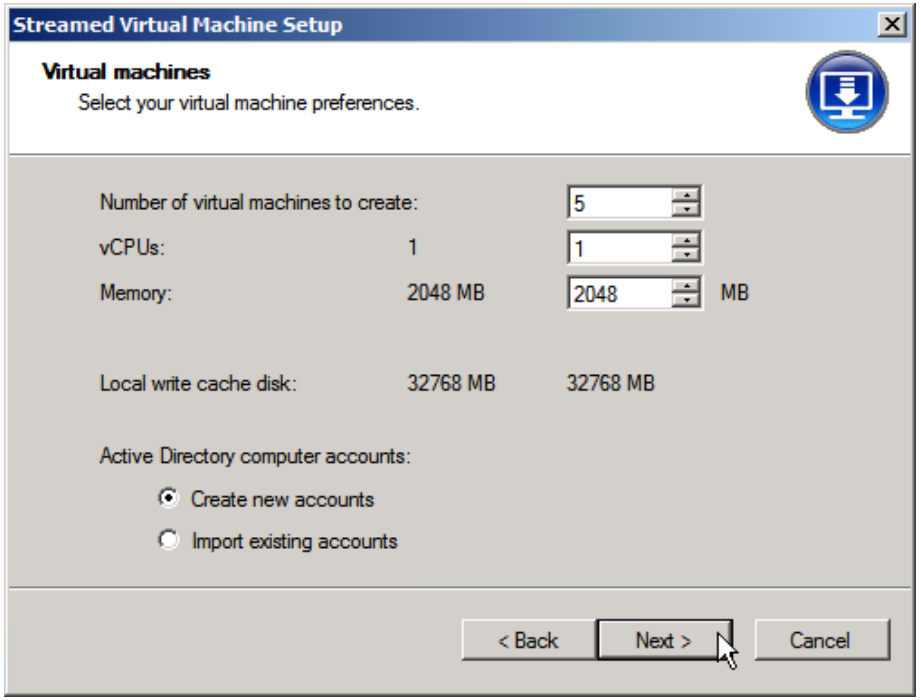
The template information is read from VMware vCenter.

Step 5: On the template listing, select the VM template created in the previous procedure (Example: H3-DesktopMaster), and then click **Next**.

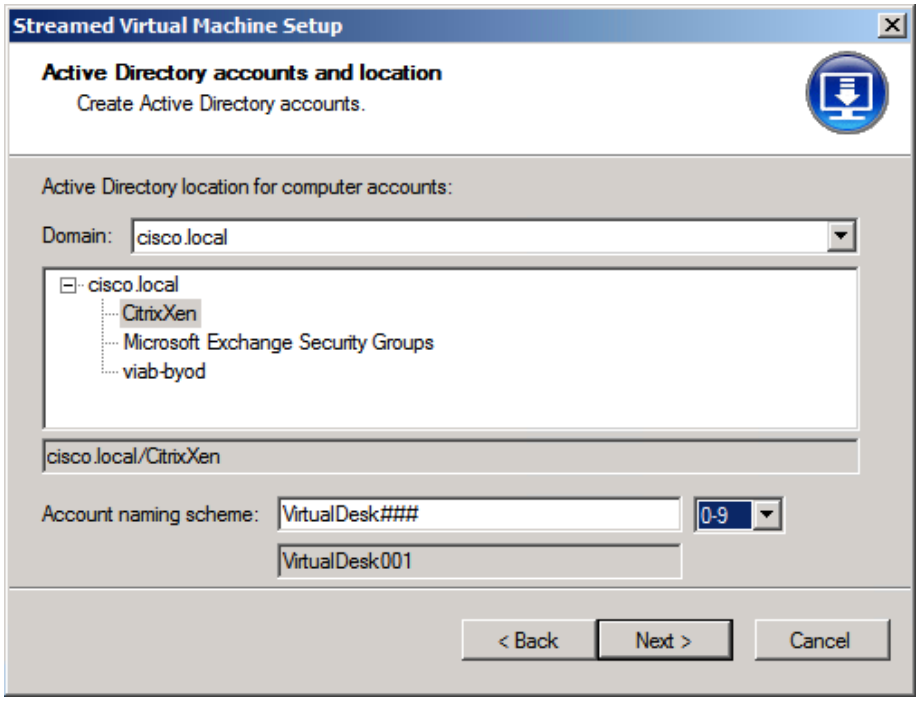
Step 6: On the Collection and vDisk page, in the **Collection** list, choose **Collection**, in the **Standard-mode vDisk** list, choose Store\Win7x64, and then click **Next**.



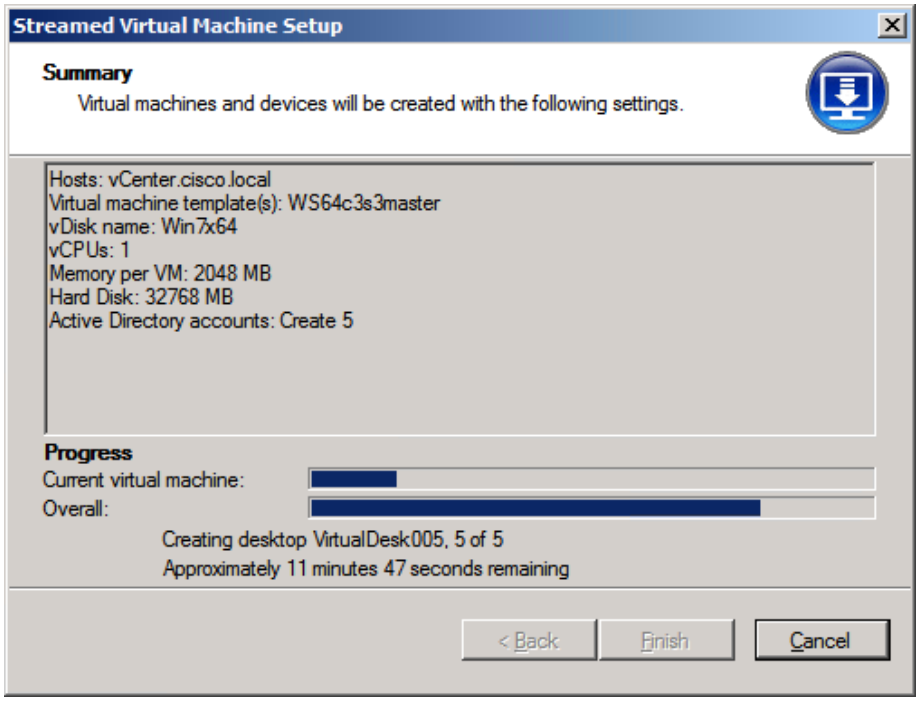
Step 7: On the Virtual machines page, in the **Number of virtual machines to create** box, enter 5, leave the remaining defaults, and then click **Next**.



Step 8: On the Active Directory accounts and location page, in the **Domain** list, choose **cisco.local**, in the tree, select **CitrixXen**, in the **Account naming scheme** box, enter **VirtualDesk###**, and then click **Next**.

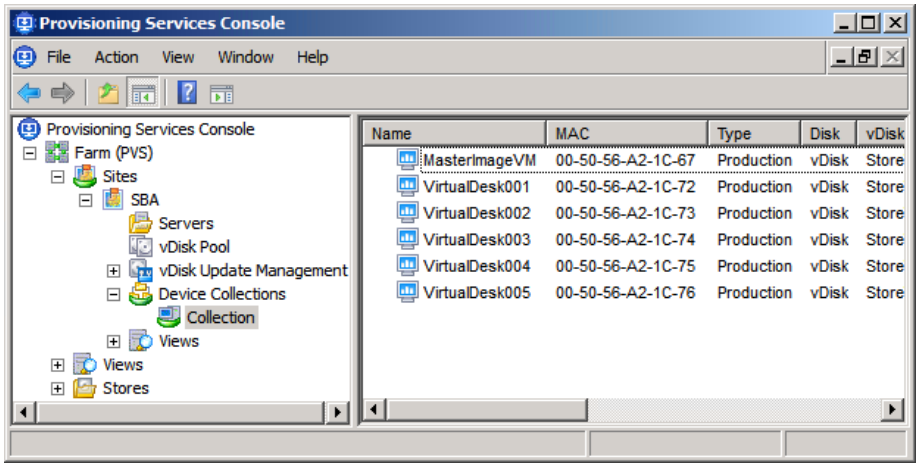


Step 9: On the Summary page, click **Finish**. Progress of virtual machine creation is indicated by the wizard. You can also observe the virtual machine creation in VMware vCenter.

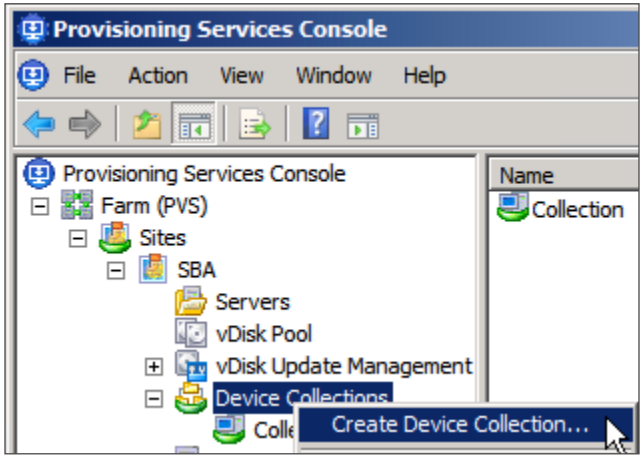


Step 10: When the "Setup complete" message is displayed, click **Done**.

Step 11: Return to the Provisioning Services Console, navigate to **Farm** > **Sites** > **SBA** > **Device Collections** > **Collection**, and then from the **Action** menu, choose **Refresh**. The created VMs are displayed.

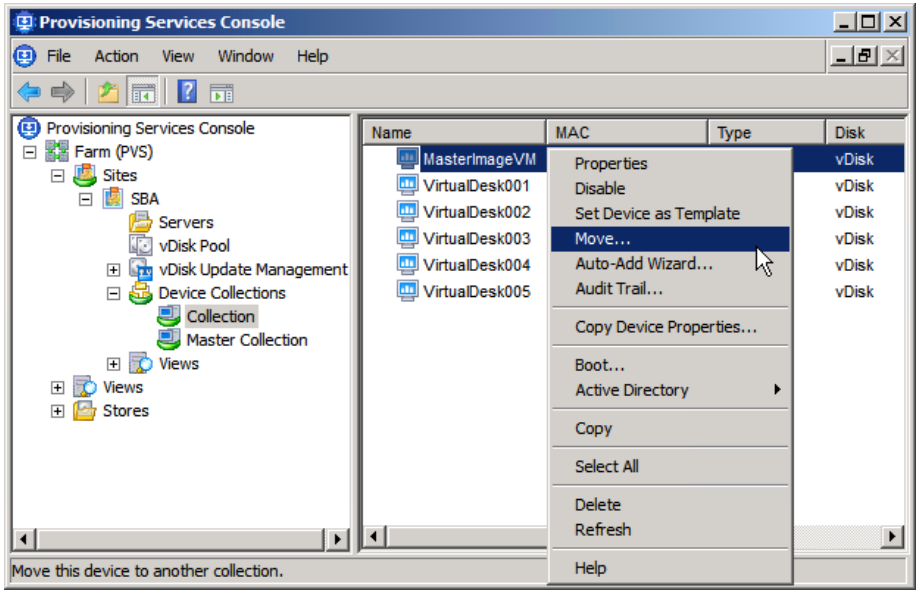


Step 12: Right-click **Device Collections**, and then choose **Create Device Collection**.

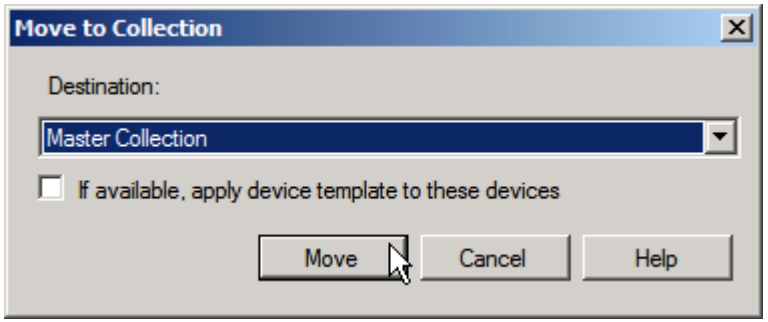


Step 13: On the dialog box, enter **Master Collection** as the name of the new collection, and then click **OK**.

Step 14: In the tree, select **Collection**, right-click the **MasterImageVM** device, and then choose **Move**.



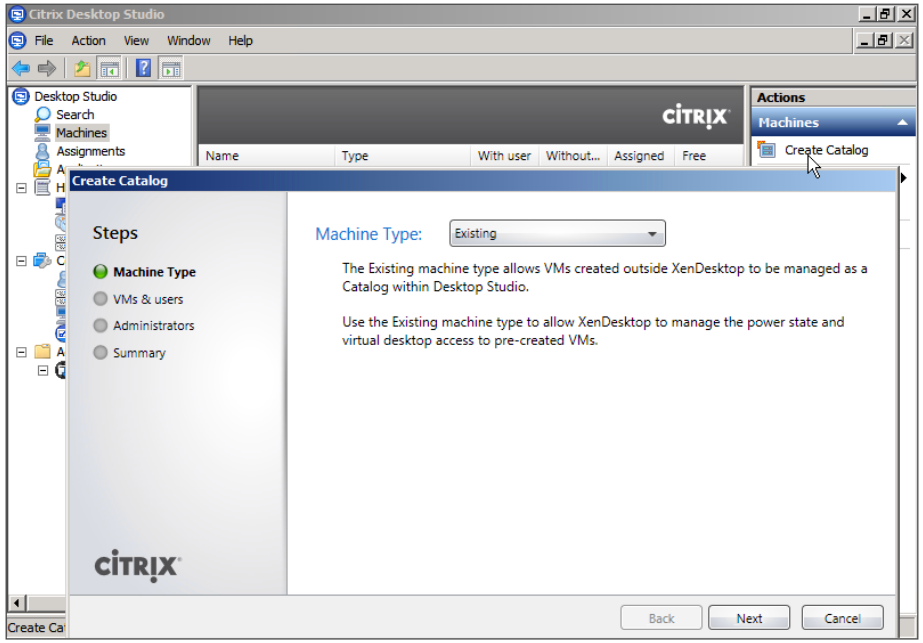
Step 15: In the **Destination** list, choose **Master Collection**, and then click **Move**.



The master VM is moved to the new collection, leaving only the VMs that were provisioned by Citrix PVS in the original collection.

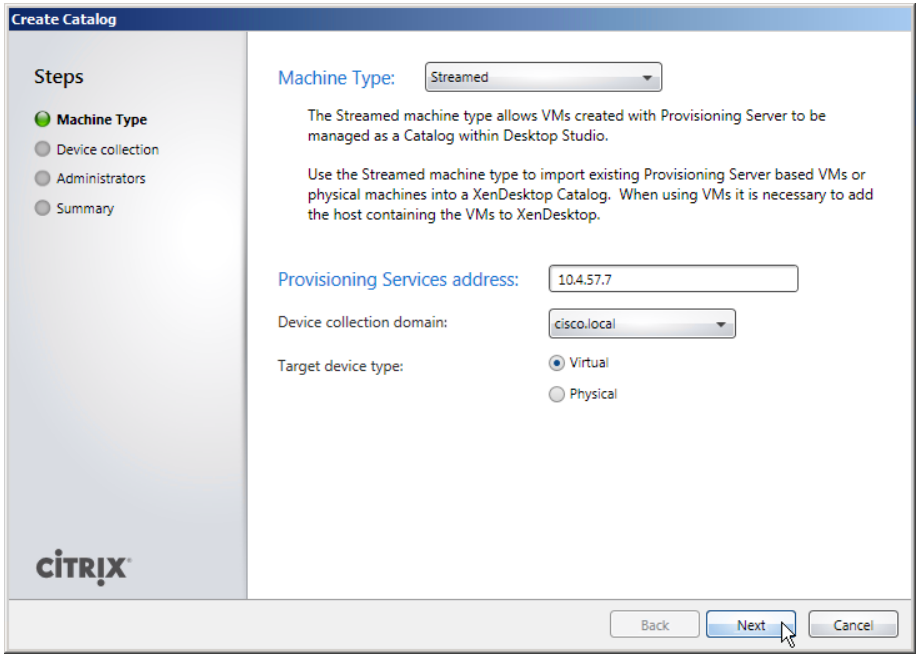
Procedure 11 Create catalog in Citrix Desktop Studio

Step 1: In VMware vCenter, open the console to the H1-DDC VM (Example: DDC.cisco.local), within the **Citrix Desktop Studio** plugin application, select **Machines**, and then from the **Actions** menu, choose **Create Catalog**. The Create Catalog wizard is launched.

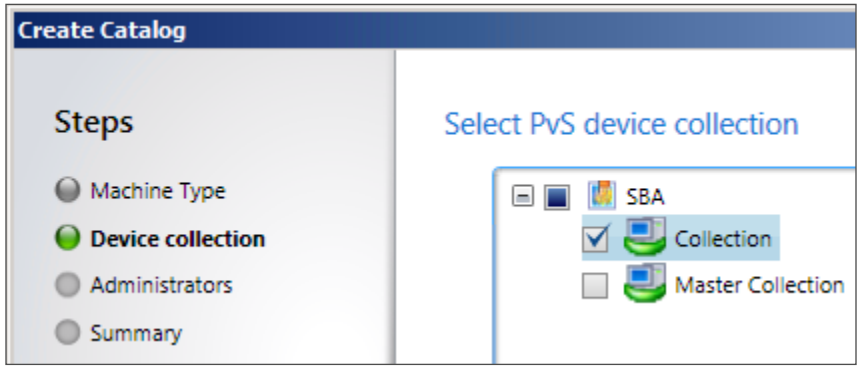


Step 2: On the Machine Type page, enter the following values, and then click **Next**:

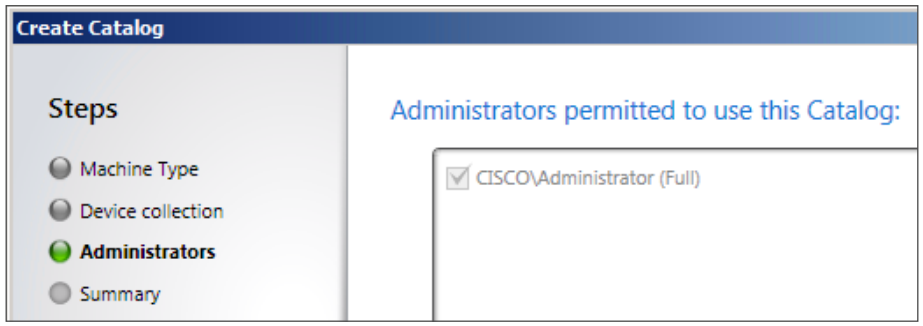
- Machine Type—**Streamed**
- Provisioning Services address—10.4.57.7 (do not use the DNS name)
- Device collection domain—cisco.local
- Target device type—**Virtual**



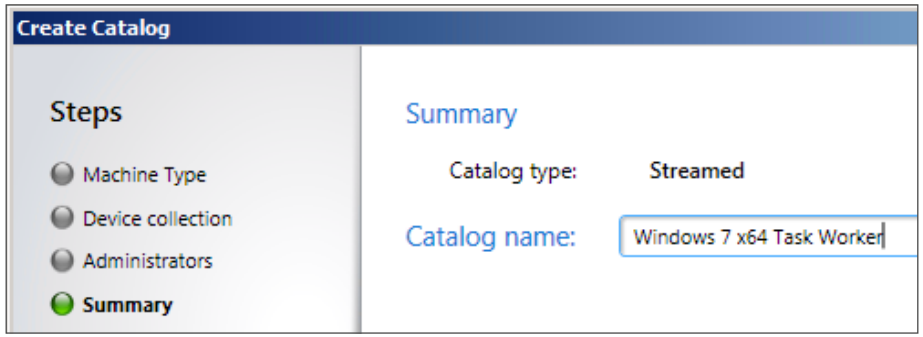
Step 3: Once the service connects and displays the information for the H1-PVS VM, on the Device Collection page, expand SBA, select Collection, and then click **Next**.



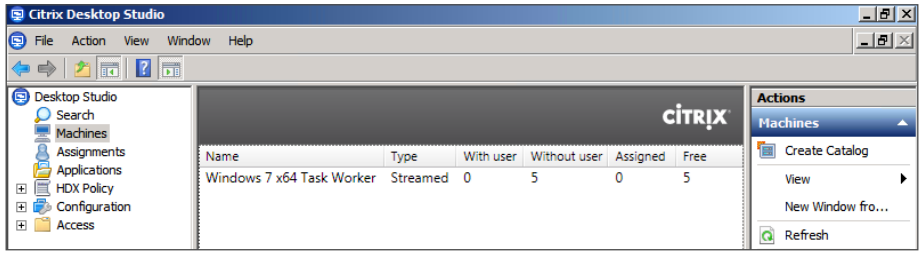
Step 4: On the Administrators page, keep the default administrator setup, and then click **Next**.



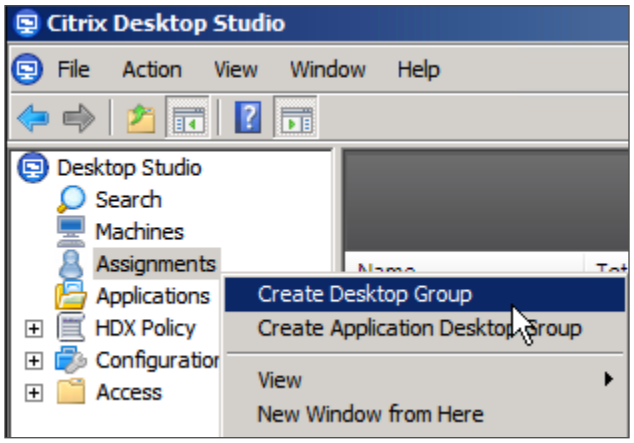
Step 5: On the Summary page, in the **Catalog name** box, enter Windows 7 x64 Task Worker, and then click **Finish**.



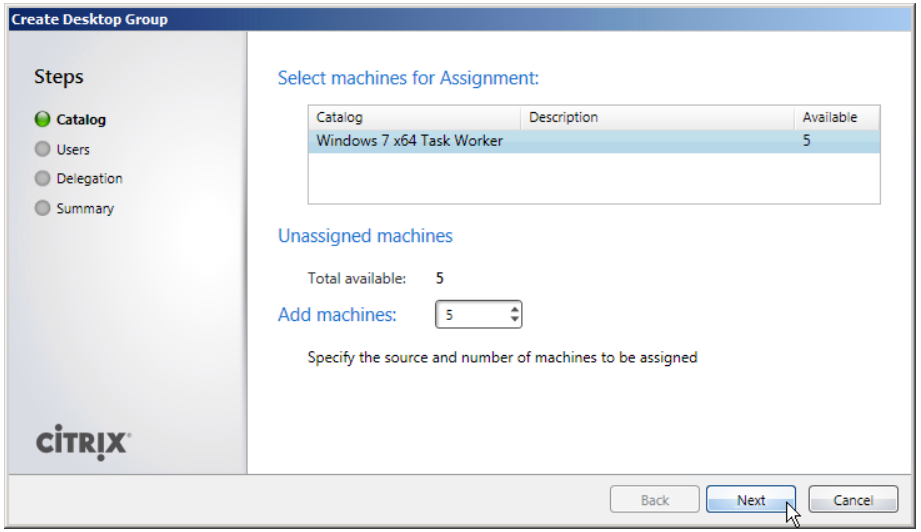
The new catalog is created and displayed in Citrix Desktop Studio.



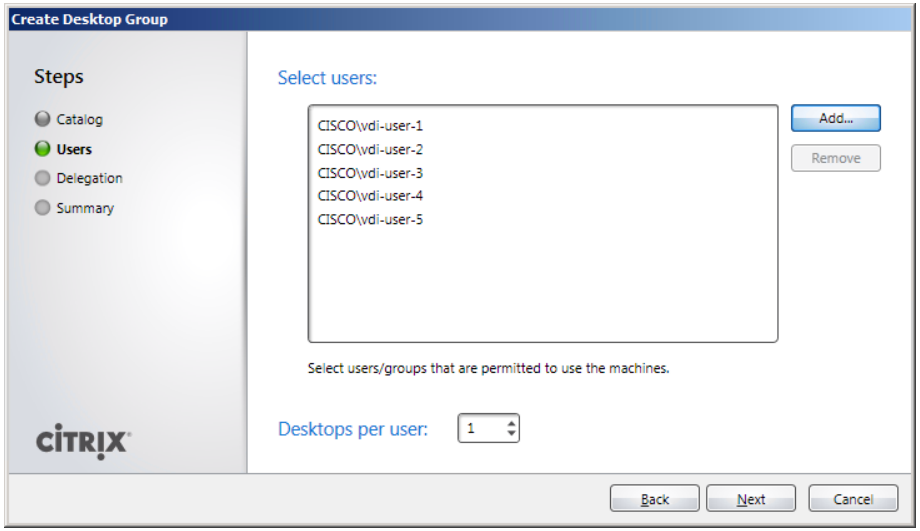
Step 6: In the tree, select **Assignments**, right-click it, and then choose **Create Desktop Group**.



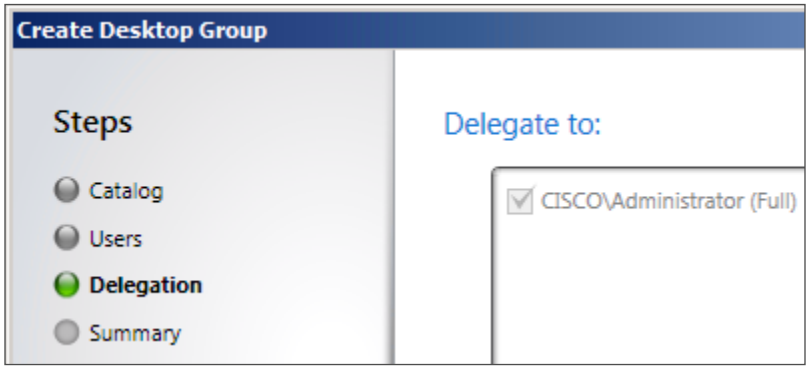
Step 7: In the Create Desktop Group wizard, on the Catalog page, in the **Select machines for Assignment** list, choose Windows 7 x64 Task Worker, in the **Add machines** box, enter 5, and then click **Next**.



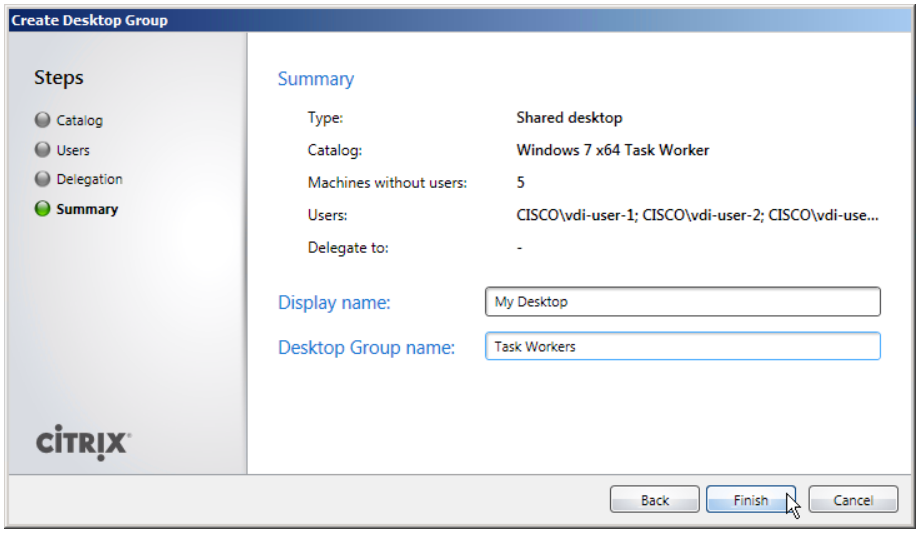
Step 8: On the **Users** page, click **Add**, select and include Active Directory users you wish to include for access to the machines, and then click **Next**.



Step 9: On the Delegation page, keep the default administrator selection, and then click **Next**.

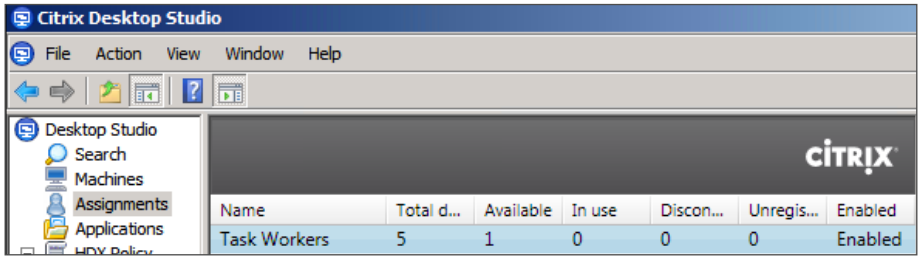


Step 10: On the Summary page, in the **Display name** box, enter My Desktop, in the **Desktop Group name** box, enter Task Workers, and then click **Finish**.



The assignment is created.

Citrix XenDesktop powers up VMs as required in order to meet its idle pool requirement. Once a VM has been fully booted and its Virtual Desktop Agent software communicates with a XenDesktop server, the VM shows as **Active** in Citrix Desktop Studio.



Procedure 12 Test connectivity to virtual desktops

Citrix Web Interface delivers virtual desktops to clients, and it is installed as part of the Citrix XenDesktop installation procedure. The clients access Citrix Web Interface directly and through the use of Citrix Receiver clients.

Step 1: In a web browser, connect to the URL for the Web Interface that resides on an active Citrix XenDesktop server:

http://DDC.cisco.local/

Note that the name or IP address in the URL is specific to one server for testing, and if you are using a load balancer, you can replace the IP address with a DNS name or virtual IP address that references all servers.

Step 2: On the Log on page, in the **User name** box, enter **vdi-user-1**, enter the password, and in the **Domain** box, enter **cisco.local**, and then click **Log On**.

Step 3: In the web browser, select **My Desktop**. Citrix Desktop Viewer launches.

The virtual desktop can now be used.

Process

Installing and Configuring Citrix XenApp

1. Install first Citrix XenApp VM
2. Install additional Citrix XenApp VM
3. Configure the Citrix XenApp farm
4. Publish a virtual application
5. Configure and test application delivery

You use Citrix License Server and SQL database during the installation of Citrix XenApp. Each installation of the XenApp software is installed into a Microsoft Windows Server 2008 R2 operating system. The details of a Windows Server installation vary by IT organization, and specific Windows installation details are not included in this guide.

Reader Tip

For more information about installing Windows Server 2008 R2, see the following:
http://technet.microsoft.com/en-us/library/dd379511.aspx

Procedure 1 Install first Citrix XenApp VM

You install Microsoft Windows Server 2008 R2 virtual machine instances (including VMware Tools) on the Cisco UCS hardware designated for infrastructure services. The following information is used.

Table 7 - Citrix XenApp configuration values for Cisco UCS server 4

Component	Parameter	Cisco SBA value
H4: Cisco UCS server 4	Name in VMware vCenter	chas3-s4
	IP address	10.4.63.114
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
XenApp virtual machine	Name in VMware vCenter	H4-XA1
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	DNS name	XA1
	IP address	10.4.57.21
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

For each Windows Server instance, ensure that:

- Network connectivity is configured and available
- Windows OS license is activated
- Windows Server patches are applied
- Microsoft Active Directory domain is joined (prerequisite for site-configuration step)

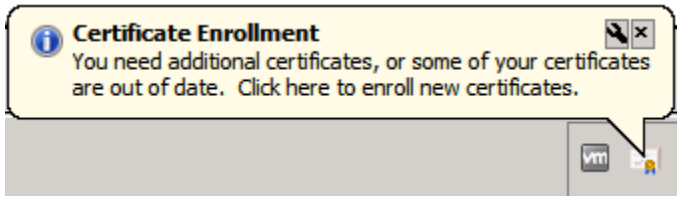
The following Windows Server prerequisite for the Citrix XenApp installation does not need to be installed at this time, because the installation software detects that it is not installed and then automatically launches the installation:

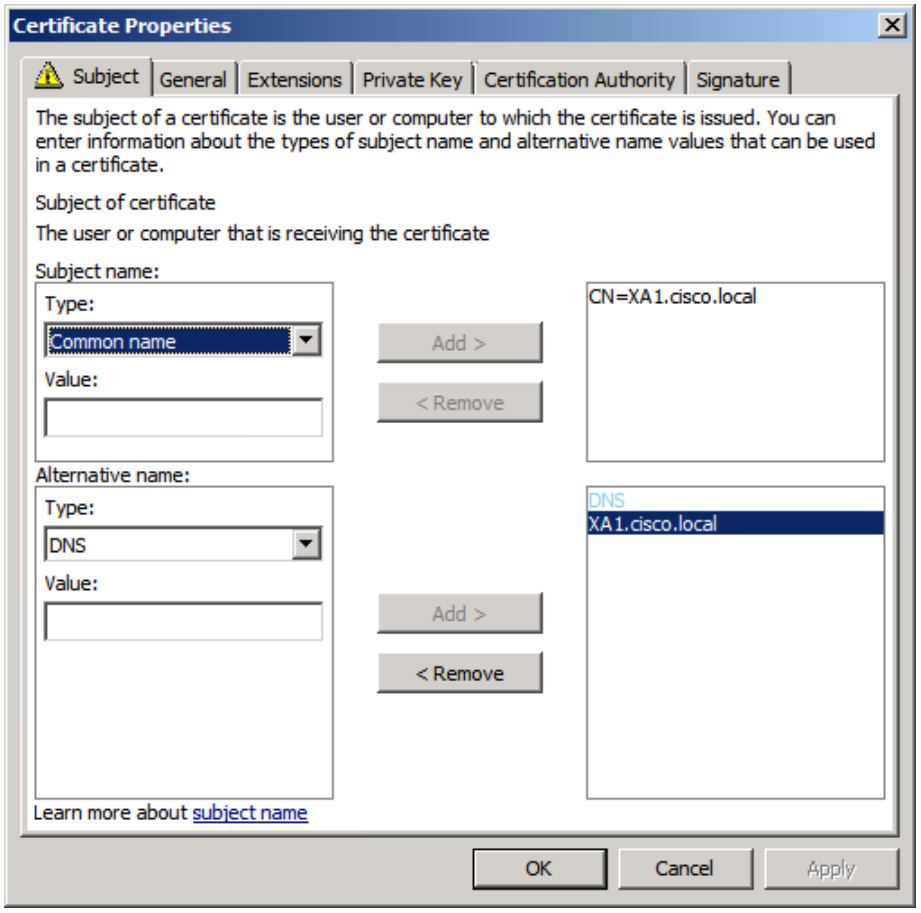
- Microsoft .NET Framework 3.5 Service Pack 1

Step 1: On Cisco UCS server 4, install a Microsoft Windows Server 2008 R2 virtual machine instance and VMware Tools, configure network connectivity by using the values above, activate Windows, and then join the Active Directory domain and apply Windows Update patches. When joining the domain and applying the patches, you will be prompted to reload the VM. This virtual machine is the H4-XA1 instance.

Step 2: After reloading for updates and Active Directory changes is complete, return to the H4-XA1 console, and then log in to the Active Directory domain as a user with administrative privileges (Example: cisco.local\administrator).

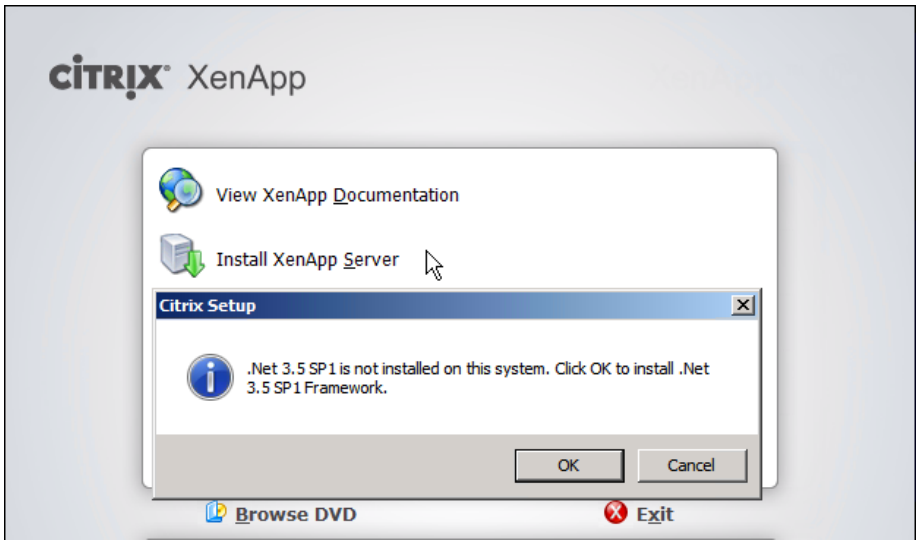
Step 3: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click on the taskbar icon, and then complete the certificate enrollment.





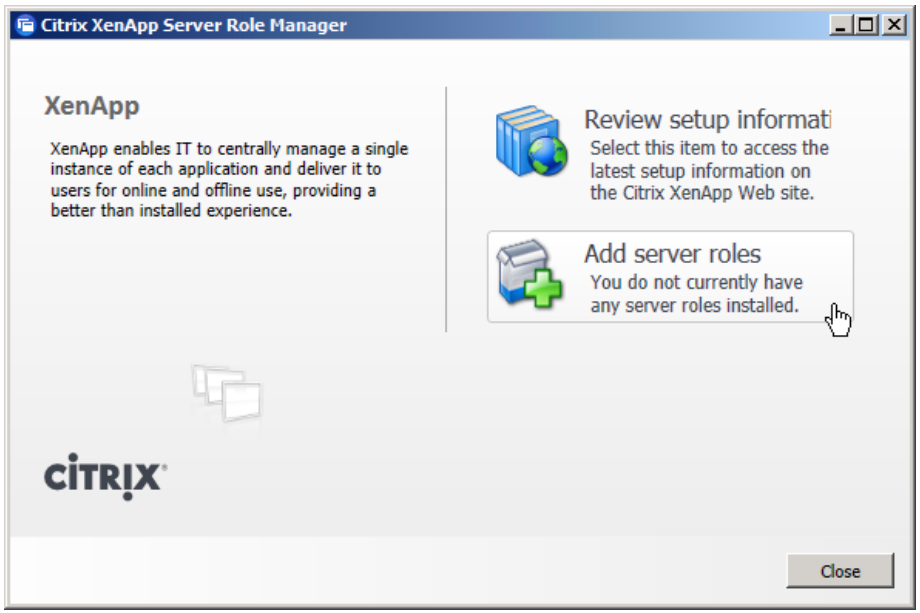
Step 4: In VMware vCenter, mount the Citrix XenApp ISO image to the H4-XA1 virtual machine, and then allow the AutoPlay service to launch the Citrix AutoSelect.exe XenApp installer. The first XenApp installation screen is displayed.

Step 5: Click **Install XenApp Server**, and then on the ".Net 3.5 SP1 is not installed on this system" message, click **OK**.



The .Net installation begins, and then the Citrix XenApp installation launches.

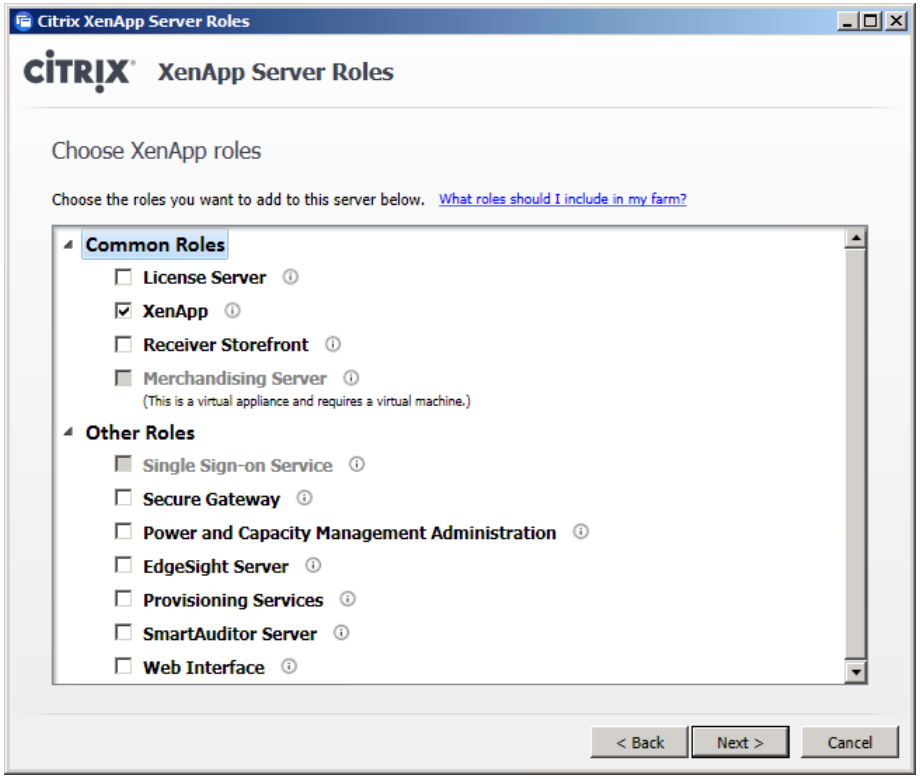
Step 6: When the Citrix XenApp Server Role Manager dialog box appears, click **Add server roles**.



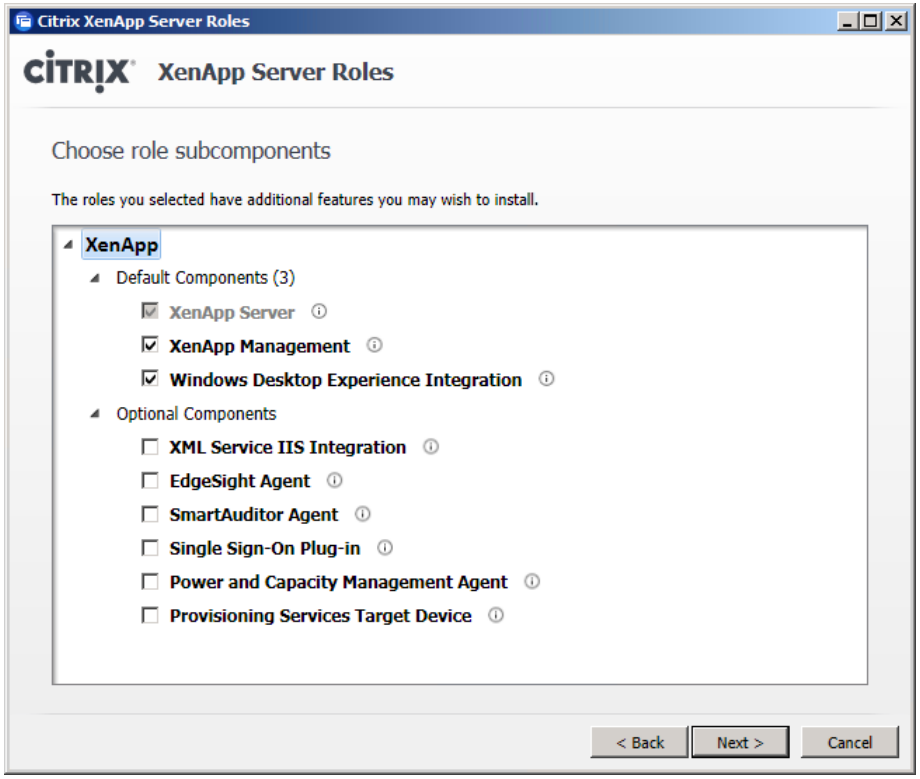
Step 7: In the Citrix XenApp Server Roles wizard, select a Citrix XenApp edition to use for the installation. This procedure uses the Platinum Edition.

Step 8: Accept the license agreement, and then click **Next**.

Step 9: On the Choose XenApp roles page, select **XenApp**, and then click **Next**.

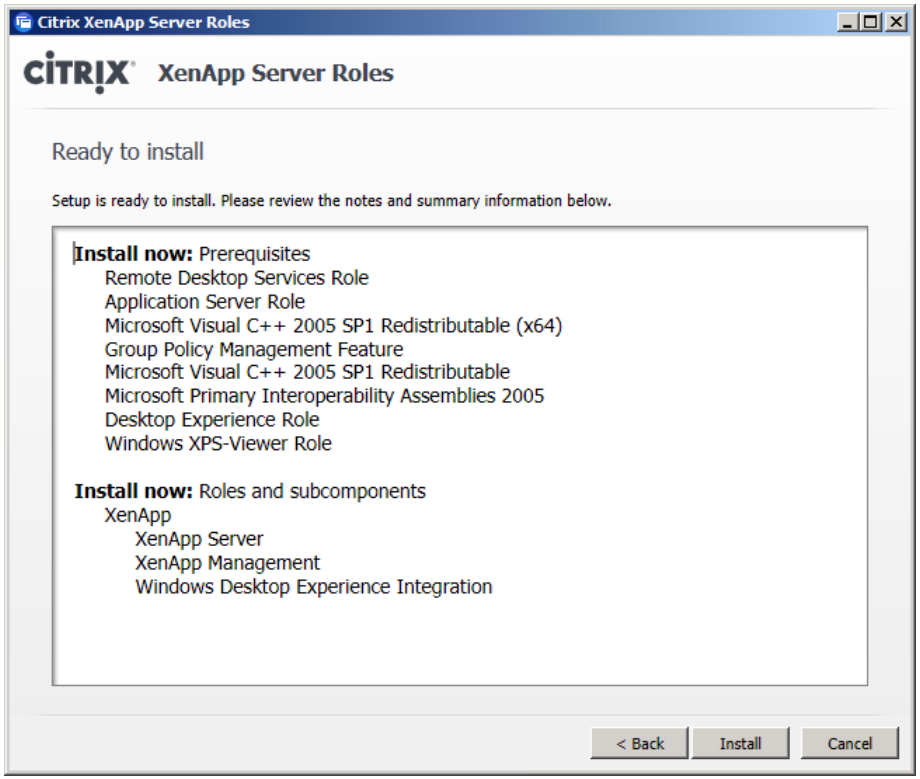


Step 10: On the Choose role subcomponents page, leave the default selections, and then click **Next**.



Step 11: On the Review Prerequisites page, review the prerequisites, and then click **Next**.

Step 12: On the Ready to install page, click **Install**.

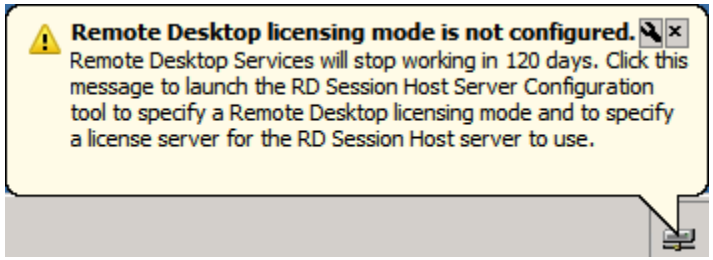


The installation begins.

Step 13: Continue to follow the instructions to complete the wizard installation activity, and select **Reboot** whenever prompted.

Step 14: Log in to the H4-XA1 VM with the same administrator credentials that you used during installation.

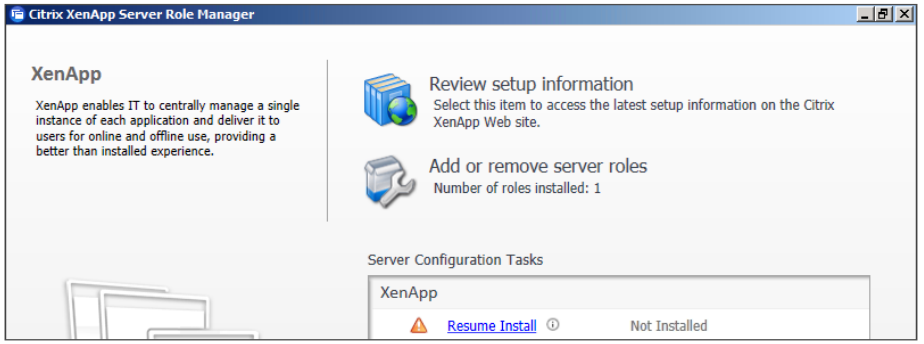
After rebooting and logging in with administrator credentials, a Microsoft Remote Desktop Services licensing message appears. You address this message at a later time.



Caution

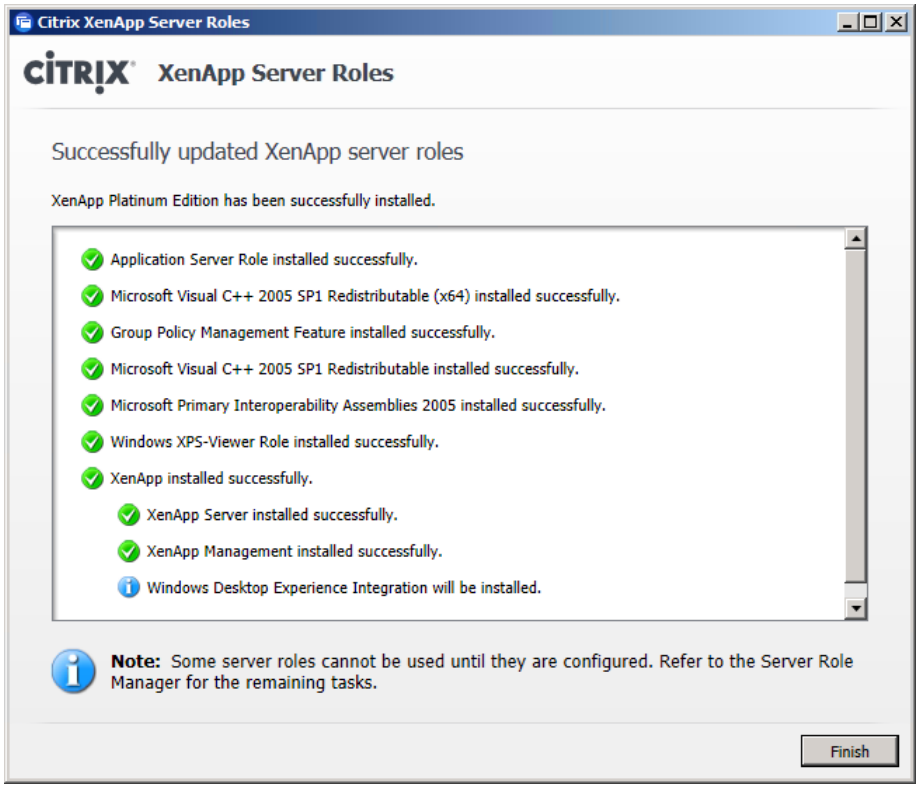
Log in using the full domain and username that you used during the installation, replacing any alternative domain and username that may be displayed. If you use credentials that are different than the installation credentials, the continuation of the installation does not launch automatically, and future installation screens are blank.

Step 15: Once the Citrix XenApp Server Role Manager dialog box automatically launches, click **Resume Install**, and then on the pop-up window, click **Install**.



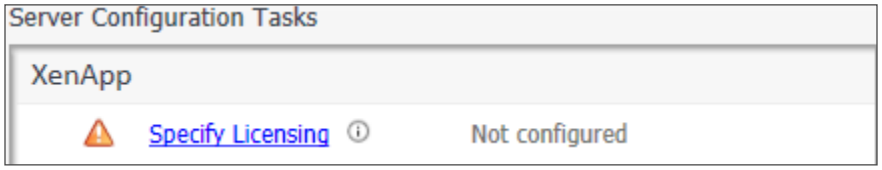
The additional server roles and services being to install.

Step 16: Follow the wizard installation instructions, including any required reboots, until the Successfully updated XenApp server roles page appears, and then click **Finish**.



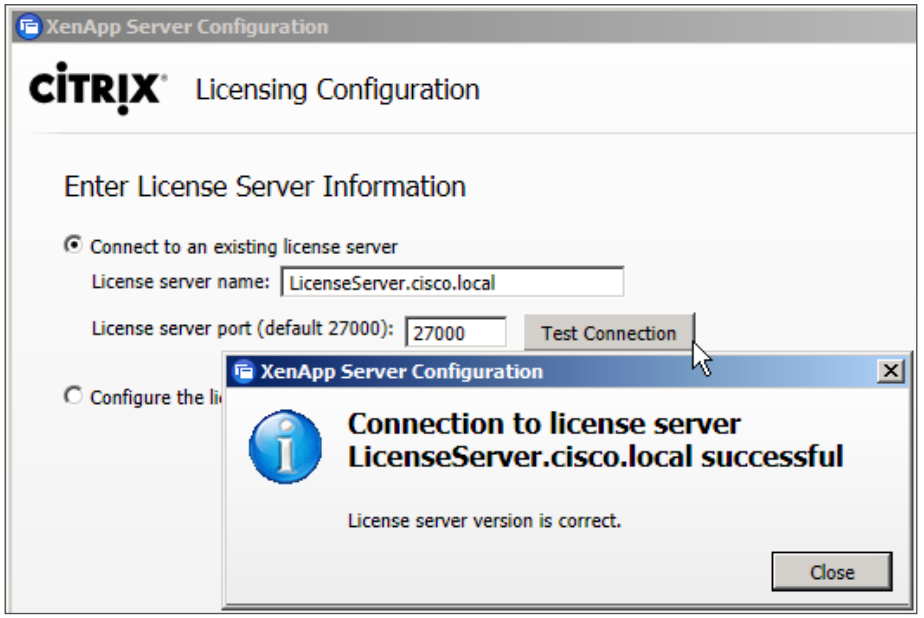
You are returned to the Citrix XenApp Server Role Manager.

Step 17: Click **Specify Licensing**.

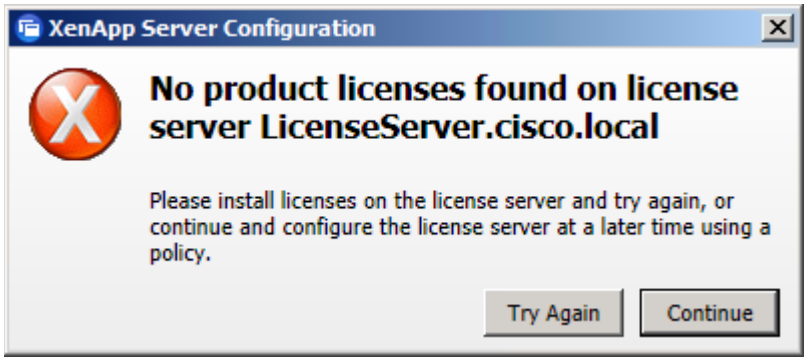


Step 18: In the Licensing Configuration wizard, on the Enter License Server Information page, in the **License server name** box, enter LicenseServer.cisco.local, and then click **Test Connection**.

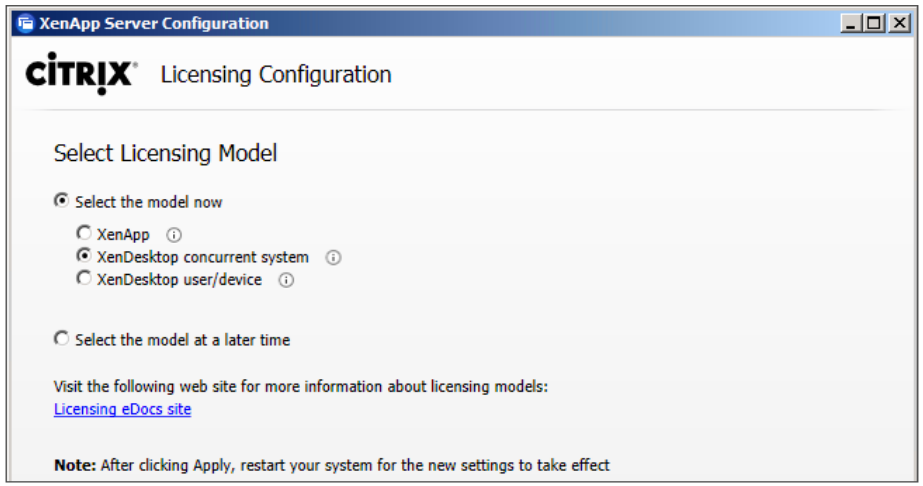
Step 19: On the "Connection to license server LicenseServer.cisco.local successful" message, click **Close**, and then on the Enter License Server Information page, click **Next**.



Step 20: On the "No product licenses found on license server" message, click **Continue**. You install licenses at a later time.



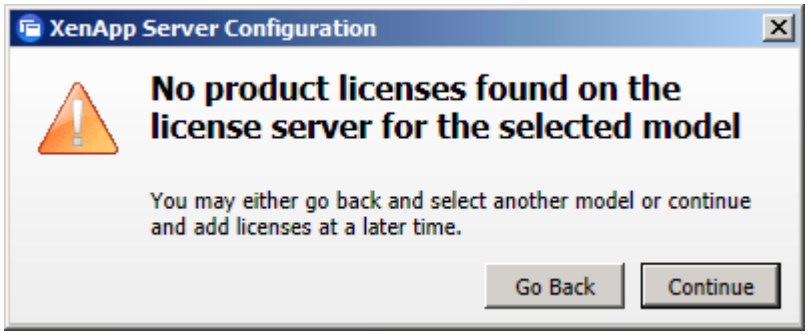
Step 21: On the Select Licensing Model page, select **Select the model now**, select **XenDesktop concurrent system**, and then click **Apply**.



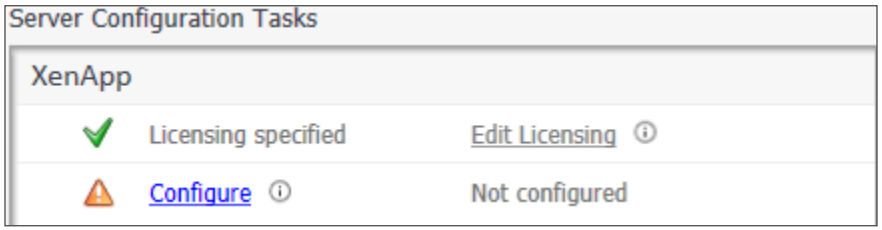
Reader Tip

Alternative licensing schemes may be better suited for some deployments. For more information, see the licensing information at the Citrix eDocs website:
http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html

Step 22: If licenses are not yet installed on your Citrix License Server, on the "No product licenses found on the license server or the selected model" message, click **Continue**.

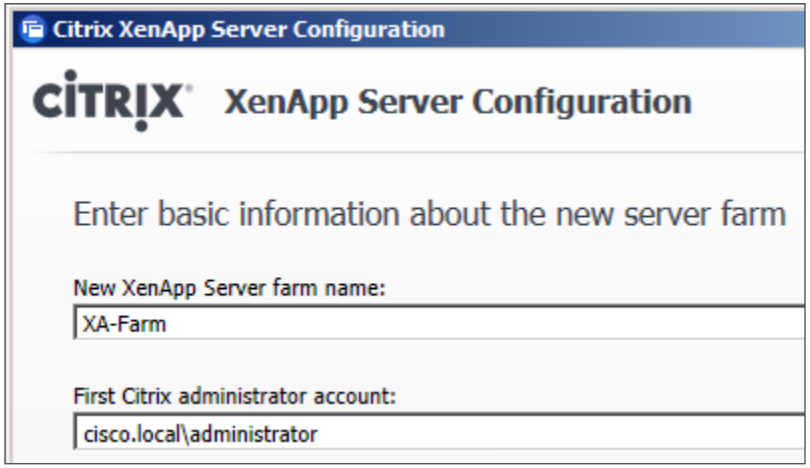


Step 23: On the Citrix XenApp Server Role Manager dialog box, under XenApp, click **Configure**.

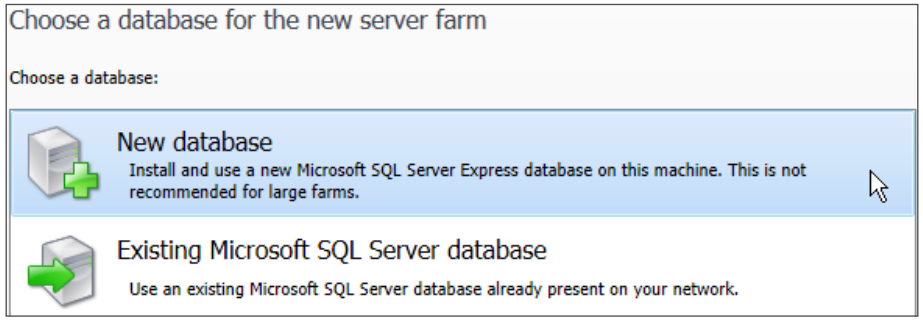


Step 24: In the Citrix XenApp Server Configuration wizard, on the Choose a task to perform page, select **Create a new server farm**.

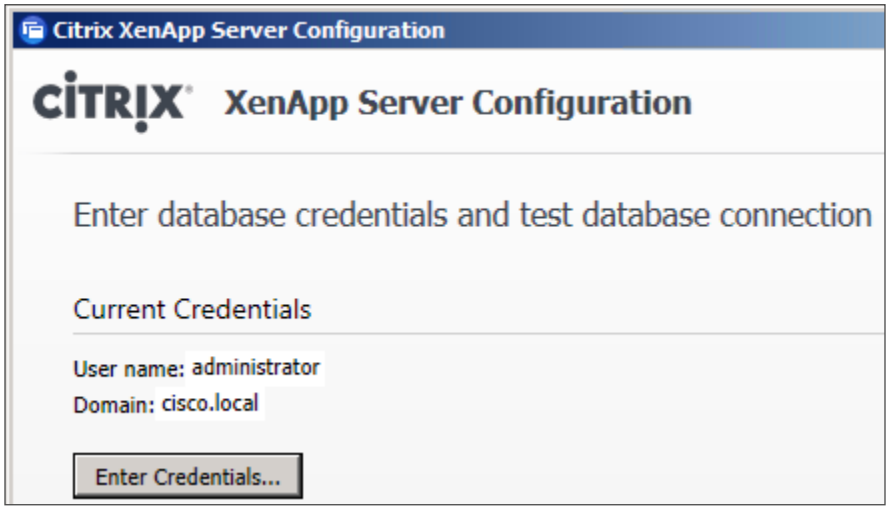
Step 25: On the Enter basic information about the new server farm page, in the **New XenApp Server farm name** box, enter XA-Farm, and in the **First Citrix administrator account** box, enter cisco.local\administrator, and then click **Next**.



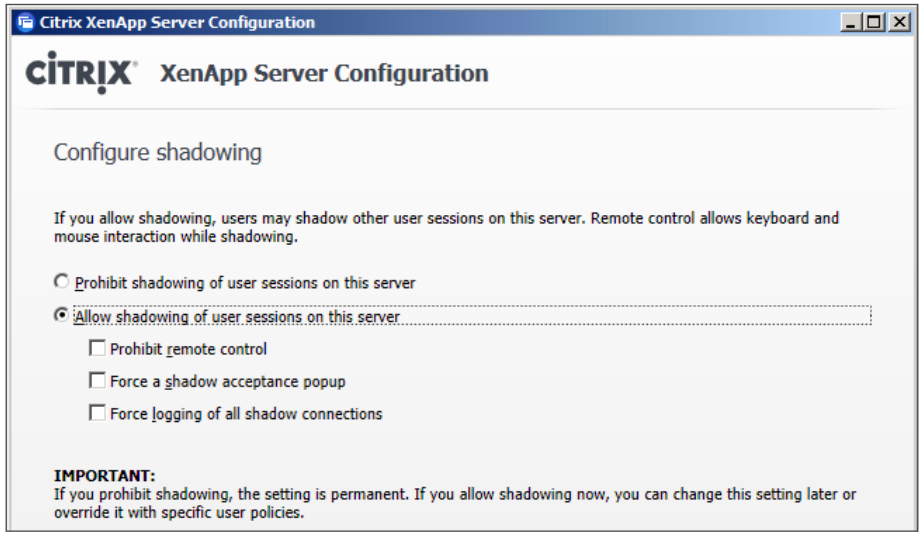
Step 26: On the Choose a database for the new server farm page, select **New database**, and then click **Next**.



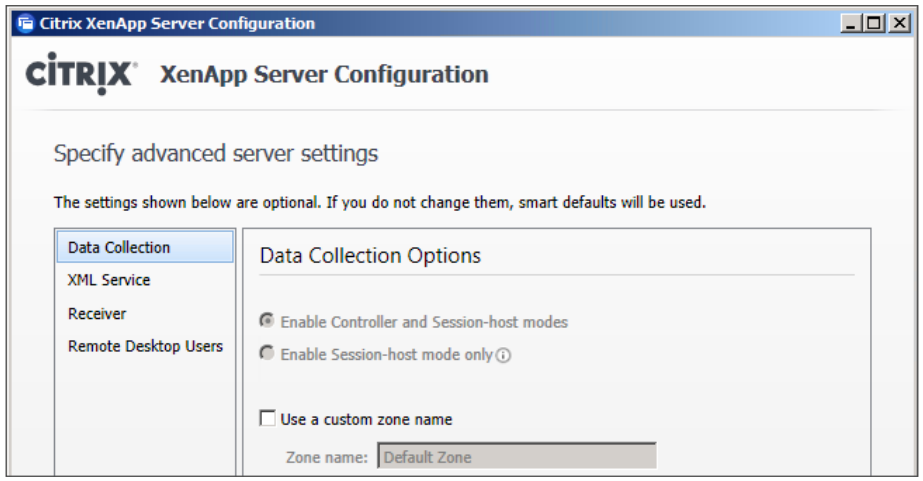
Step 27: On the Enter database credentials and test database connection page, click **Enter Credentials**, update the administrator password, and then click **Next**.



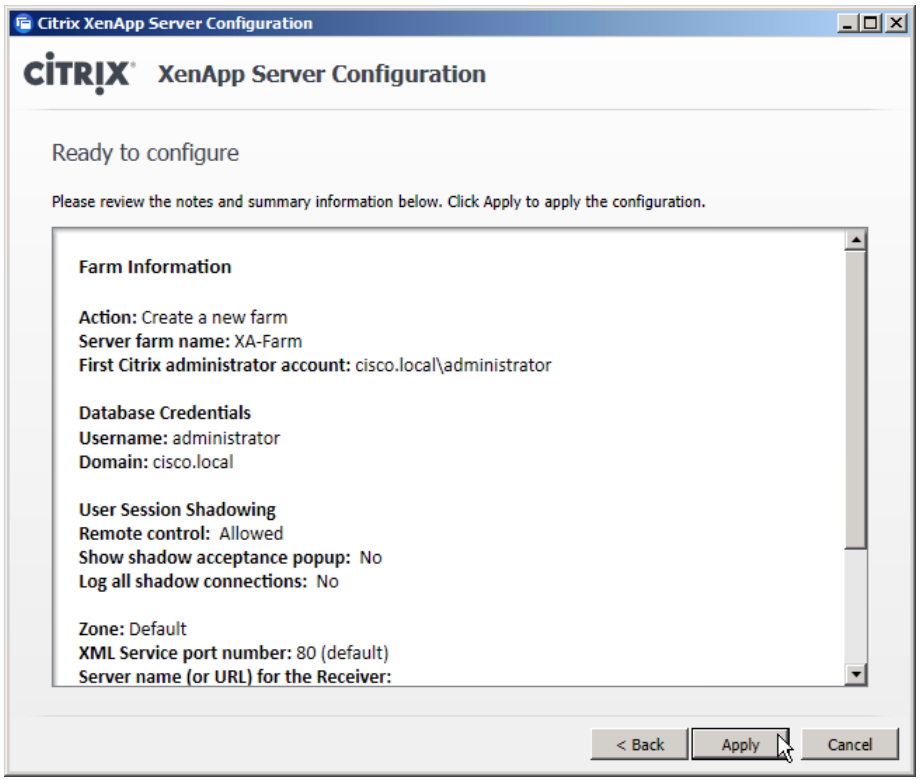
Step 28: On the Configure shadowing page, select **Allow shadowing of user sessions on this server**, and then click **Next**.



Step 29: On the Specify advanced server settings page, do not specify any advanced server settings, and then click **Next**.



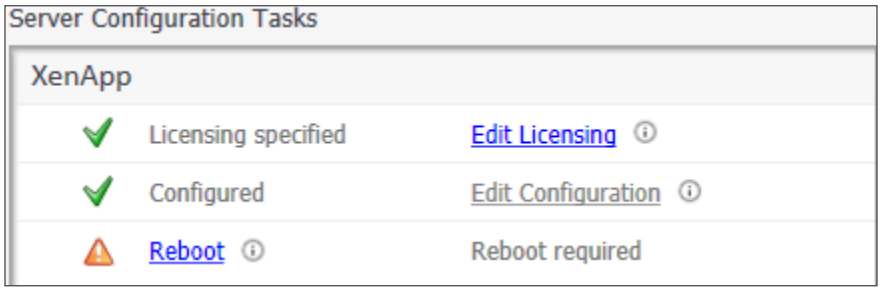
Step 30: On the Ready to configure page, review the settings, and then click **Apply**.



The Citrix XenApp Server Configuration wizard applies the additional settings.

Step 31: When the server configuration is completed successfully, click **Finish**.

Step 32: On the Citrix XenApp Server Role Manager dialog box, click **Reboot**, and then click **Yes**.



Step 33: After the reboot is complete, log in with administrator credentials and use the full domain format (Example: cisco.local\administrator).

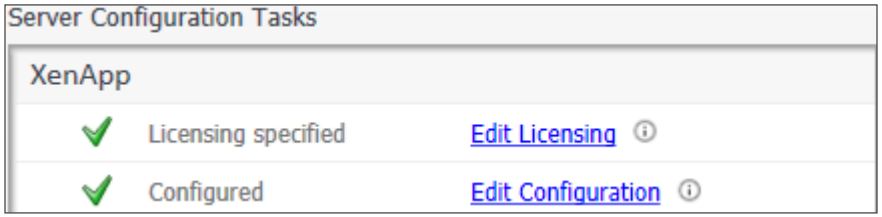
Caution

Log in using the full domain and username that you used during the installation, replacing any alternative domain and username that may be displayed. If you use credentials that are different than the installation credentials, the continuation of the installation does not launch automatically, and future installation screens are blank.

Step 34: If a license error displays, click **OK**.

Step 35: Before continuing, launch Windows Update, apply all updates, and reboot. At minimum, patches to .NET Framework are required. Repeat until all patches are applied.

The Citrix XenApp Server Role Manager dialog box automatically launches again, showing that XenApp is configured.



Procedure 2 Install additional Citrix XenApp VM

Additional Citrix XenApp servers are installed on virtual instances of Microsoft Windows Server 2008 R2. The virtual instances installed on the same hardware and hypervisor can scale better than a single large VM. For added resiliency, one or more of the additional Citrix XenApp VMs are installed on another host server.

You install Microsoft Windows Server 2008 R2 virtual machine instances (including VMware Tools) on the Cisco UCS hardware designated for infrastructure services. The following information is used.

Table 8 - High availability Citrix XenApp configuration values for Cisco UCS server 6

Component	Parameter	Cisco SBA value
H6: Cisco UCS server 6	Name in VMware vCenter	chas3-s6
	IP address	10.4.63.116
	Subnet mask	255.255.255.0
	Default gateway	10.4.63.1
HA XenApp virtual machine	Name in VMware vCenter	H6-XA4
	Destination storage	VDI shared-storage on NetApp
	Hard disk 1	Virtual disk with default 40 GB drive (C:/ drive)
	Network adapter 1	VMXNET 3 attached to VDI_Servers VLAN
	DNS name	XA4
	IP address	10.4.57.24
	Subnet mask	255.255.255.0
	Default gateway	10.4.57.1
	DNS and Active Directory server	10.4.48.10
	DNS and Active Directory domain	cisco.local

For each Windows Server instance, ensure that:

- Network connectivity is configured and available
- Windows OS license is activated
- Windows Server patches are applied
- Microsoft Active Directory domain is joined (prerequisite for site configuration step)

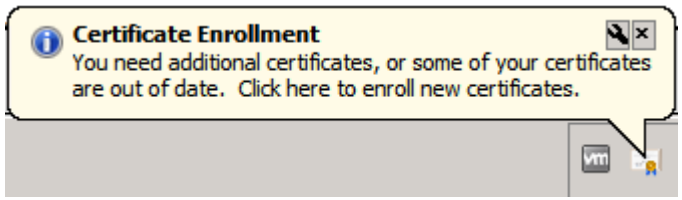
The following Windows Server prerequisite for the Citrix XenApp installation does not need to be installed at this time, because the installation software detects that it is not installed and then automatically launches the installation:

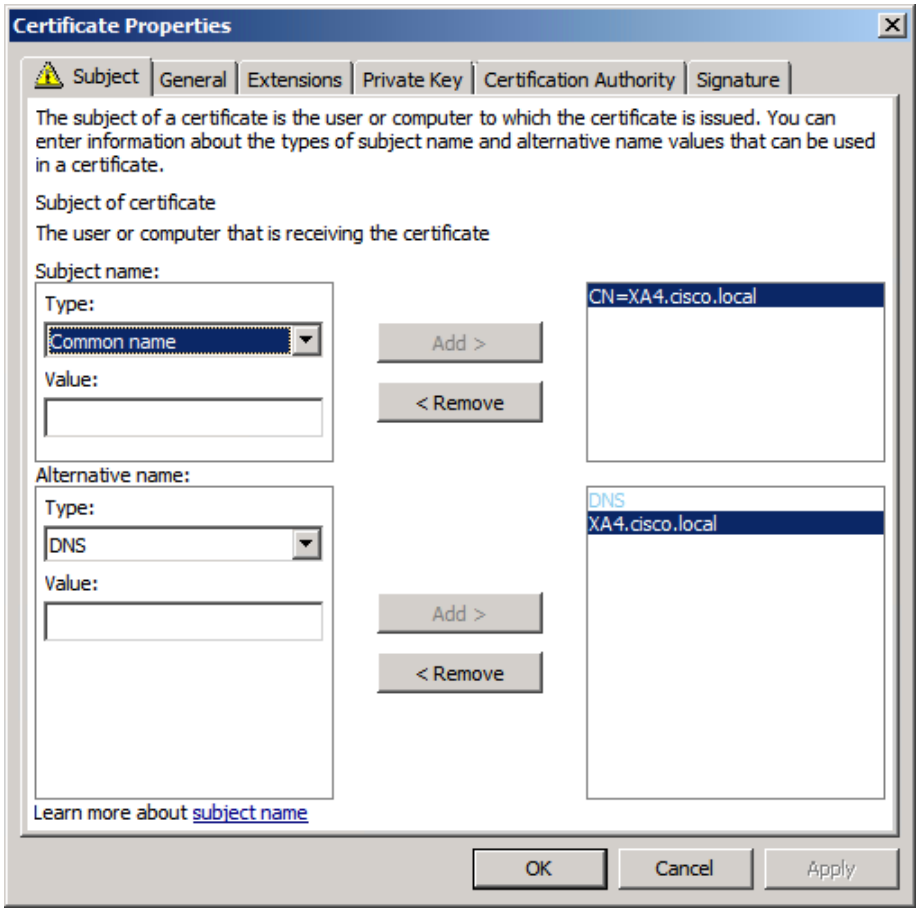
- Microsoft .NET Framework 3.5 Service Pack 1

Step 1: On Cisco UCS server 6, install a Microsoft Windows Server 2008 R2 virtual machine instance and VMware Tools, configure network connectivity by using the values above, activate Windows, join the Active Directory domain and apply Windows Update patches. When joining the domain and applying the patches, you will be prompted to reload the VM. This virtual machine is the H6-XA4 instance.

Step 2: After reloading for updates and Active Directory changes is complete, return to the H6-XA4 VM console, and then log in to the Active Directory domain as a user with administrative privileges (Example: cisco.local\administrator).

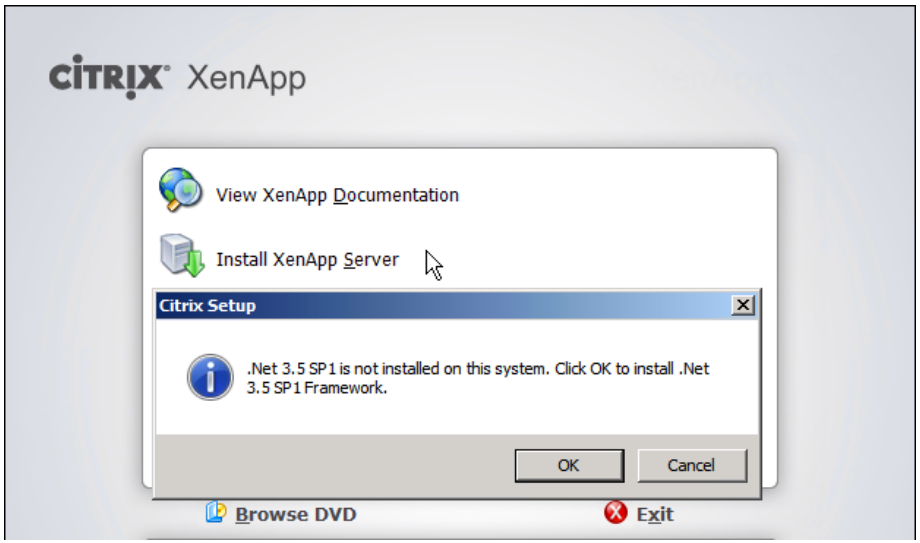
Step 3: If the Active Directory domain requires setup of a certificate for the SCEP service, a message is displayed. Click on the taskbar icon, and then complete the certificate enrollment.





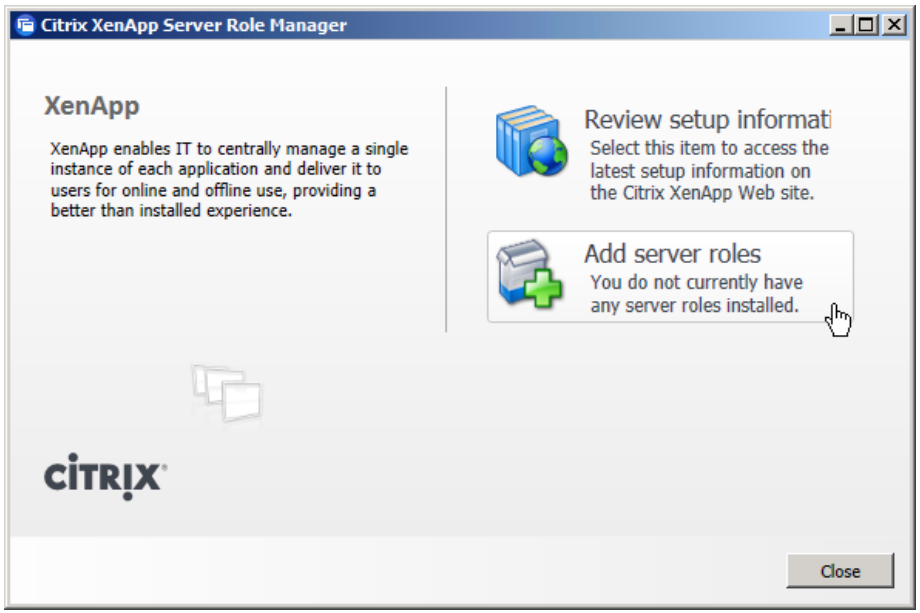
Step 4: In VMware vCenter, mount the Citrix XenApp ISO image to the H6-XA4 virtual machine, and then allow the AutoPlay service to launch the Citrix AutoSelect.exe XenApp installer. The first XenApp installation page is displayed.

Step 5: Click **Install XenApp Server**, and then on the ".Net 3.5 SP1 is not installed on this system" message, click **OK**.



The .Net installation begins, and then the Citrix XenApp installation launches.

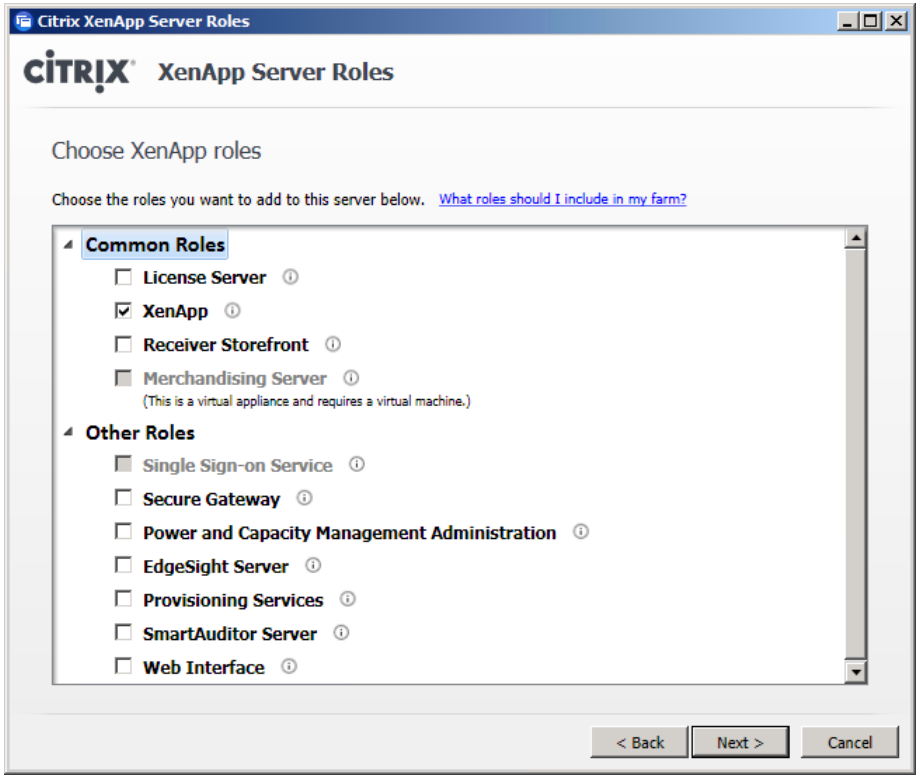
Step 6: When the Citrix XenApp Server Role Manager dialog box appears, click **Add server roles**.



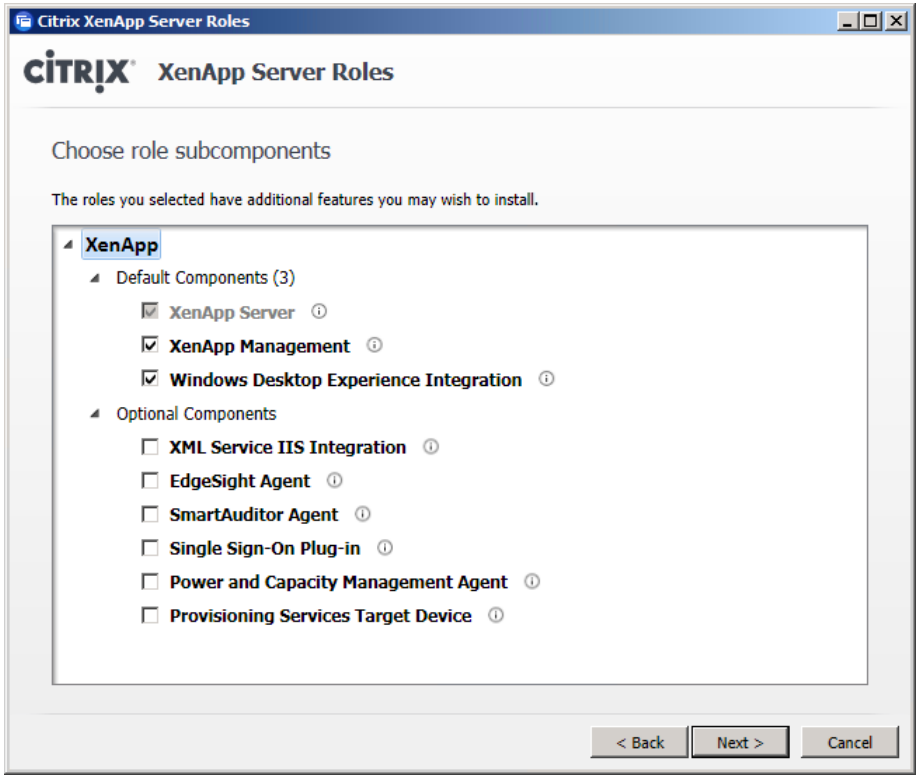
Step 7: In the Citrix XenApp Server Roles wizard, select a Citrix XenApp edition to use for the installation. This procedure uses the Platinum Edition.

Step 8: Accept the license agreement, and then click **Next**.

Step 9: On the Choose XenApp roles page, select **XenApp**, and then click **Next**.

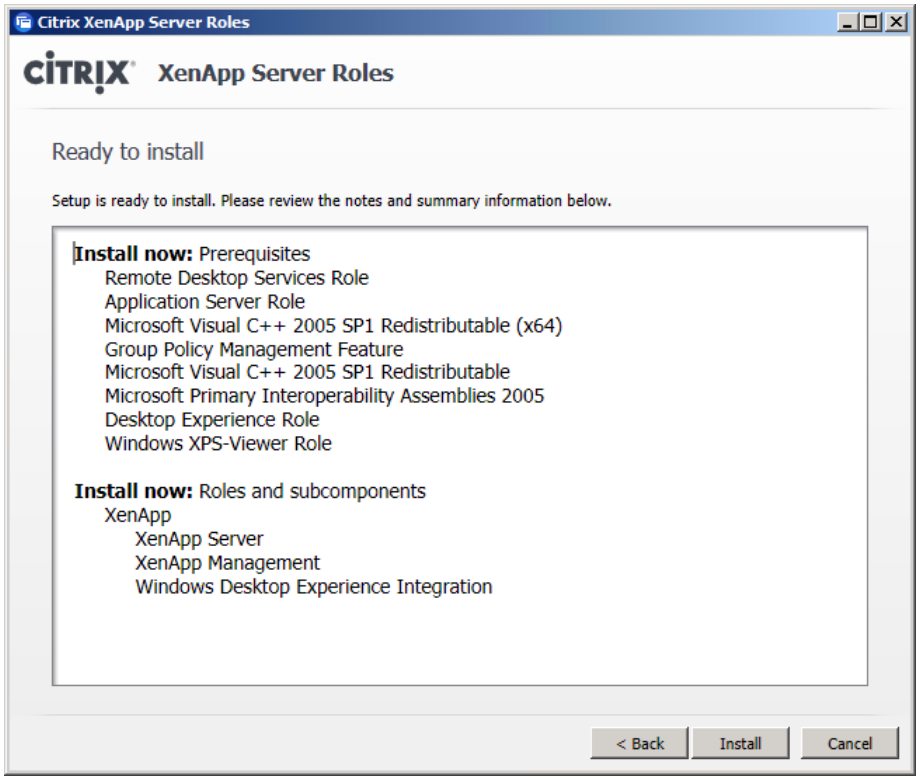


Step 10: On the Choose role subcomponents page, leave the default selections, and then click **Next**.



Step 11: On the Review Prerequisites page, review the prerequisites, and then click **Next**.

Step 12: On the Ready to install page, click **Install**.

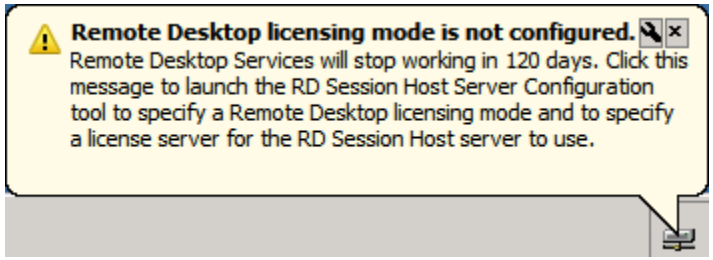


The installation begins.

Step 13: Continue to follow the instructions to complete the wizard installation activity, and select **Reboot** whenever prompted.

Step 14: Log in to the H6-XA4 VM with the same administrator credentials that you used during installation.

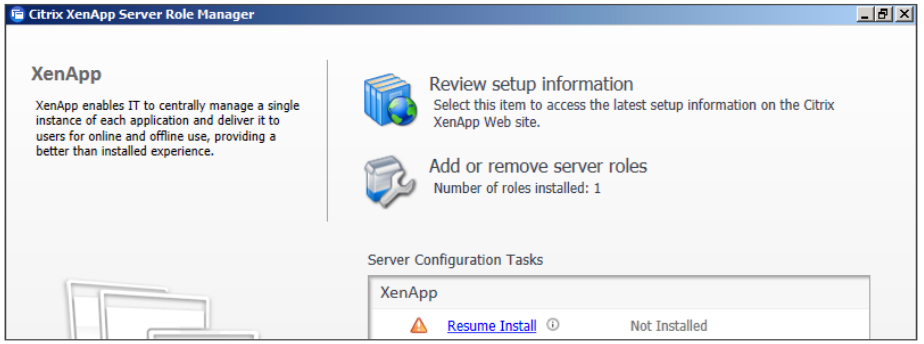
After rebooting and logging in with administrator credentials, a Microsoft Remote Desktop Services licensing message appears. You address this message at a later time.



Caution

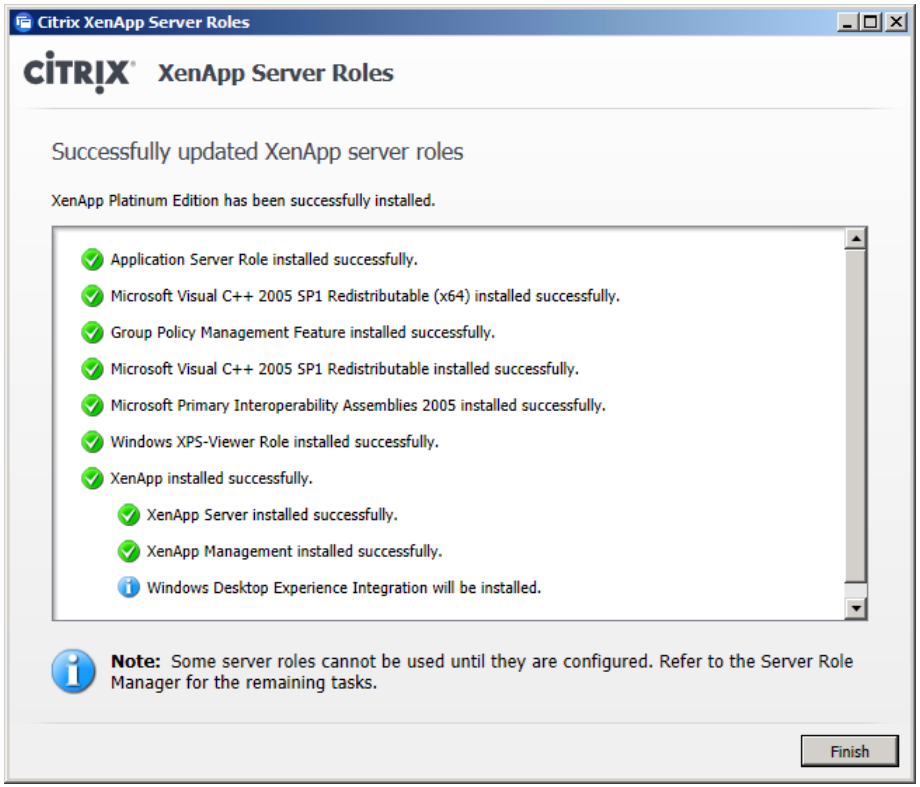
Log in using the full domain and username that you used during the installation, replacing any alternative domain and username that may be displayed. If you use credentials that are different than the installation credentials, the continuation of the installation does not launch automatically, and future installation screens are blank.

Step 15: Once the Citrix XenApp Server Role Manager dialog box automatically launches, click **Resume Install**, and then on the pop-up window, click **Install**.



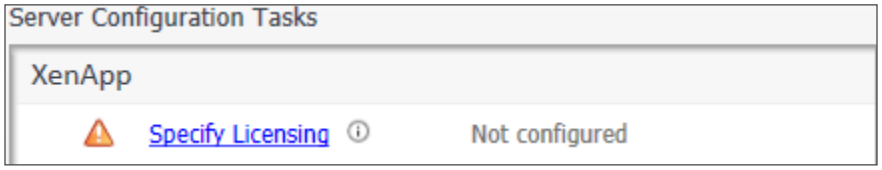
The additional server roles and services begin to install.

Step 16: Follow the wizard installation instructions, including any required reboots, until the Successfully updated XenApp server roles page appears, and then click **Finish**.



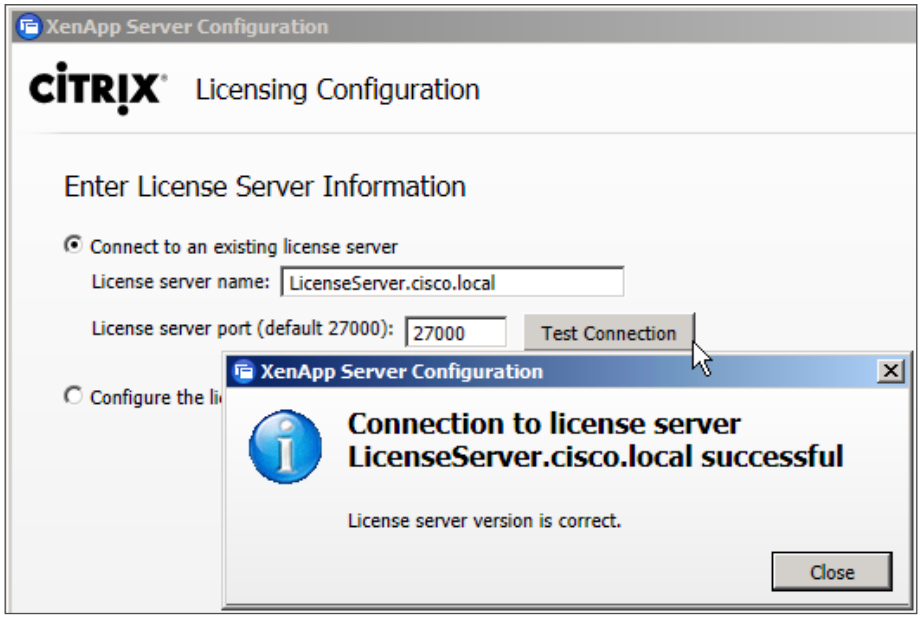
You are returned to the Citrix XenApp Server Role Manager.

Step 17: Click **Specify Licensing**.

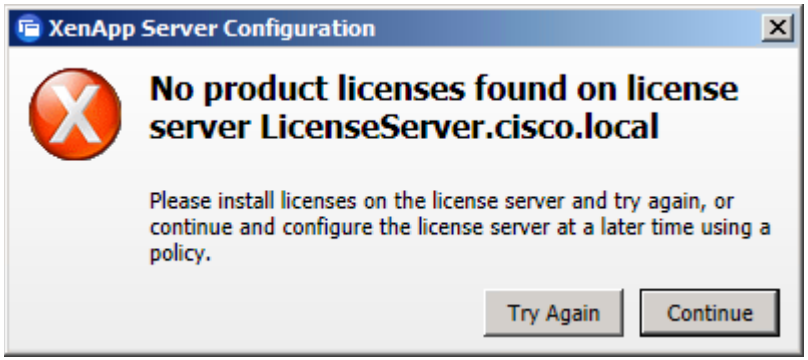


Step 18: In the Licensing Configuration wizard, on the Enter License Server Information page, in the **License server name** box, enter LicenseServer.cisco.local, and then click **Test Connection**.

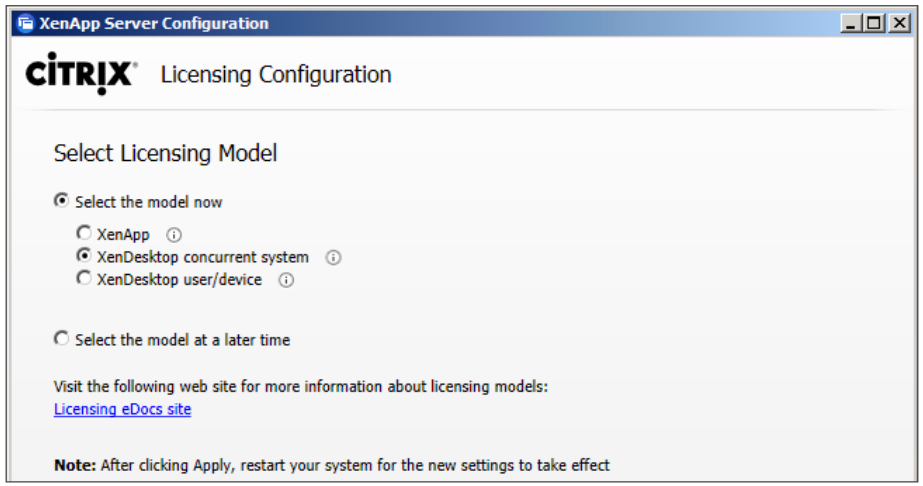
Step 19: On the "Connection to license server LicenseServer.cisco.local successful" message, click **Close**, and then on the Enter License Server Information page, click **Next**.



Step 20: On the "No product licenses found on license server" message, click **Continue**.



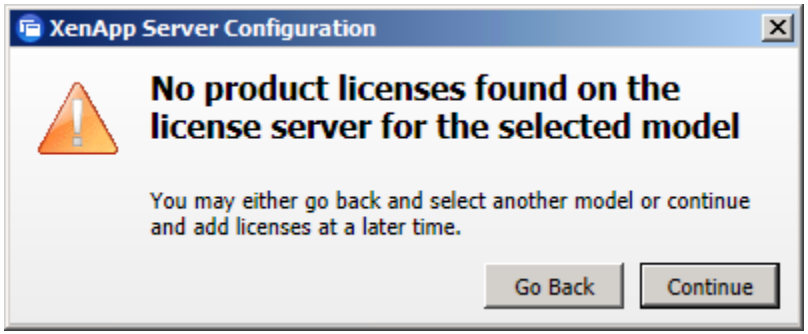
Step 21: On the Select Licensing Model page, select **Select the model now**, select **XenDesktop concurrent system**, and then click **Apply**.



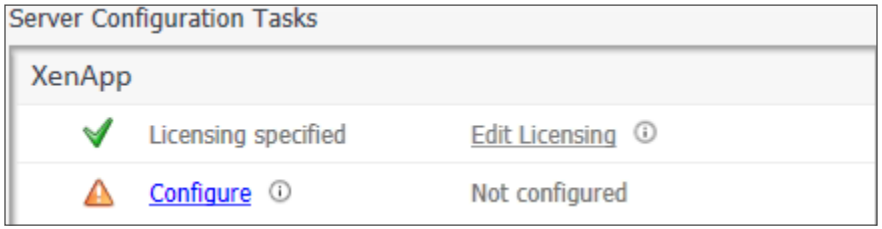
Reader Tip

Alternative licensing schemes may be better suited for some deployments. For more information, see the licensing information at the Citrix eDocs website: http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html

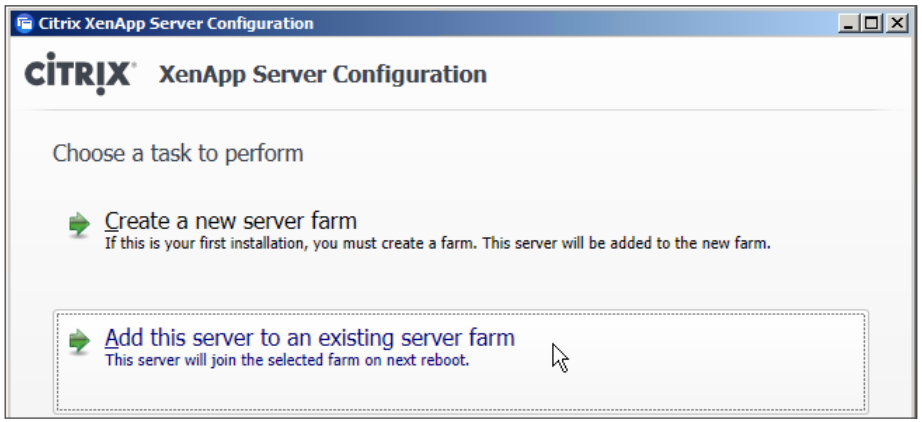
Step 22: If licenses are not yet installed on your Citrix License Server, on the "No product licenses found on the license server or the selected model" message, click **Continue**.



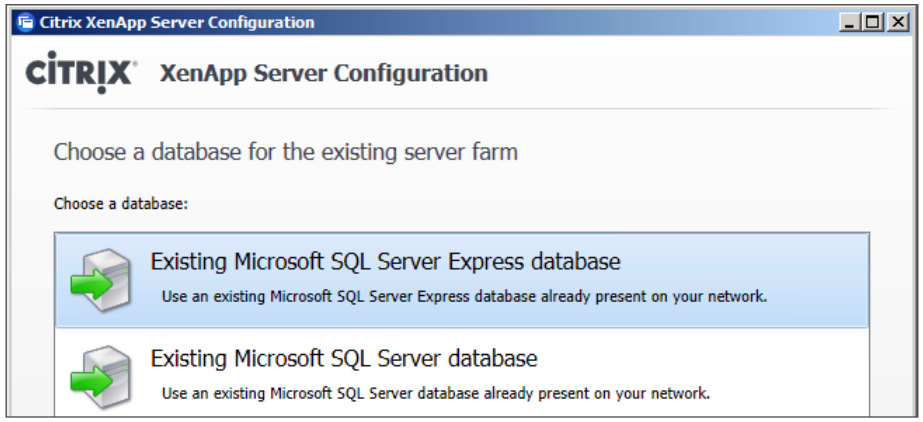
Step 23: On the Citrix XenApp Server Role Manager dialog box, under XenApp, click **Configure**.



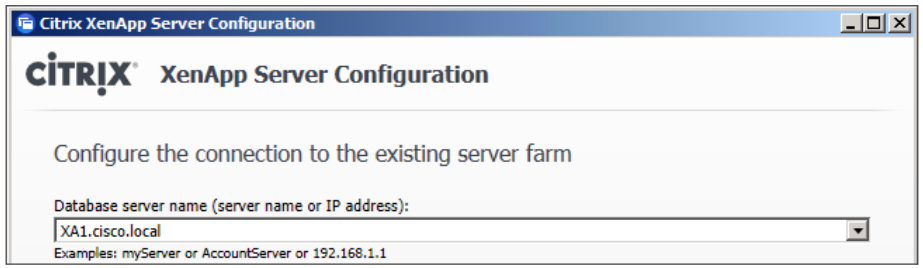
Step 24: In the Citrix XenApp Server Configuration wizard, on the Choose a task to perform page, select **Add this server to an existing server farm**.



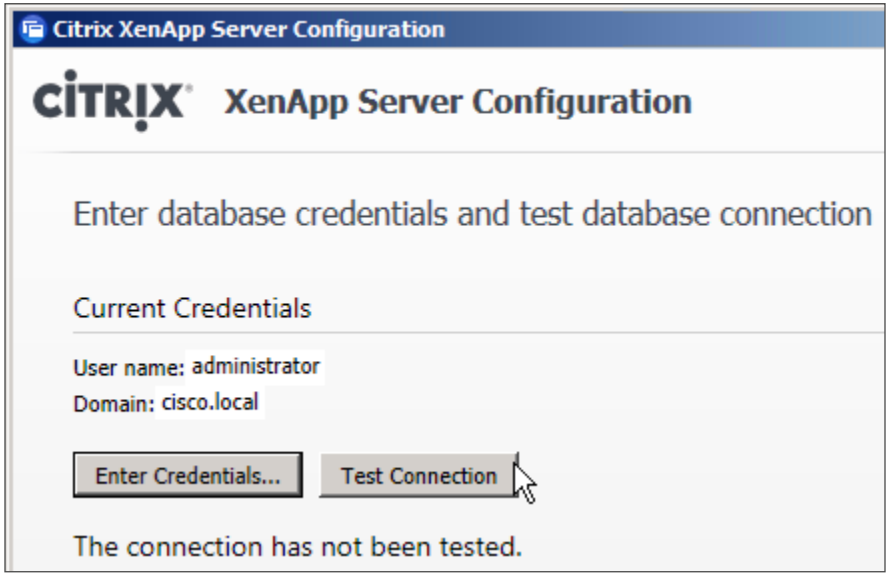
Step 25: On the Choose a database for the existing server farm page, select **Existing Microsoft SQL Server Express database**, and then click **Next**.



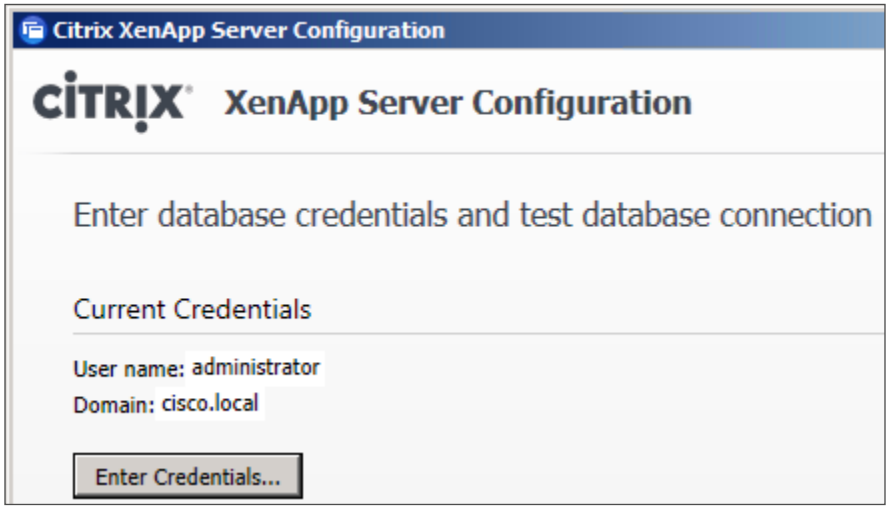
Step 26: On the Configure the connection to the existing server farm page, in the **Database server name** box, enter XA1.cisco.local, and then click **Next**.



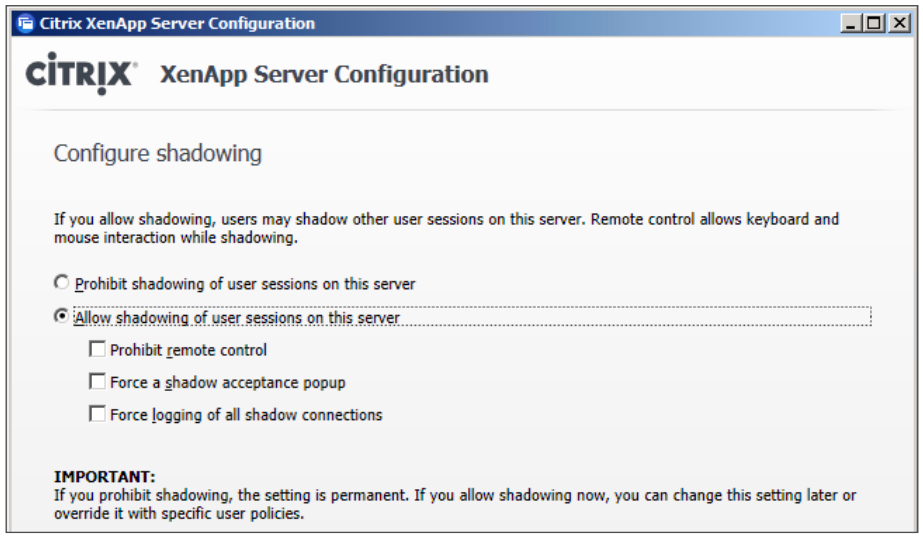
Step 27: On the Enter database credentials and test database connection page, click **Enter Credentials**, enter the administrator username and password (Example: cisco.local\administrator), click **Next**, and then on the wizard page, click **Test Connection**.



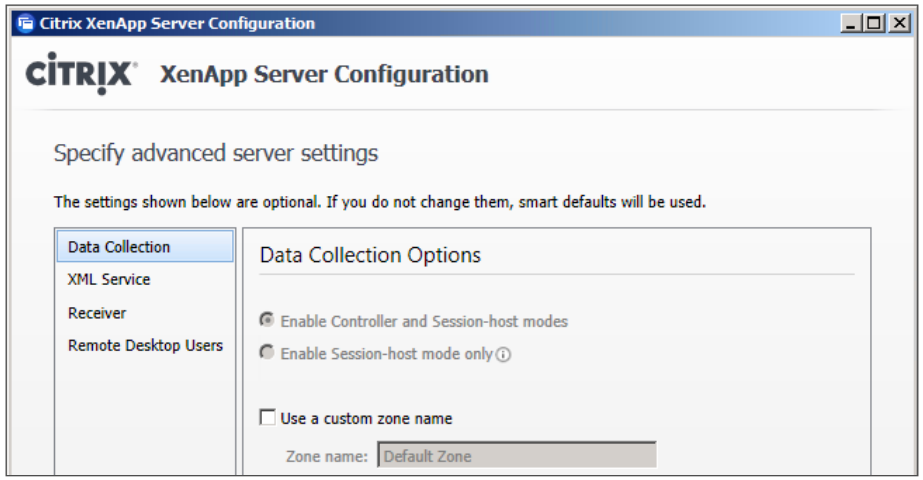
Step 28: On the "Test completed successfully" message, click **OK**, and then on the Enter database credentials and test database connection page, click **Next**.



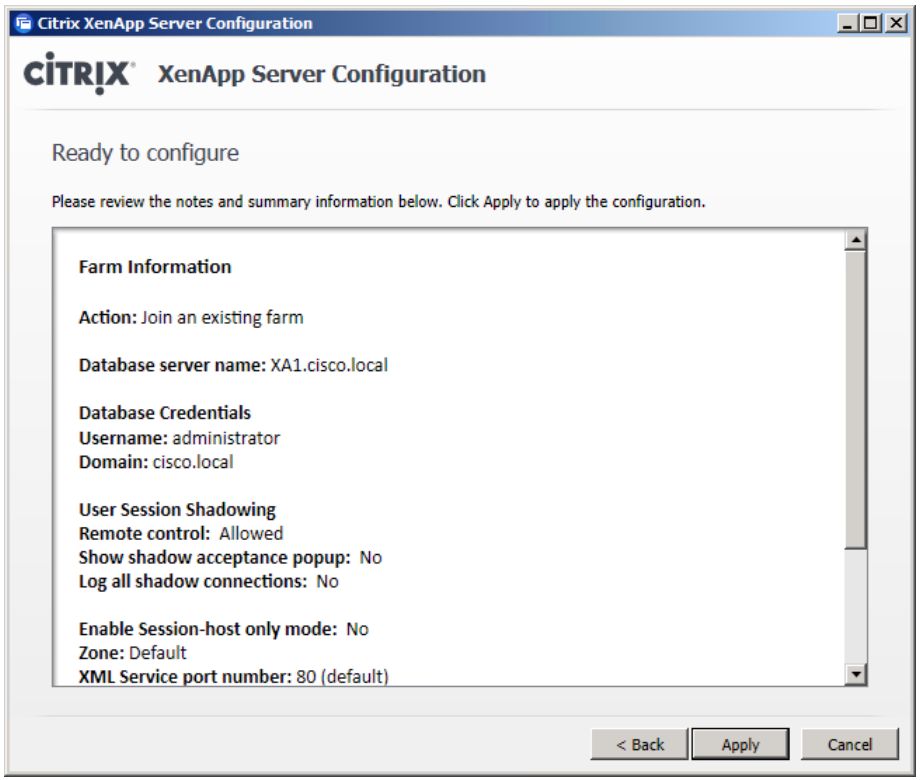
Step 29: On the Configure shadowing page, select **Allow shadowing of user sessions on this server**, and then click **Next**.



Step 30: On the Specify advanced server settings page, do not specify any advanced server settings, and then click **Next**.



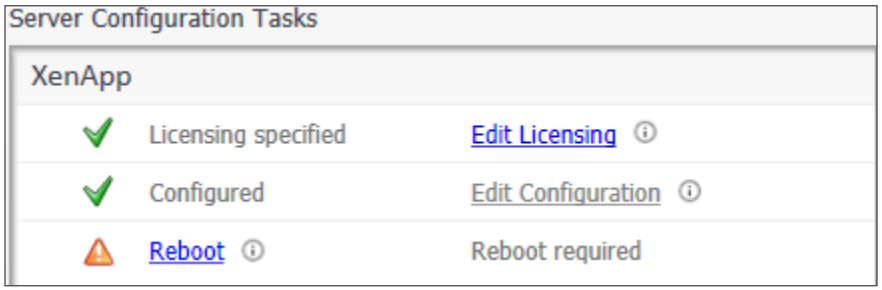
Step 31: On the Ready to configure page, review the settings, and then click **Apply**.



The Citrix XenApp Server Configuration wizard applies the additional settings.

Step 32: When the server configuration is completed successfully, click **Finish**.

Step 33: On the Citrix XenApp Server Role Manager dialog box, click **Reboot**, and then click **Yes**.



Step 34: After the reboot is complete, log in with administrator credentials and use the full domain format (Example: cisco.local\administrator).

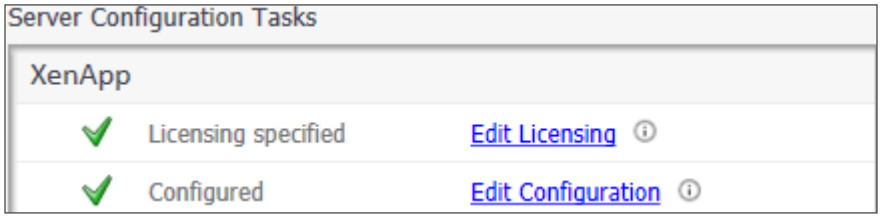
Caution

Log in using the full domain and username that you used during the installation, replacing any alternative domain and username that may be displayed. If you use credentials that are different than the installation credentials, the continuation of the installation does not launch automatically, and future installation screens are blank.

Step 35: If a license error displays, click **OK**.

Step 36: Before continuing, launch Windows Update, apply all updates, and reboot. At minimum, patches to .NET Framework are required. Repeat until all patches are applied.

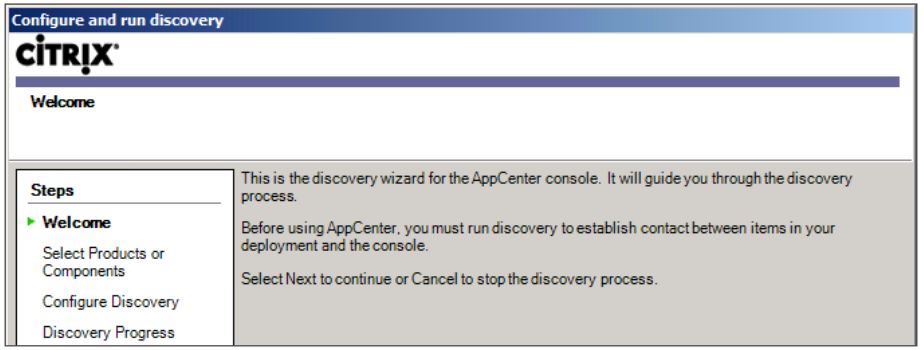
The Citrix XenApp Server Role Manager dialog box automatically launches again, showing that XenApp is configured on the additional server.



Step 37: If you choose to deploy additional Citrix XenApp servers, repeat this procedure to create and add all remaining XenApp servers to the XA-Farm farm.

Procedure 3 Configure the Citrix XenApp farm

Step 1: From the console of the H4-XA1 VM (Example: XA1.cisco.local), navigate to **Start** > **Administrative Tools** > **Citrix** > **Management Consoles**, and then choose **Citrix AppCenter**. The Citrix AppCenter management console appears.

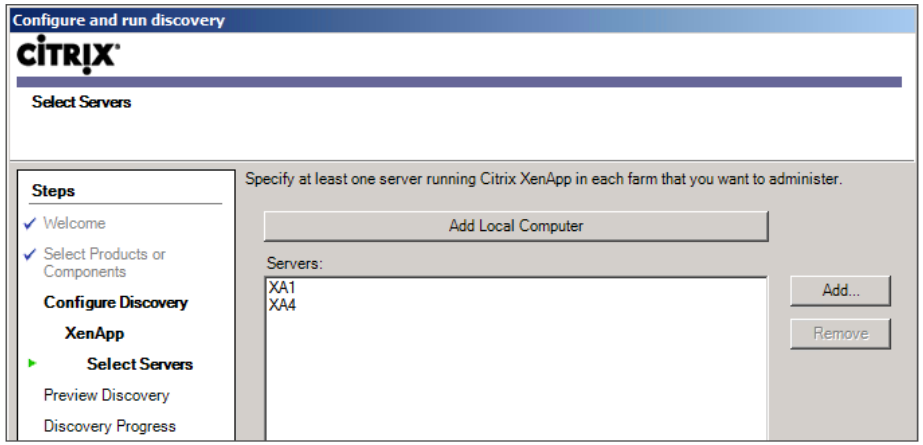


Step 2: In the Configure and run discovery wizard, on the Welcome page, click **Next**.

Step 3: On the Select Products or Components page, clear **Single Sign-On**, and then click **Next**.

Step 4: On the Select Servers page, click **Add Local Computer**.

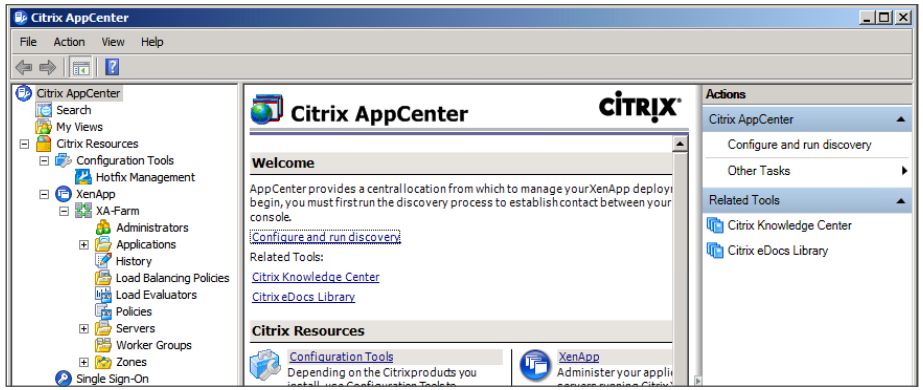
Step 5: Click **Add**, enter the DNS name of an additional XenApp server that you want to manage (Example: XA4), and then click **OK**. Repeat adding additional servers as configured in your environment.



Step 6: On the Select Servers page, click **Next**.

Step 7: On the Preview Discovery page, click **Next**.

Step 8: On the Discovery Progress page, click **Finish**. You have completed the Configure and run discovery wizard, and Citrix AppCenter appears.



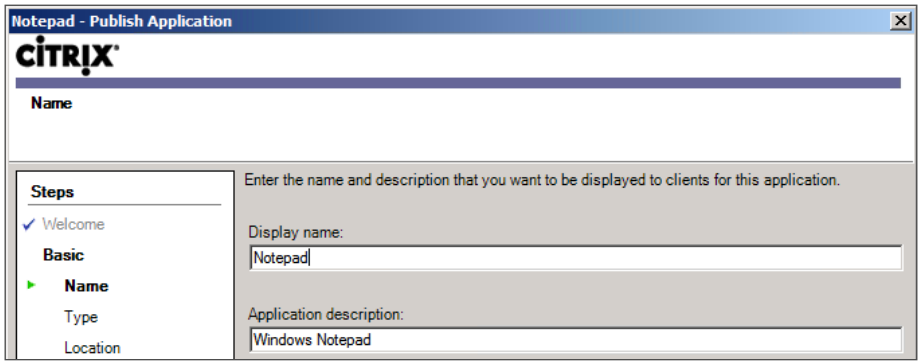
Procedure 4 Publish a virtual application

The following steps show how to publish Windows Notepad as a virtual application, and you can apply this procedure to any available application.

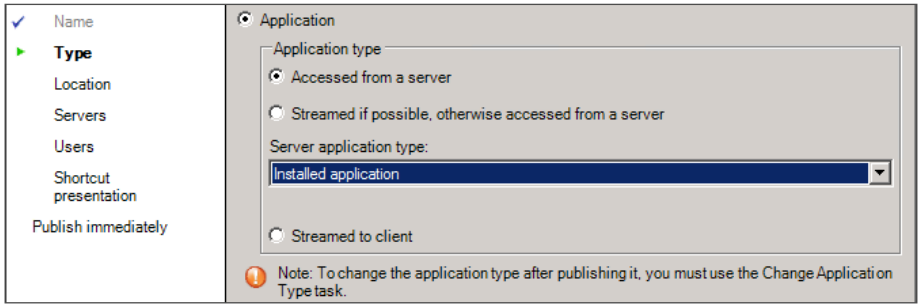
Step 1: In the tree, expand **XA-Farm**, right-click **Applications**, and then choose **Publish application**. The Publish Application wizard launches.

Step 2: On the Welcome page, click **Next**.

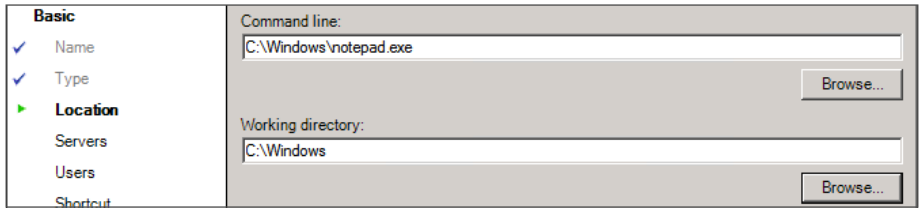
Step 3: On the Name page, in the **Display name** box, enter **Notepad**, in the **Application description** box, enter **Windows Notepad**, and then click **Next**.



Step 4: On the Type page, keep the default selections of **Application**, **Accessed from a server**, and **Installed application**, and then click **Next**.



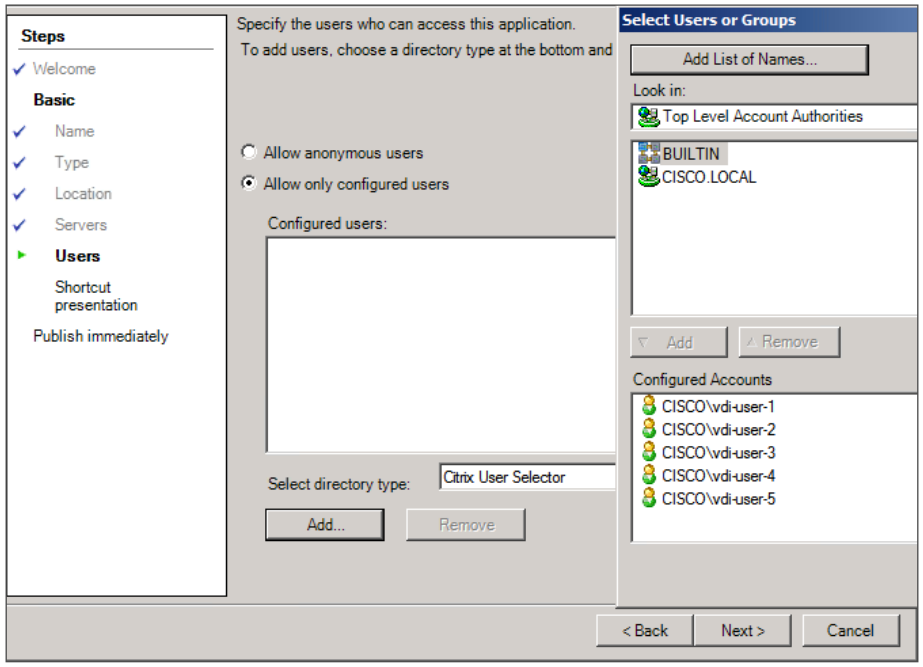
Step 5: On the Location page, for **Command line**, click **Browse**, navigate to **notepad.exe** and select it, and in the **Working directory** box, enter **C:\Windows**, and then click **Next**.



Step 6: On the Select Servers page, in the **Look in** list, choose **XA-Farm**, click the **Servers** folder, and click **Add All** to select all the created servers, including **XA1** and **XA4**, and then click **Next**.

You have selected the servers on which you want to virtualize the **notepad.exe** application.

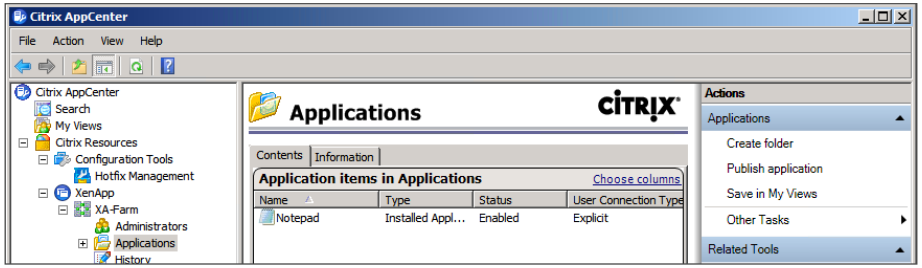
Step 7: On the Users page, select **Allow only configured users**, click **Add**, and then in the Select Users or Groups dialog box, select the appropriate Active Directory users or groups for which you want to enable access, and then click **Next**. This example adds users **CISCO\vdi-user-1** through **CISCO\vdi-user-5**.



Step 8: On the Shortcut presentation page, keep the default selections, and then click **Next**.

Step 9: On the Publish immediately page, keep the default selections, and then click **Finish**.

The published application appears in Citrix AppCenter.

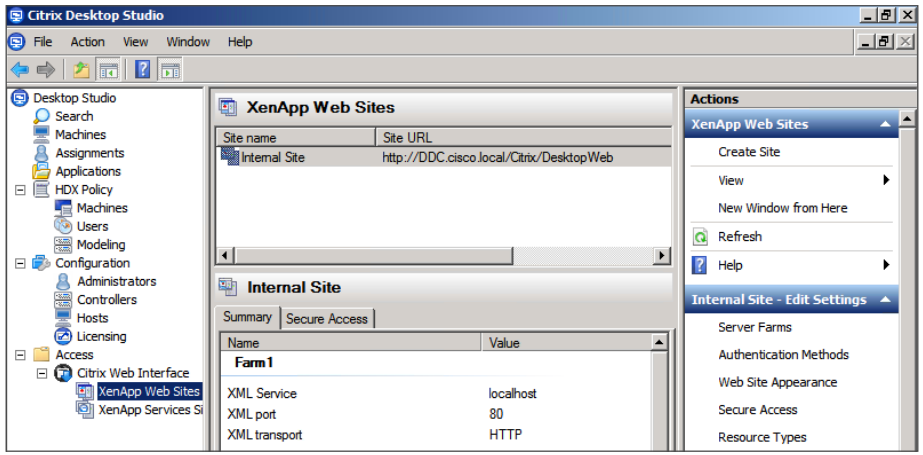


Procedure 5 Configure and test application delivery

The Citrix Web Interface functionality installed with Citrix XenDesktop is also used to access the applications published by Citrix XenApp, presenting a unified view of virtual desktops and virtual applications. Citrix Web Interface was automatically configured with the XenDesktop farm for virtual desktop delivery, and the XenApp farm is now added for delivery.

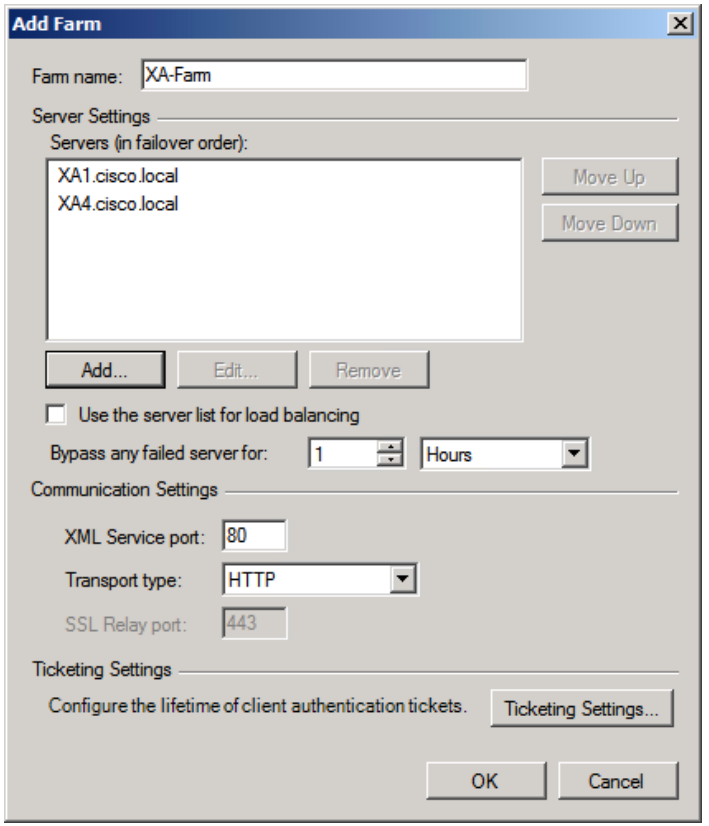
Step 1: From the console of the **H1-DDC** VM (Example: DDC.cisco.local), log in using the credentials for **cisco.local\administrator**, and then open Citrix Desktop Studio.

Step 2: In Citrix Desktop Studio, in the tree, navigate to **Access** > **Citrix Web Interface**, and then click **XenApp Web Sites**.

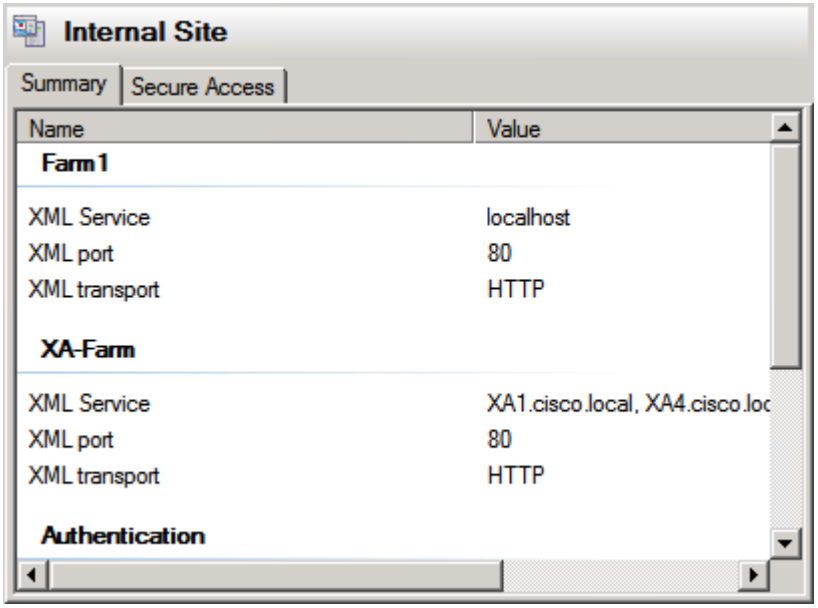


Step 3: On the right, in the **Actions** pane, select **Server Farms**, and then click **Add**.

Step 4: In the Add Farm dialog box, in the **Farm name** box, enter XA-Farm, click **Add**, enter the XA1.cisco.local and XA4.cisco.local servers, and then click **OK**.



In Citrix Desktop Studio, in the Internal Site pane, the XA-Farm XenApp farm is now listed with the Farm1 Citrix XenDesktop farm.

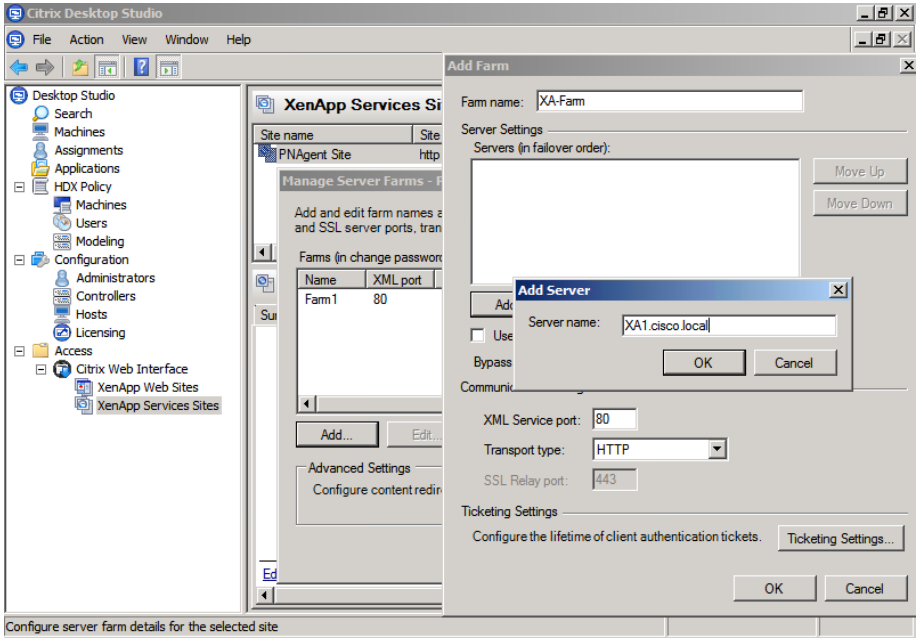


Step 5: In Citrix Desktop Studio, in the tree, navigate to **Access** > **Citrix Web Interface**, and then click **XenApp Services Sites**.

Step 6: On the right, in the Actions pane, select **Server Farms**, and then click **Add**.

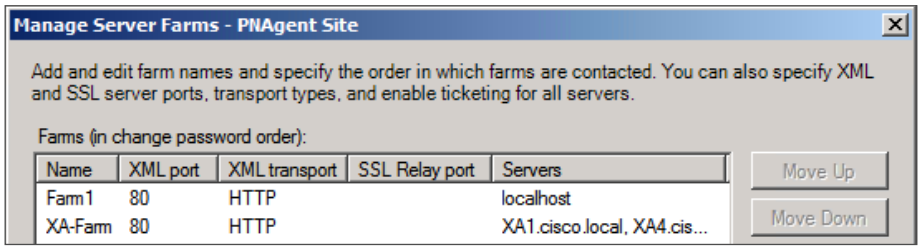
Step 7: On the Add Farm dialog box, in the **Farm name** box, enter XA-Farm, and then click **Add**.

Step 8: On the Add Server dialog box, in the **Server name** box, enter XA1.cisco.local, and then click **OK**.



Step 9: For each additional XenApp server configured, click **Add**, enter the **Server name** (Example: XA4.cisco.local), and then click **OK**.

Step 10: Once you have completed adding servers, on the Add Server dialog box, click **OK**. The additional application farm and servers are displayed.



Step 11: On the Manage Server Farms dialog box, click **OK**. The applications published by Citrix XenApp are now available to be accessed in Citrix Receiver, along with the published desktops from Citrix XenDesktop.

Step 12: In a web browser, open a connection to the H1-DDC VM (Example: DDC.cisco.local).

Step 13: In the **User name** and **Password** boxes, enter the user credentials for a user that has access to the virtual application that you wish to test (Example: vdi-user-1) and in the **Domain** box, enter **cisco.local**, and then click **Log On**.

The newly added Notepad application is displayed along with available desktops, and you can launch any application or desktop from this interface and also from installed Citrix Receiver clients.

Process

Installing and Testing Citrix Receiver Access

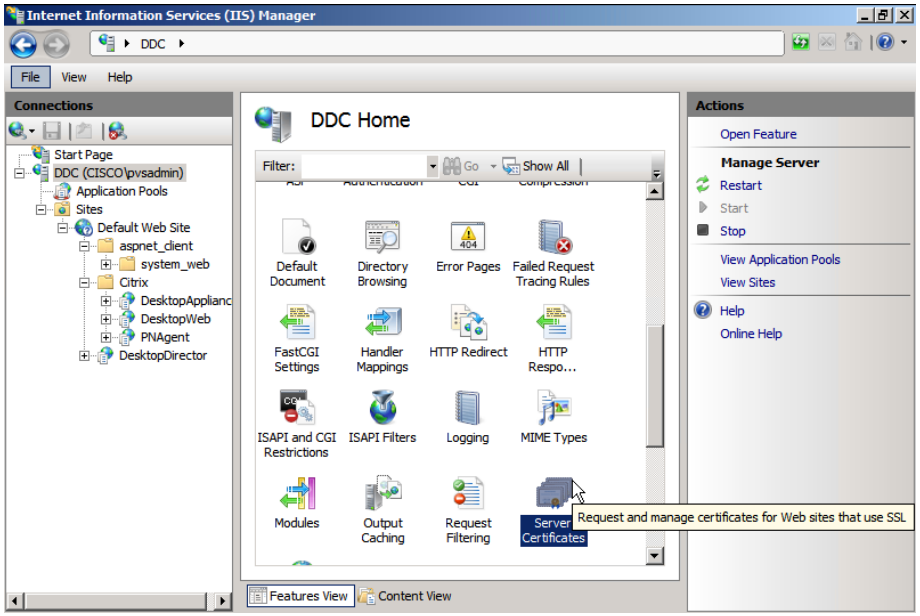
1. Enable SSL on the web servers
2. Configure Citrix Receiver
3. Observe optimized WAN for Citrix Receiver

The Citrix XenDesktop deployment uses the Internet Information Services (IIS) web server role installed in Windows Server 2008 R2. For some Citrix Receiver applications, an SSL connection is required, so you must enable this connectivity on the web server.

Procedure 1 Enable SSL on the web servers

Step 1: In VMware vCenter, log in to the console of the VM running the Microsoft IIS web server with administrator privileges (Example: DDC.cisco.local), and then launch the Internet Information Services (IIS) Manager tool.

Step 2: In the tree, navigate to **DDC**, at the bottom of the screen, click **Features View**, and then in the DDC Home pane, double-click **Server Certificates**.



Step 3: In the Actions pane, double-click **Create Certificate Request**, fill out the server information, save the request file, and then use it as a request to your CA. If you are using a local Microsoft CA for proof-of-concept purposes, the URL for the request is in the format http://ca.cisco.local/certsrv.

Step 4: In the IIS Manager Server Certificates Actions pane, select **Complete Certificate Request**. This uses the signed certificate returned by the CA and imports it into the web server.

Step 5: In IIS Manager, in the tree, navigate to **DDC > Sites > Default Web Site**, and then in the **Actions** pane, click **Bindings**.

Step 6: Click **Add**, in the **Type** list, select **https**, and in the **SSL certificate** list, select the new certificate, click **OK to accept the changes**, and then click **Close**.

Step 7: In the Actions pane, click **Restart**. The web server can now be accessed by using HTTPS with SSL.

Step 8: Repeat all previous steps in this procedure on the web servers built for the deployment. This enables the same functionality, for high availability.

Procedure 2 Configure Citrix Receiver

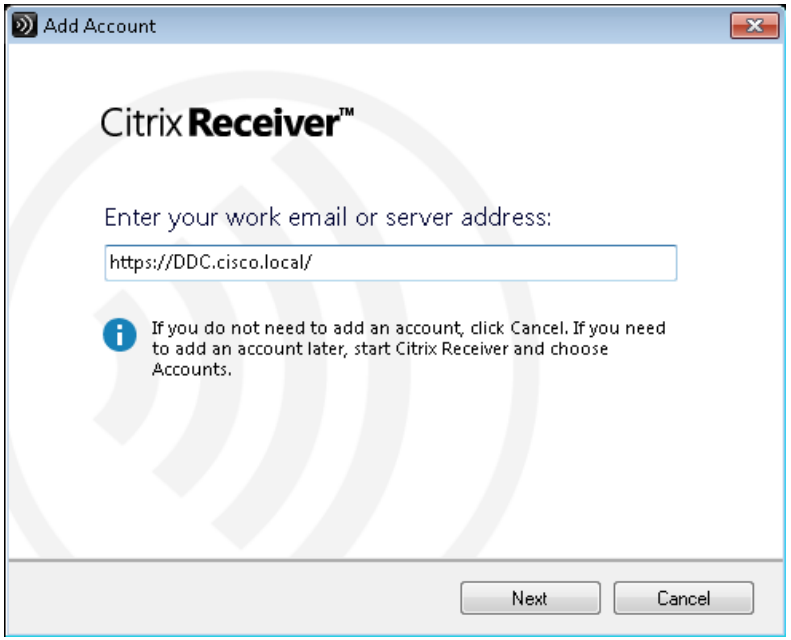
Citrix Receiver is the application used to access virtual environments. Android clients are available from Google Play, and iOS clients for the iPad are available at the Apple App Store. Windows clients are available from the Citrix website, here:
http://www.citrix.com

This guide uses the Windows version of Citrix Receiver on a test laptop in this procedure.

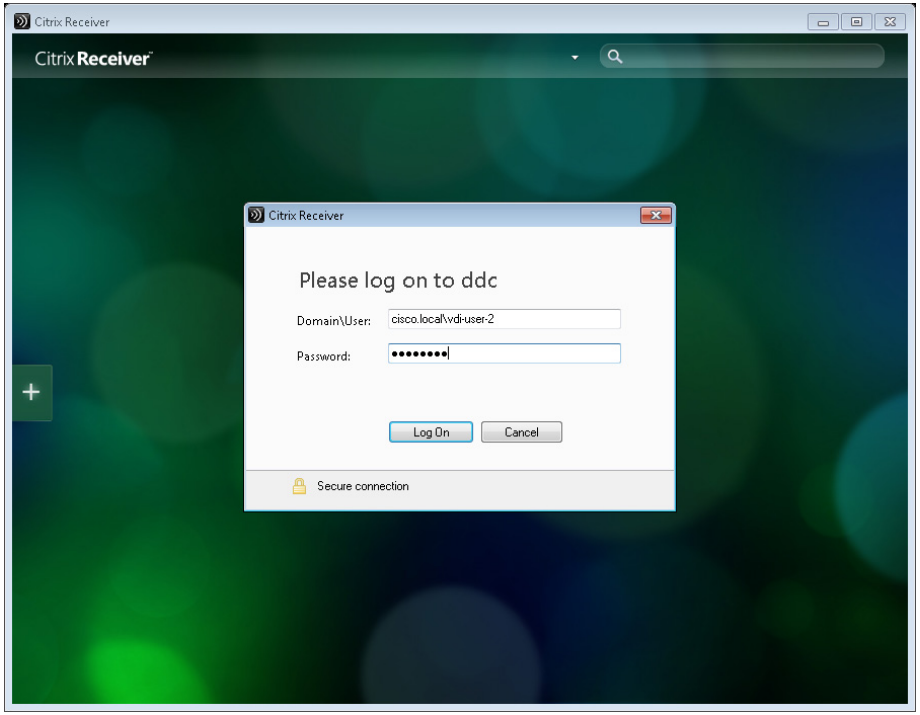
Step 1: On the Windows test laptop, download the appropriate Citrix Receiver for the remote client, and then install the Citrix Receiver application.

Step 2: Launch Citrix Receiver.

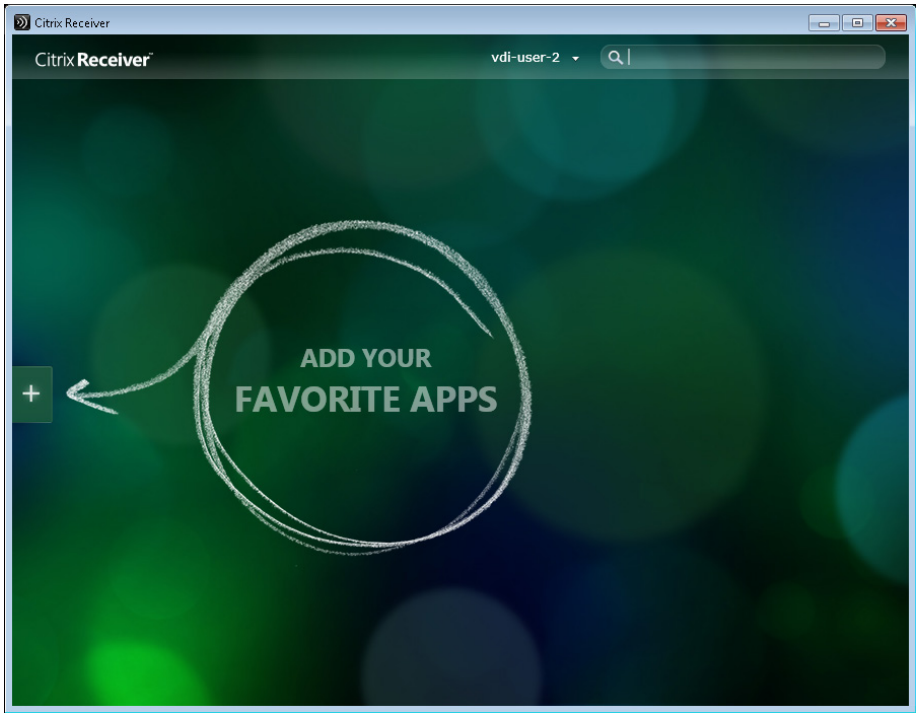
Step 3: If this is the first time Citrix Receiver is launched, in the **Enter your work email or server address** box, enter the server address to which you wish to connect (Example: https://DDC.cisco.local), and then click **Next**.



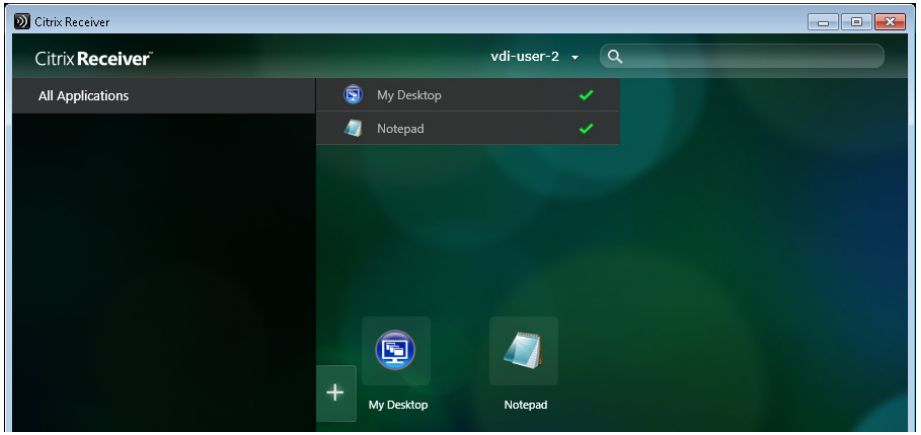
Step 4: In the **Domain\User** box, enter a domain or user account (Example: cisco.local\vdi-user-2), enter the password, and then click **Log On**.



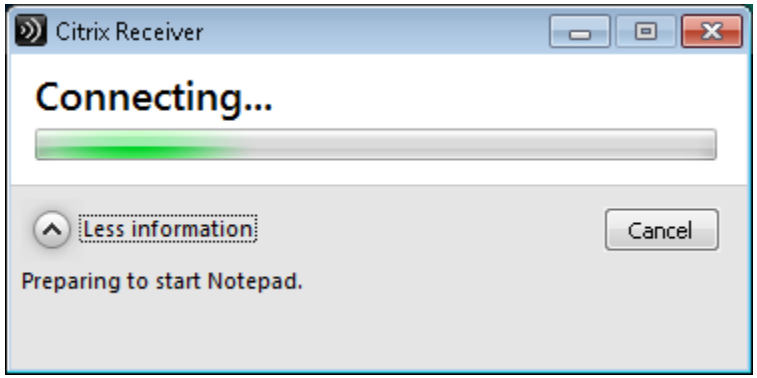
Step 5: Click the plus sign.

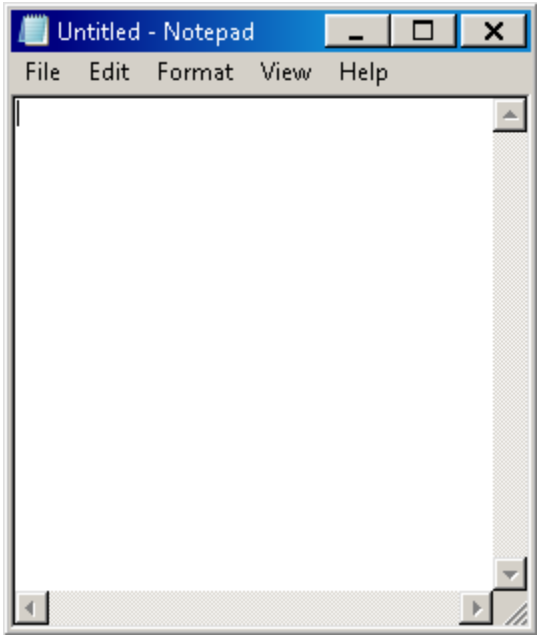


Step 6: Click **All Applications**, and then click the **My Desktop** virtual desktop and **Notepad** virtual application. The virtual desktop and virtual application icons are added to the selection screen.



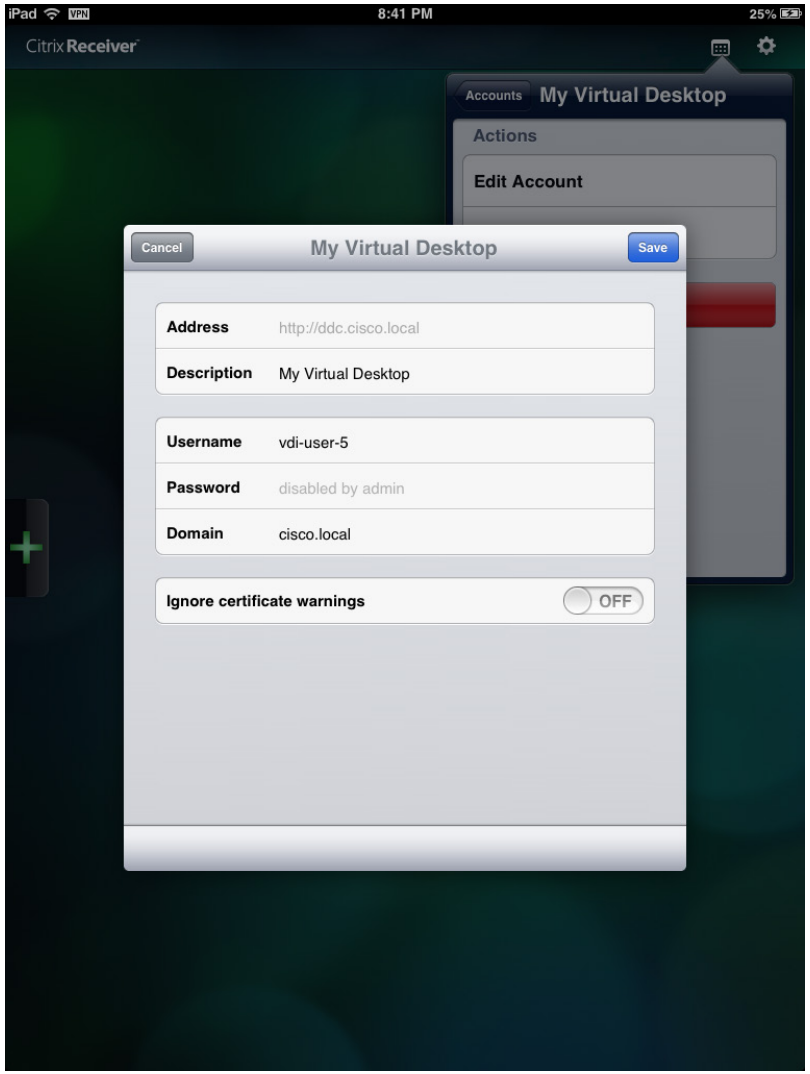
Step 7: Click the **Notepad** icon. The virtual application launches.

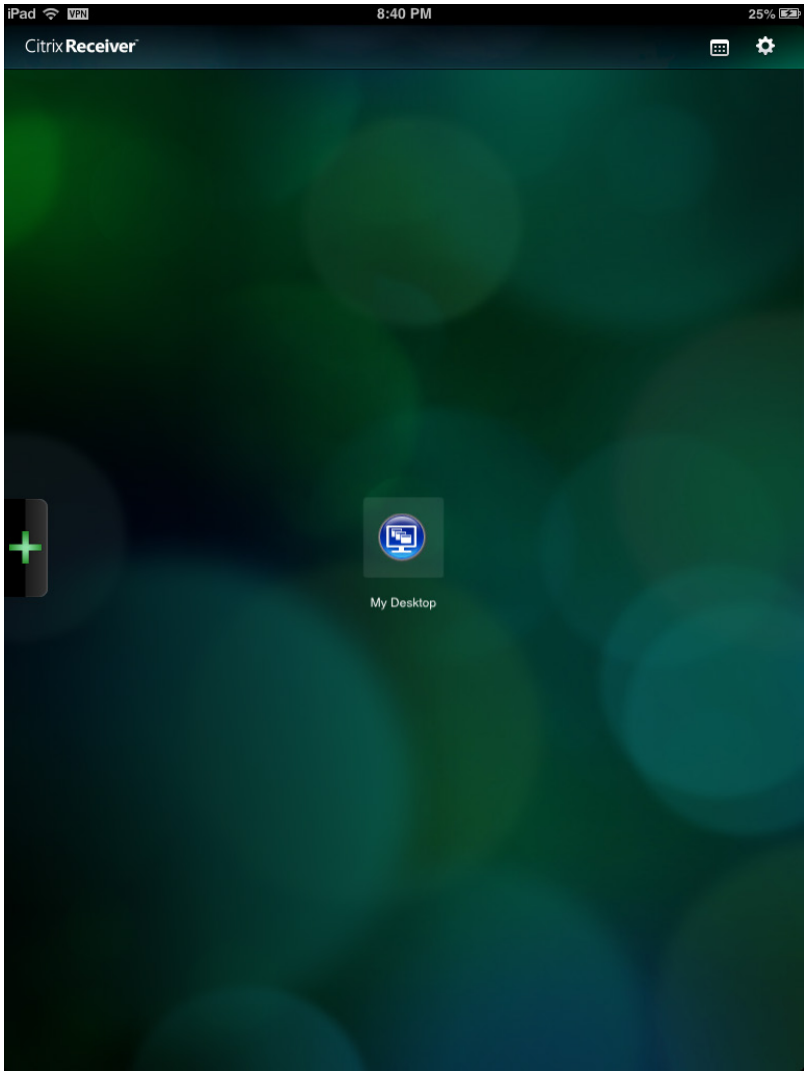




Step 8: On the Citrix Receiver window, click the **My Desktop** icon. The virtual desktop launches.

Example: Installation screens with an iOS device

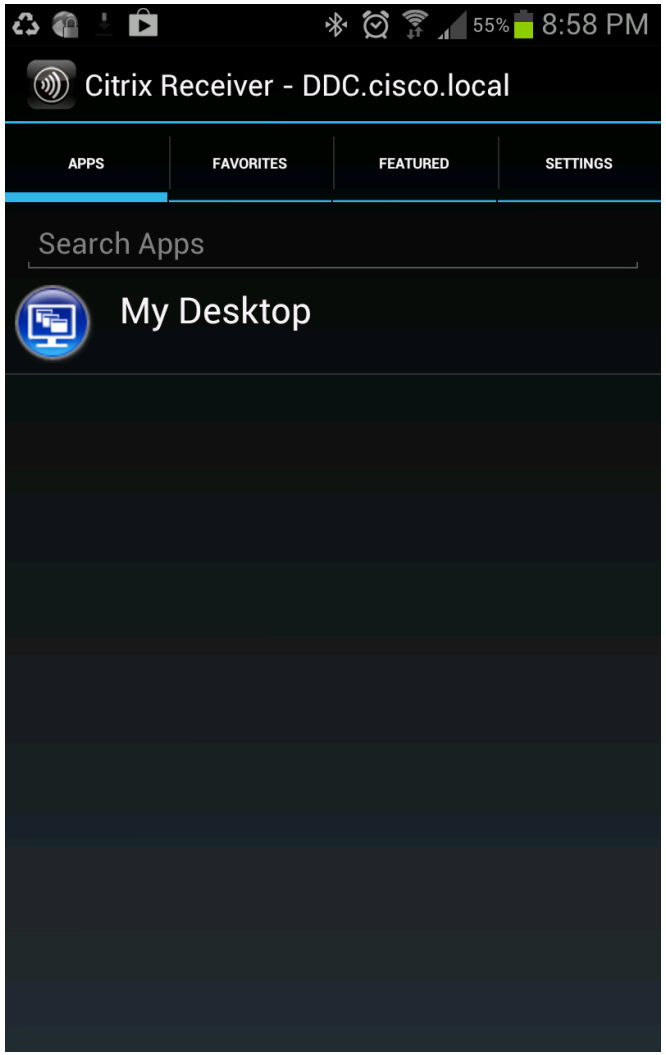


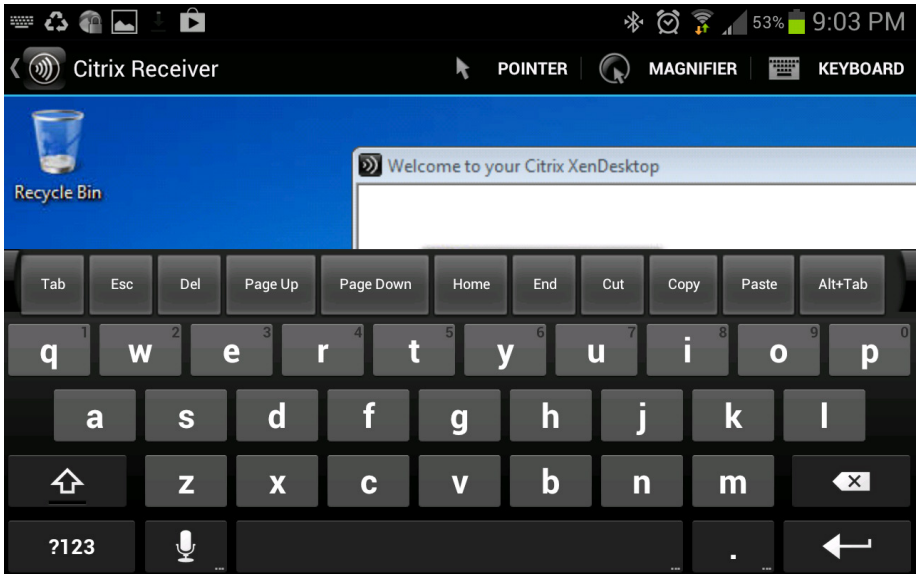


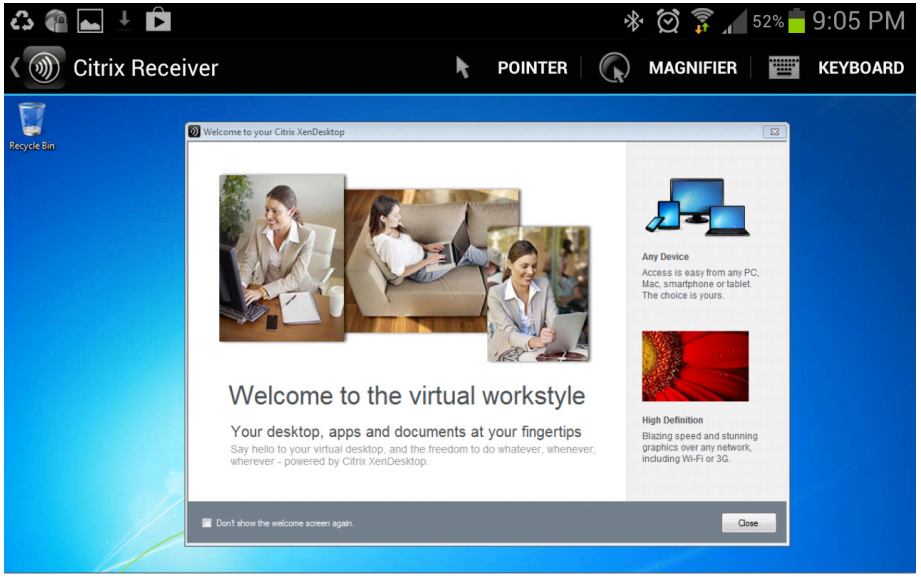
Recycle Bin
Home
Pair
Arrow Keys
Keyboard
Pointer
Magnifier
Gestures
Switch
Welcome to your Citrix XenDesktop
Welcome to the virtual workstyle
Your desktop, apps and documents at your fingertips
Say hello to your virtual desktop, and the freedom to do whatever, whenever, wherever - powered by Citrix XenDesktop.
Any Device
Access is easy from any PC, Mac, smartphone or tablet. The choice is yours.
High Definition
Blazing speed and stunning graphics over any network, including Wi-Fi or 3G.
Don't show the welcome screen again.
Close
8:39 PM
2/12/2013

Notes

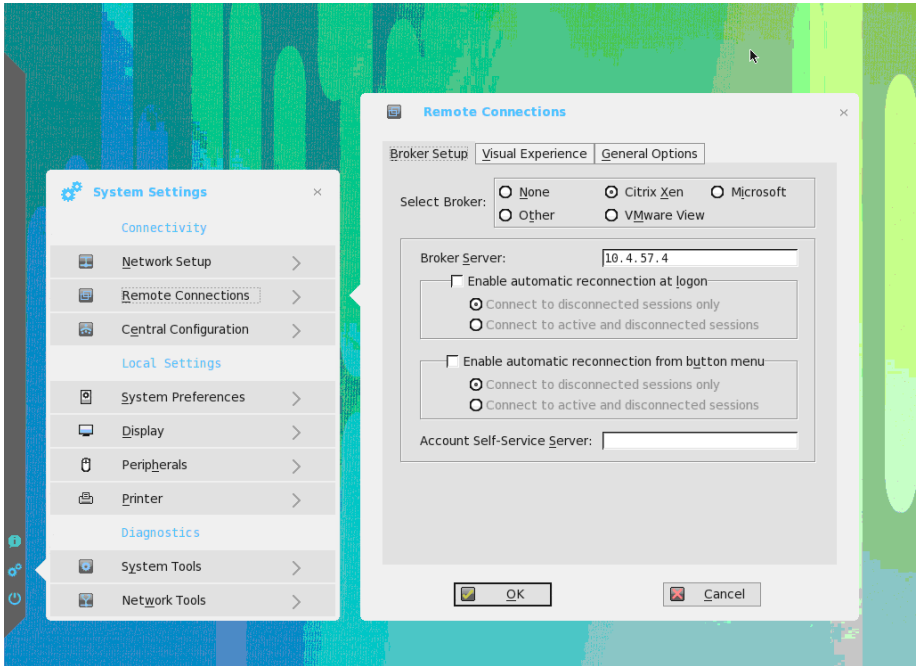
Example: Installation screens with an Android device

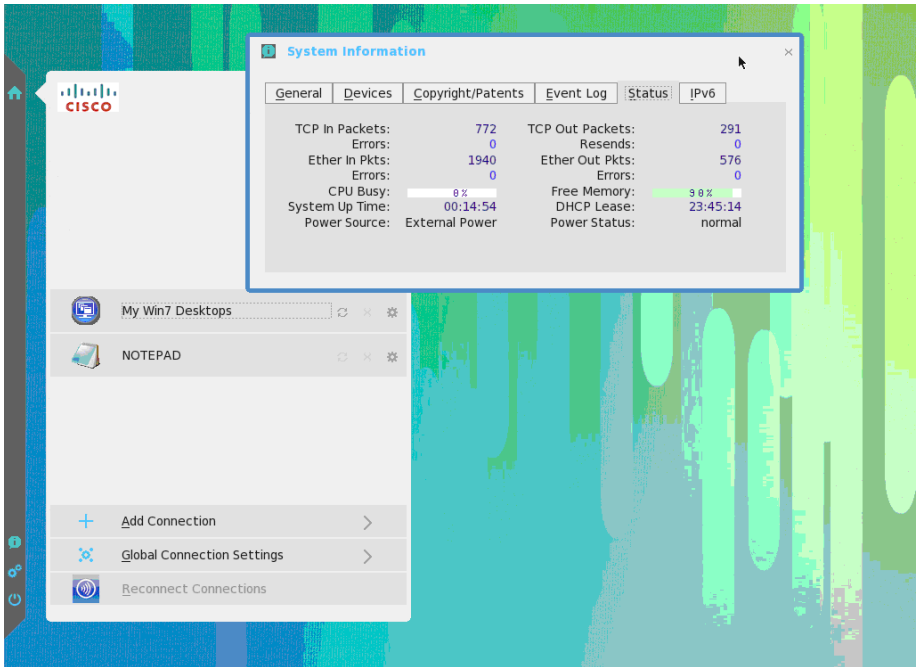






Example: Installation screens with Cisco Virtualization Exprience Client (VXC) 2212 device



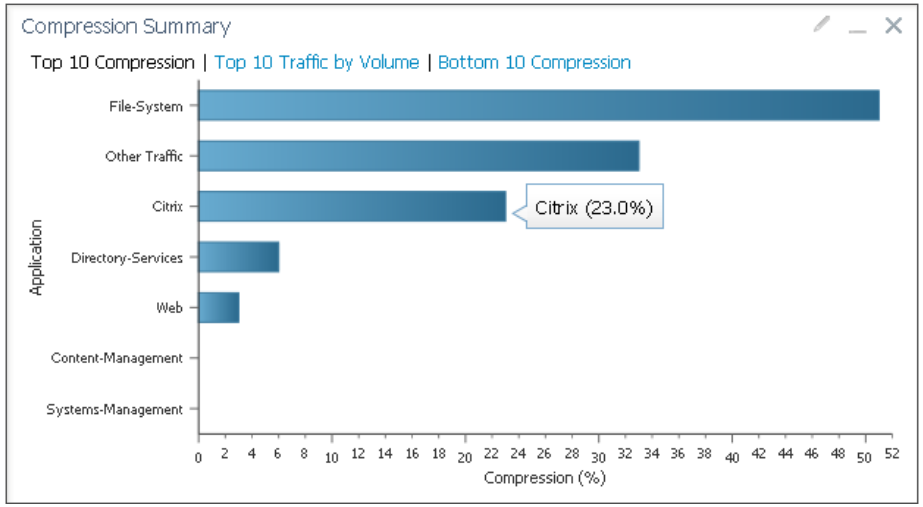


Procedure 3 Observe optimized WAN for Citrix Receiver

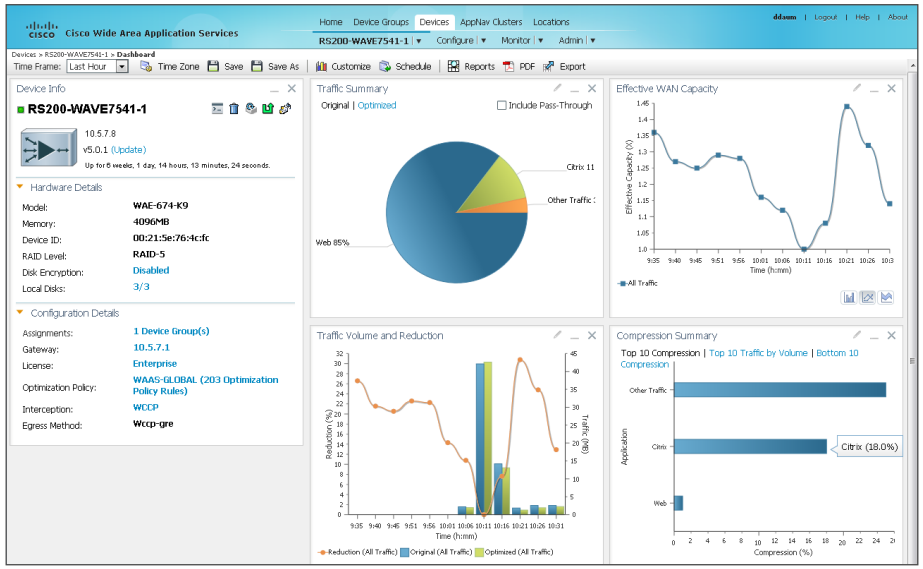
For Citrix Receiver clients at WAN-attached remote sites, the user experience for the virtualized sessions is improved when using Cisco WAAS appliances in order to accelerate communication and reduce traffic over the WAN. The default WAAS policy accelerates Citrix ICA protocols. In the Cisco SBA architecture, this behavior is observed by using the WAAS Central Manager.

Step 1: In a web browser, open the Cisco WAAS Central Manager URL (example: https://10.4.48.100:8443), and then log in.

If compression of Citrix ICA traffic is in the top 10 compressed application protocols, it appears on the home dashboard.



Step 2: Navigate to **Devices**, and select the Cisco WAAS appliance servicing a site with an active Citrix Receiver. A graphical view showing the Citrix accelerated traffic is displayed.



Notes

Appendix A: Product List

Data Center Virtualization

Functional Area	Product Description	Part Numbers	Software
Hypervisor	VMware vSphere	ESXi	5.0U1
Operating System	Windows Server 2008 R2	Windows Server	2008 R2, SP1 Standard
Workspace Virtualization	Citrix XenDesktop	XenDesktop	5.6 Platinum
	Citrix Provisioning Services	Provisioning Services	6.1
	Citrix Provisioning Services Target Device Software	Provisioning Services TDS	
	Citrix XenApp	XenApp	6.5

Computing Resources

Functional Area	Product Description	Part Numbers	Software
UCS Fabric Interconnect	Cisco UCS up to 48-port Fabric Interconnect	UCS-FI-6248UP	2.1(1a) Cisco UCS Release
	Cisco UCS up to 96-port Fabric Interconnect	UCS-FI-6296UP	
UCS B-Series Blade Servers	Cisco UCS Blade Server Chassis	N20-C6508	2.1(1a) Cisco UCS Release
	Cisco UCS 8-port 10GbE Fabric Extender	UCS-IOM2208XP	
	Cisco UCS 4-port 10GbE Fabric Extender	UCS-IOM2204XP	
	Cisco UCS B200 M3 Blade Server	UCSB-B200-M3	
	Cisco UCS B200 M2 Blade Server	N20-B6625-1	
	Cisco UCS B250 M2 Blade Server	N20-B6625-2	
	Cisco UCS 1280 Virtual Interface Card	UCS-VIC-M82-8P	
	Cisco UCS M81KR Virtual Interface Card	N20-AC0002	

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(1b) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Data Center Services

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	ASA 9.0(1) IPS 7.1(6) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

WAAS Central Manager

Functional Area	Product Description	Part Numbers	Software
Central Manager Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.0.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Central Manager Virtual Appliance	Virtual WAAS Central Manager	WAAS-CM-VIRT-K9	5.0.1
	License to manage up to 2000 WAAS Nodes	LIC-VCM-2000N	
	License to manage up to 100 WAAS Nodes	LIC-VCM-100N	

WAAS Aggregation

Functional Area	Product Description	Part Numbers	Software
WAVE Aggregation Appliance	Cisco Wide Area Virtualization Engine 8541	WAVE-8541-K9	5.0.1
	Cisco Wide Area Virtualization Engine 7571	WAVE-7571-K9	
	Cisco Wide Area Virtualization Engine 7541	WAVE-7541-K9	
	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	

WAAS Remote Site

Functional Area	Product Description	Part Numbers	Software
Remote Site WAVE Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.0.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Remote-Site WAVE SRE	Cisco SRE 910 with 4-8 GB RAM, 2x 500 GB 7,200 rpm HDD, RAID 0/1, dual-core CPU configured with ISR G2	SM-SRE-910-K9	5.0.1
	WAAS software container for SRE SM 900	SM9-WAAS	
	WAAS Enterprise License for SRE Large deployment	WAAS-ENT-SM-L	
	WAAS Enterprise License for SRE Medium deployment	WAAS-ENT-SM-M	
	WAAS Enterprise License for SRE Small deployment	WAAS-ENT-SM-S	
	Cisco SRE 710 with 4 GB RAM, 500 GB 7,200 rpm HDD, single-core CPU configured with Cisco ISR G2	SM-SRE-710-K9	
	WAAS software container for SRE SM 700	SM7-WAAS	
	WAAS Enterprise License for SRE Medium deployment	WAAS-ENT-SM-M	
	WAAS Enterprise License for SRE Small deployment	WAAS-ENT-SM-S	
Remote-Site WAAS Express	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M5 securityk9 license datak9 license
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	

Appendix B: Data Center Network Infrastructure Configuration

Cisco Nexus 5596UPa

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient data center core for both Ethernet and Fibre Channel network transport. This switch is also the Fibre Channel SAN-A switch. The *Cisco SBA—Data Center Deployment Guide* along with the *Data Center Configuration Files Guide* provide the base network configuration guidance and platform configurations used for this deployment. Portions of the configuration that deviate from the base configuration are shown here.

```
vlan 157
  name VDI_Desktop

route-map static-to-eigrp permit 30
  match ip address 10.4.57.0/24

vsan database
  vsan 4 name "General-Storage"

device-alias database
  device-alias name Netapp-e1a-fcoe pwwn 50:0a:09:81:8d:90:dc:42
device-alias commit

interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155,157
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155,157
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 54

router eigrp 100
  router-id 10.4.56.254
  redistribute static route-map static-to-eigrp

ip route 10.4.57.0/24 Vlan153 10.4.53.126

zone name VDI-Servers-SHARED-Storage-fc0_netapp-e1a vsan 4
    member pwwn 20:ff:00:25:b5:0a:00:5f
    memb
zoneset activate name SAN_4 vsan 4
er pwwn 50:0a:09:81:8d:90:dc:42
!               [Netapp-e1a-fcoe]
    member pwwn 20:ff:00:25:b5:0a:00:2f
    member pwwn 20:ff:00:25:b5:0a:00:3f
    member pwwn 20:ff:00:25:b5:0a:00:0f
    member pwwn 20:ff:00:25:b5:0a:00:1f
    member pwwn 20:ff:00:25:b5:0a:00:6e

zoneset name SAN_4 vsan 4
    member VDI-Servers-SHARED-Storage-fc0_netapp-e1a

zoneset activate name SAN_4 vsan 4
```

Cisco Nexus 5596UPb

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient data center core for both Ethernet and Fibre Channel network transport. This switch is also the Fibre Channel SAN-B switch. The *Cisco SBA—Data Center Deployment Guide* along with the *Data Center Configuration Files Guide* provide the base network configuration guidance and platform configurations used for this deployment. Portions of the configuration that deviate from the base configuration are shown here.

```
vlan 157
  name VDI_Desktop

route-map static-to-eigrp permit 30
  match ip address 10.4.57.0/24

vsan database
  vsan 5 name "General-Storage"

device-alias database
  device-alias name Netapp-e1b-fcoe pwwn 50:0a:09:82:8d:90:dc:42
device-alias commit

interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155,157
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155,157
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 54

router eigrp 100
  router-id 10.4.56.253
  redistribute static route-map static-to-eigrp

ip route 10.4.57.0/24 Vlan153 10.4.53.126

zone name VDI-Servers-SHARED-Storage-fc1_netapp-e1b vsan 5
    member pwwn 20:ff:00:25:b5:0b:00:5f
    member pwwn 50:0a:09:82:8d:90:dc:42
!               [Netapp-e1b-fcoe]
    member pwwn 20:ff:00:25:b5:0b:00:2f
    member pwwn 20:ff:00:25:b5:0b:00:3f
    member pwwn 20:ff:00:25:b5:0b:00:0f
    member pwwn 20:ff:00:25:b5:0b:00:1f
    member pwwn 20:ff:00:25:b5:0b:00:6e

zoneset name SAN_5 vsan 5
    member VDI-Servers-SHARED-Storage-fc1_netapp-e1b

zoneset activate name SAN_5 vsan 5
```

Cisco ASA 5585—Primary

The Cisco ASA 5585 firewalls for the Cisco SBA data center are provisioned in pairs for resiliency. This is the primary firewall configuration. The *Cisco SBA—Data Center Deployment Guide* along with the *Data Center Configuration Files Guide* provide the base network configuration guidance and platform configurations used for this deployment. The portion of the configuration that deviates from the base configuration is shown here.

```
interface Port-channel10.157
 description DC VDI_Desktop VLAN
 vlan 157
 nameif DC-VDI_Desktop
 security-level 75
 ip address 10.4.57.1 255.255.255.0 standby 10.4.57.2
```

Cisco ASA 5585—Secondary

The Cisco ASA 5585 Adaptive Security Appliances for the Cisco SBA data center are provisioned in pairs for resiliency. Although this is the secondary Cisco ASA 5585, the configuration is the same as the primary Cisco ASA 5585, with the exception of a few lines in the base configuration. The *Cisco SBA—Data Center Deployment Guide* along with the *Data Center Configuration Files Guide* provide the base network configuration guidance and platform configurations used for this deployment. The portion of the configuration that deviates from the base configuration is shown here.

```
interface Port-channel10.157
 description DC VDI_Desktop VLAN
 vlan 157
 nameif DC-VDI_Desktop
 security-level 75
 ip address 10.4.57.1 255.255.255.0 standby 10.4.57.2
```

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

B-0000322-1 4/13