



Reviewer's Guide for View in Horizon 6

VMware Horizon 6

WHITE PAPER

Table of Contents

Introduction	5
Audience	5
What You Will Learn	5
Navigating This Document for Key Use Cases	5
Terminology Used in This Guide	6
What Is Horizon 6?	6
Features of the View Virtual Desktop Solution	7
Key Features in This Release of View	7
Hosted Apps	7
Cloud Pod Architecture	7
View Integration with VMware Virtual SAN Technology	7
Additional Features	8
Discontinued Feature	8
Components That Interact with View	9
View Components	9
View Connection Server	11
View Security Server	11
View Composer Server	11
View Agent	11
Horizon Clients	11
View Persona Management	11
View Administrator	12
ThinApp	12
vCenter Operations Manager for View	13
vSphere Platform	13
vCenter Server	14
Hands-On Evaluation Exercises	15
Installation Prerequisites	15
Infrastructure Requirements	15
Network Requirements	17
Graphics Card	17
Remote Desktop Session Host Requirements for App Remoting	17
Hardware Requirements	18
Operating System Requirements	18
Create Virtual Machines for View Components	19
Download the View Installer Files	20

Complete the Prerequisite Worksheet	20
Prepare the ESXi Host for vSGA 3D Graphics.....	21
Installing View Components.....	22
Install View Connection Server.....	22
Install a View Security Server	29
Install View Composer Server.....	38
Remote Desktop Session Host Configuration	47
Set Up an RDSH Server on Windows Server 2012 R2.....	47
Install View Agent on the RDSH Server	55
Configure Group Policy Settings for RDSH	59
Configuring View	72
Add a License.....	73
Connect vCenter Server Appliance and Configure the View Composer Settings ..	74
Configure Persona Management Administrative Templates in Active Directory...	80
Adjust PCoIP Settings for PCoIP Tuning.....	81
Configure Syslog Event Logging	81
Enable Windows Server 2008 R2 SP1.....	82
Create a Farm for Remote Desktop Session Hosts	83
Preparing Virtual Machines for Linked-Clone Desktop Pool Deployment	85
Create the Master Image for Desktop Deployment	86
Install View Agent	86
Install the View Agent Direct-Connection Plug-In (Optional)	91
Optimize the Virtual Machine for Desktop Deployment	94
Install Custom Applications and Configure the Operating System (Options) ..	94
Prepare the Virtual Machine for Linked-Clone Deployment.....	94
Preparing a Virtual Machine for Full-Clone Desktop Pool Deployment	95
Create a Virtual Machine to Be Used for Desktop Deployment.....	95
Install View Agent on the Virtual Machine	101
Install the View Agent Direct-Connection Plug-In (Optional)	106
Install Custom Applications and Configure the Operating System (Options) ..	109
Prepare the Virtual Machine for Full-Clone Deployment.....	110
Deploying View Desktop and Application Pools	112
Deploy a Linked-Clone Desktop Pool	112
Deploy a Full-Clone Desktop Pool.....	130
Deploy an RDSH Desktop Pool.....	138
Deploy an Application Pool.....	142

Entitling Users to View Desktops and Applications 144

 Entitle Users to a Desktop Pool 144

 Entitle Users to an Application Pool 147

Connecting to View Desktops and Applications 151

 Connect to View Desktops Using Horizon Client 151

 Connect to View Desktops Using HTML Access..... 155

 Connect to View Desktops from a Mobile Horizon Client..... 159

 Connect to an Application Using the Horizon Client..... 164

Summary 169

Additional Documentation 169

About the Authors and Contributors 170

Introduction

Welcome to the View Reviewer's Guide for VMware Horizon® 6, which introduces you to the new features and capabilities in the context of use-case scenarios. The self-guided, hands-on set of exercises and associated feature descriptions enable you to evaluate both new and core capabilities.

Audience

The View Reviewer's Guide is for prospective IT administrators and media reviewers of View. Some familiarity with VMware technologies is assumed, including a basic knowledge of

- VMware vSphere® ESXi™ and VMware vCenter™
- How to configure networking and storage in a virtual environment

What You Will Learn

This document provides step-by-step exercises to guide you through installation and setup of core and deployment scenarios. This guide is not intended as a substitute for product documentation. You can find more detailed information about installation, configuration, administration, and use of View in the [VMware Horizon 6 Documentation](#). You can also consult the [VMware Knowledge Base](#) if you have additional questions. For more in-depth technical white papers, see [View resources](#).

Navigating This Document for Key Use Cases

You can navigate directly to descriptions of key use cases and then to the hands-on exercises:

- [Installation Prerequisites](#)
- [Installing View Components](#)
- [Remote Desktop Session Host Configuration](#)
- [Configuring View](#)
- [Preparing Virtual Machines for Linked-Clone Desktop Pool Deployment](#)
- [Preparing a Virtual Machine for Full-Clone Desktop Pool Deployment](#)
- [Deploying View Desktops and Applications](#)
- [Entitling Users to View Desktops and Applications](#)
- [Connecting to View Desktops and Applications](#)

Terminology Used in This Guide

The following terms are used:

- *Virtual machine*, from the VMware perspective in this document, is one that is located in the data center.
- *Virtual desktop* refers to a Windows-based PC that has been virtualized. An end user accesses the virtual desktop.
- *Master image* is a virtual machine that has been created and configured for desktop deployment and which will serve as the core image for clones. It can also be referred to as *desktop template*, *desktop image*, *golden image*, *parent virtual machine*, and *linked-clone desktop image*.
- *Full clone* is a virtual machine that is a complete copy of another virtual machine. *Full-clone desktops* are copies of a master image, and provide each end-user with a dedicated virtual desktop, which is not refreshed, recomposed, or rebuilt.
- *Linked clone* is based on a snapshot of a virtual machine. *Linked-clone desktops* run off of snapshots of a master image (the master image can be considered the parent virtual machine).

What Is Horizon 6?

Horizon 6 is a desktop virtualization solution that enables organizations to deliver virtualized or remote desktops and applications to end users through a single platform.

View, a component of Horizon 6, offers a virtual desktop infrastructure (VDI). With View, IT departments can run virtual machine desktops and applications in the data center and remotely deliver virtual desktops and applications to employees as a managed service.

A major advantage of using View is that remote desktops and applications follow the end user regardless of device or location. Users can access their personalized virtual desktops or remote applications from company laptops, their home PCs, thin client devices, Macs, tablets, or smartphones. The benefits to administrators include centralized control, efficiency, and security with desktop data stored in the data center.

The three Horizon editions, Horizon View Standard, Horizon Advanced, and Horizon Enterprise, include View as their foundation. Each edition builds successively on the other so that Advanced is based on View Standard with additional components and products, and Enterprise extends the capabilities of Advanced.

The Horizon Standard Edition is licensed only on a per-concurrent-connection basis. The Horizon Advanced and Horizon Enterprise editions are available in two license models:

- **Per named user** – For virtual environments with staff members who need dedicated access to a virtual machine throughout the day
- **Per concurrent connection** – For virtual environments with a high number of users who share machines throughout the day, such as students and shift workers

Horizon 6 leverages the best of View in Horizon and extends the following benefits beyond VDI:

- VMware Identity Manager™ to build a self-service app store that provides end users access to any application from any device
- VMware Mirage™ for image management, backup, and recovery
- VMware ThinApp® for application virtualization
- VMware User Environment Manager™ for personalization and dynamic policy configuration
- vSphere to deliver desktop and application workloads
- VMware Virtual SAN™ to automate storage provisioning

These features provide end users with one place to securely access all their desktops, applications, and online services from any device, everywhere.

For more information about the different editions, see [Packaging and Licensing](#).

Features of the View Virtual Desktop Solution

In general, the key features of View include:

- Tight integration with the latest features of VMware vSphere
- PCoIP remoting protocol
- Linked-clone technology, supported by View Composer
- Support for rich 3D graphics
- Security features such as RSA SecurID, Remote Authentication Dial-In User Service (RADIUS), Active Directory, SSL tunneling, and VMware High Availability
- Centralized administration and management

Key Features in This Release of View

This release of View delivers a number of important new features and enhancements.

Hosted Apps

The hosted-apps feature of View

- Delivers hosted apps (remote applications) through integration with Microsoft Remote Desktop Session Host (RDSH) on Windows Server operating systems.
- Provides a robust way to access one or more remote applications seamlessly from any Horizon Client 3.0 or later using PCoIP.

Cloud Pod Architecture

The Cloud Pod Architecture feature of View

- Lets you deploy View in multiple data centers and manage as a single deployment.
- Provides global entitlements to desktops in multiple data centers.
- Provides the ability to scale up to 20,000 desktops across two sites and four View pods.

View Integration with VMware Virtual SAN Technology

View is now integrated with VMware Virtual SAN technology. This feature

- Aggregates local server-attached storage to satisfy performance and capacity requirements of virtual desktops.
- Recognizes the Virtual SAN storage type and automates the creation of Virtual SAN storage policies based on the type of desktops being deployed.

Note: If you intend to use Virtual SAN, download vSphere 5.5 U1 or later, which is required to support the Virtual SAN feature.

Additional Features

Some other new features of View in Horizon 6 are

- Support for View Connection Server, security server, and View Composer on a Windows Server 2012 R2 operating system.
- Ability to send View logs to a Syslog server such as VMware vCenter Log Insight.
- Support for RDSH remote applications and desktops with the View Agent Direct-Connection Plug-In.
- Enhanced smart card authentication.
- Integration of remote applications with VMware Workspace Portal. Users can launch View applications from the Workspace Portal User Portal.
- Real-Time Audio-Video installs a new kernel-mode webcam driver on View desktops that provides better compatibility with browser-based video apps and other third-party conferencing software.
- Integration of the Remote Experience Agent with View Agent. Previously, you had to install View Agent and the Remote Experience Agent to use features such as HTML Access, Unity Touch, Real-Time Audio-Video, and Windows 7 Multimedia Redirection. Now you obtain these features by installing View Agent only.
- Support for virtual machine space reclamation for Windows 8 and 8.1 linked-clone machines in a vSphere 5.5 or later environment.
- Support for View Persona Management on Windows 8.1 desktops. It is also supported on Windows Server 2008 R2 SP1 desktops that are based on physical or virtual machines.
- Blast Secure Gateway (BSG) support of up to 800 connections to remote desktops from clients using HTML Access. This connection limit applies to a Blast Secure Gateway on one View Connection Server instance or security server.

For more information, see the [View in Horizon 6 Datasheet](#).

Discontinued Feature

View Client with Local Mode functionality, which allowed users to check out a virtual desktop and run it on a Windows physical computer while disconnected from the network, has been removed from Horizon 6.

After the release of Horizon 6, VMware introduced VMware Horizon® FLEX™. Although Horizon FLEX is not an exact replacement for the Local Mode feature, it enables IT administrators to create, secure, and manage local desktops. This policy-based, containerized desktop solution meets the needs of workers with their own computers, “road warriors,” and Mac users in the enterprise. End users work within a restricted virtual machine on their endpoints and can be either connected or disconnected from the enterprise network.

For more information, see

- [Horizon FLEX](#)
- [VMware Horizon FLEX and View Local Mode: Similar Features, But Definitely Not the Same](#)

Components That Interact with View

This section describes the components and VMware products that interact with View, and provides an architectural overview of a View deployment.

View Components

View includes six main components:

- [View Connection Server](#)
- [View Security Server](#)
- [View Composer Server](#)
- [View Agent](#)
- [Horizon Clients](#)
- [View Persona Management](#)

Note: In the VMware Horizon 6 with View release, the View Local Mode feature was removed.

The following diagram illustrates how the View main components, and the multiple smaller components, work together to provide the virtual desktop infrastructure.

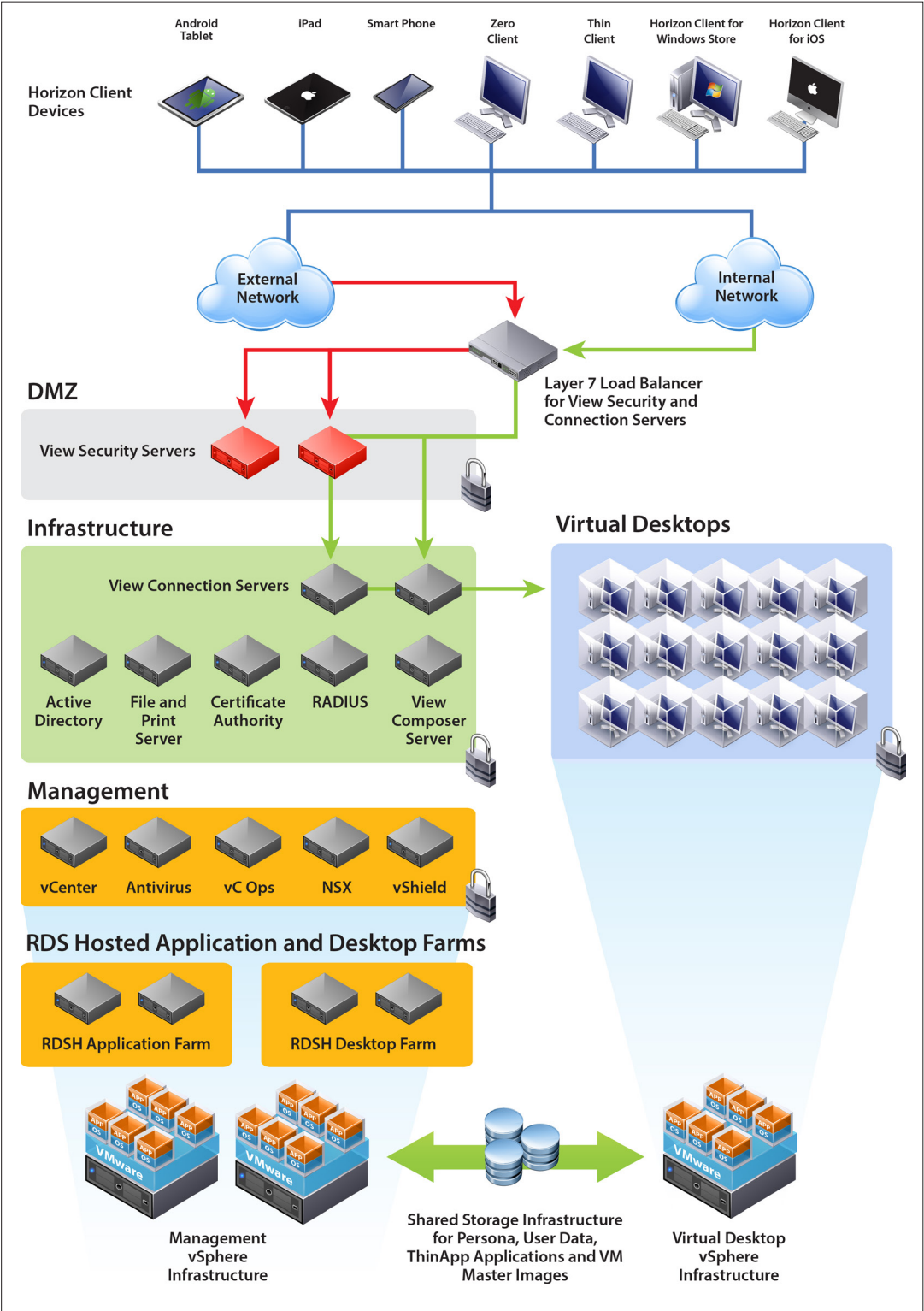


Figure 1: View Deployment and Components

View Connection Server

End users connect through View Connection Server to securely and easily access their personalized virtual desktops. View Connection Server acts as a broker for client connections by authenticating and directing incoming user desktop requests.

View Security Server

A View security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. Outside the corporate firewall, in the DMZ, you can install and configure View Connection Server as a View security server. Security servers in the DMZ communicate with View Connection Servers inside the corporate firewall. Security servers ensure that the only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. Users can access only the desktop resources for which they are authorized.

View Composer Server

View Composer Server is an optional service that enables you to manage pools of “like” desktops, called linked-clone desktops, by creating master images that share a common virtual disk. Linked-clone desktops are one or more copies of a master image that share the virtual disks of the parent, but which operate as individual virtual machines. Linked-clone desktops can optimize your use of storage space and facilitate updates. You can make changes to a single master image through the vSphere Client. These changes trigger View Composer Server to apply the updates to all cloned user desktops that are linked to that master image, without affecting users' settings or persona data.

Note: Although View Composer Server is not required to run the standalone Horizon 6 edition, it is required to complete the [linked-clone exercises](#) in this guide.

View Agent

The View Agent service communicates between virtual machines and Horizon Client. You must install the View Agent service on all virtual machines managed by vCenter Server so that View Connection Server can communicate with them. View Agent also provides features such as connection monitoring, virtual printing, persona management, and access to locally connected USB devices. View Agent is installed in the guest operating system of the virtual machine in the data center.

Horizon Clients

Horizon Clients are available for Windows, Mac, Ubuntu Linux, iOS, and Android to provide the connection to remote desktops from your device of choice.

By installing Horizon Client on each endpoint device, your end users can access their virtual desktops from devices such as smartphones, zero clients, thin clients, Windows PCs, Macs, and iOS- and Android-based mobile devices. Unity Touch for Horizon Clients makes it easier to run Windows apps on iPhone, iPad, and Android devices. Horizon Clients enable users to:

- Connect to View Connection Server or a View security server
- Log in to their remote desktops in the data center
- Edit the list of servers they connect to

As a Horizon 6 administrator, you can enable your end users to download Horizon Clients directly from the [Download Center](#). Or you can control which Horizon Clients each end user can download and store the client installers on a local storage device using the View user portal, the default landing page for View Connection Server. By default, links on the View user portal connect users to the [Download Center](#).

View Persona Management

View Persona Management is an optional component included with View that provides persistent, dynamic user profiles across user sessions on different desktops. You can deploy pools of stateless, floating desktops and enable users to maintain their designated settings between sessions. User profile data is downloaded as needed to speed up login and logout time. New user settings are automatically sent to the user profile repository during desktop use. For deployment recommendations, see the [View Persona Management Deployment Guide](#).

Figure 2 shows the View Persona repository in a View deployment and the location of the user profile (persona) on the remote desktop. View Persona Management is enabled as an option during View Agent installation on the virtual desktop.

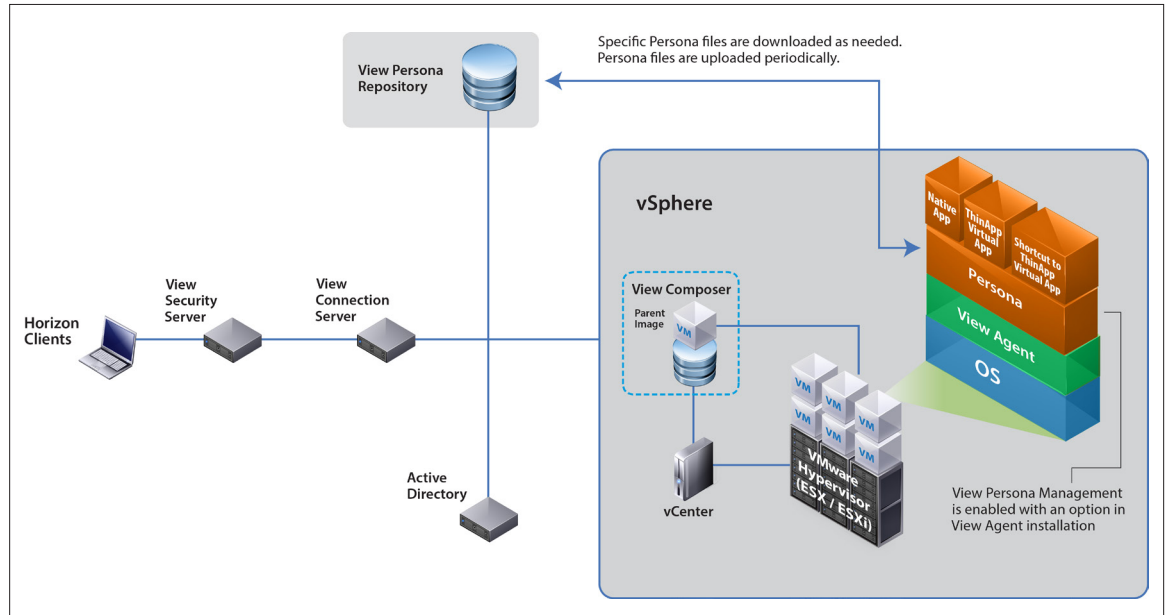


Figure 2: View Persona Management Architecture

View Administrator

View Administrator is the Web-based administrative console for managing users, desktops, applications, and other View objects in a View Connection Server instance. View Administrator is installed when you install the View Connection Server. View Administrator streamlines the management, provisioning, and deployment of virtual desktops. As an administrator, you can centrally manage thousands of virtual desktops from a single console.

ThinApp

ThinApp is a product included with each edition of Horizon and which creates virtualized applications. In a View implementation, these virtual packages reside on a ThinApp repository on a network share. As an administrator, you can copy a full ThinApp package from the repository to the virtual desktop. You can also place a shortcut on the virtual desktop, which points to the ThinApp package on the repository. Applications on remote desktops can be natively installed applications, ThinApp virtual applications, hosted applications, or shortcuts to ThinApp virtual applications. As part of the three Horizon editions, ThinApp simplifies repetitive administrative tasks and reduces storage needs for virtual desktops by maintaining applications independently of the underlying OS.

Figure 3 shows the two possible deployment modes for ThinApp (local and streaming) and the location of the ThinApp repository within the View architecture.

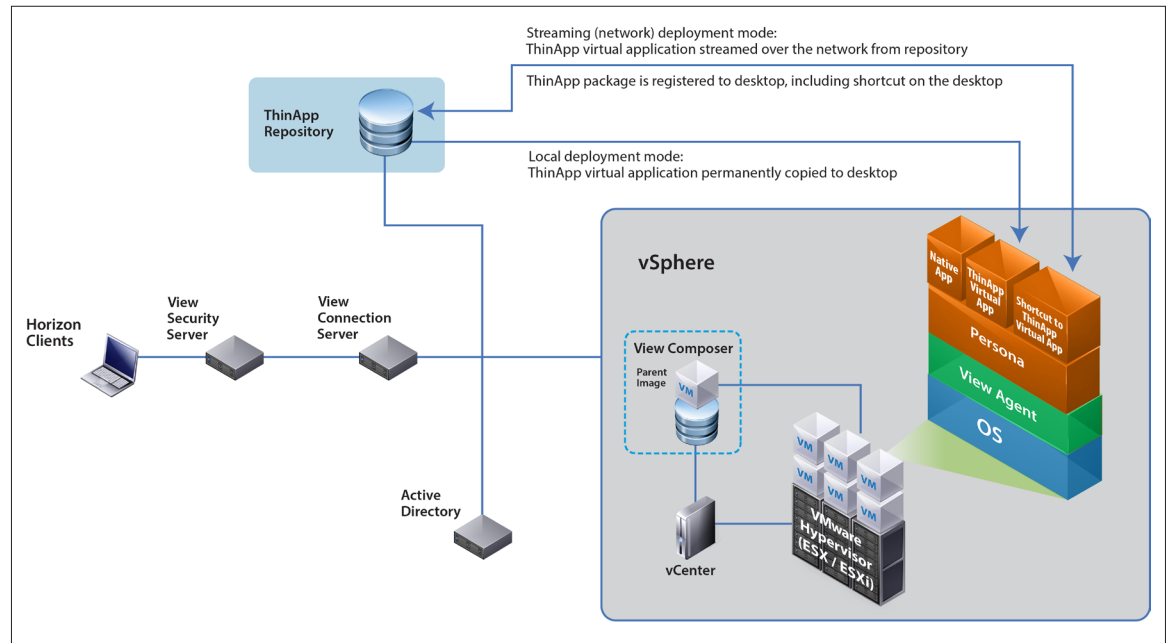


Figure 3: ThinApp Architecture in a View Deployment

vCenter Operations Manager for View

VMware vCenter Operations Manager for View is an optional monitoring solution that extends the capability of vCenter Operations Manager Enterprise to monitor and manage the health, capacity, and performance of your View environments.

It consists of the following major components:

- An adapter that collects data from the desktop agents and sends it to vCenter Operations Manager
- A broker agent that collects View inventory information and sends it to the adapter
- Multiple desktop agents that collect desktop performance data and send it to the adapter

See also [VMware vCenter Operations Manager for View Documentation](#).

vSphere Platform

Designed for desktops, vSphere is a scalable platform for running virtual desktops and applications, and it offers business-continuity and disaster-recovery capabilities to protect desktop data and availability without the cost and complexity of traditional solutions. VMware vSphere Desktop has all the key features of the VMware vSphere Enterprise Plus Edition™.

Included in vSphere Desktop is VMware vShield Endpoint™, which offloads and centralizes antivirus and antimalware solutions to a hardened security virtual machine. The VMware endpoint security APIs access the file system to scan and remediate viruses, removing the need for agents in the guest operating system and preventing antivirus storms from consuming CPU cycles during scanning or antivirus update activities. Offloading antivirus functions provides enhanced security because a malware attack often begins by disabling antivirus agents. For more information, see the [VMware vSphere Documentation](#).

vCenter Server

VMware vCenter Server™ is the central management hub for vSphere and provides control over and visibility into clusters, hosts, virtual machines, storage, networking, and other critical elements of your virtual infrastructure. VMware vCenter provides management capabilities for your View infrastructure. For more information, see [VMware vCenter Server](#).

Hands-On Evaluation Exercises

This section provides hands-on exercises to help you evaluate the installation and use of your View instance. The exercises cover the following topics:

- Installation Prerequisites
- Installing View Components
- Remote Desktop Session Host Configuration
- Configuring View
- Preparing Virtual Machines for Linked-Clone Desktop Pool Deployment
- Preparing a Virtual Machine for Full-Clone Desktop Pool Deployment
- Deploying View Desktops and Applications
- Entitling Users to View Desktops and Applications
- Connecting to View Desktops and Applications

The exercises are sequential and build upon one another, so make sure to complete each exercise in each section before moving on to the next.

Installation Prerequisites

This section describes the prerequisites and hardware, server, and installation minimum requirements. It provides corresponding exercises to walk you through the installation of a basic View instance:

- [Infrastructure Requirements](#)
- [Network Requirements](#)
- [Graphics Card](#)
- [Hardware Requirements](#)
- [Operating System Requirements](#)
- [Remote Desktop Session Host Requirements for App Remoting](#)
- [Create Virtual Machines for View Components](#)
- [Download the View Installer Files](#)
- [Complete the Prerequisite Worksheet](#)
- [Prepare ESXi Host for vSGA 3D Graphics \(Optional\)](#)

Infrastructure Requirements

View ships as Windows-server-based installers that you install on virtual machines residing on a vSphere host. To take advantage of all the new features of this release, you must first install and configure vSphere and vCenter Server Appliance™ on your host. For current compatibility information, see [VMware Product Interoperability Matrixes](#).

Verify that your environment has the following prerequisites before you deploy View.

Active Directory Domain Controller

View integrates with your existing Microsoft Active Directory infrastructure. Active Directory is a Windows service for authenticating and authorizing users and computers, applying and enforcing security policies, installing and updating software, and more. View Connection Server joins to the existing Active Directory and sets up a lightweight directory services instance for the storage of View configuration information.

Gather the information in Table 1 before proceeding.

VIEW	CONFIGURATION INFORMATION
Server name of an Active Directory domain controller in the environment	
FQDN of an Active Directory domain controller in the environment	
Base DN user name	
Base DN password	
Active Directory user name with privileges to join computers to the domain	

Table 1: Active Directory Information for View Configuration

VMware vCenter Credentials

For a desktop deployment, you must connect to the vCenter host. Gather the information listed in Table 2.

VIEW CONNECTION SERVER	CONFIGURATION INFORMATION
vCenter host name FQDN	
vCenter port number	
vCenter administrator user name	
vCenter administrator password	

Table 2: View Connection Server Configuration Information

SSL Certificate

By default, View includes a self-signed certificate that can be used for testing purposes. For a production environment, we recommend that you replace the self-signed certificate with an approved certificate signed by a Certificate Authority.

SQL Database

View Composer Server requires a SQL database to store the connections and components of linked-clone desktops. Supported databases include:

- Microsoft SQL Server 2012 Standard or Enterprise SP1 (32- and 64-bit)
- Microsoft SQL Server 2012 Express (32- and 64-bit)
- Microsoft SQL Server 2008 Express R2 SP2 (64-bit)
- Microsoft SQL Server 2008 Standard or Enterprise R2 SP2 (32- and 64-bit)
- Microsoft SQL Server 2008 Standard, Enterprise, or Datacenter SP3 (32- and 64-bit)
- Oracle 10g Release 2 [10.2.0.4] Standard, Standard ONE, or Enterprise (32- and 64-bit)
- Oracle 11g Release 2 [11.2.0.3] Standard, Standard ONE, or Enterprise (32- and 64-bit)

Gather the database information in Table 3.

VIEW COMPOSER SERVER	CONFIGURATION INFORMATION
IP address for database	
FQDN for database	
Database instance name	
Name of the newly created database specifically for View Composer Server data	
Name of the newly created database specifically for View events data	
Login credentials with database owner rights on the database	

Table 3: Database Information for View Composer Server

File and Print Server

View Persona Management and ThinApp require a network file server for the storage of roaming persona data and ThinApp packages. Make sure that you have adequate storage allocated if you want to use these features.

Network Requirements

We recommend that you have at least 1 Gbps network connectivity between all the required components and desktops.

Graphics Card

To use vSGA or vDGA from a View desktop, you must install a supported graphics card on your ESXi host. You must also download the ESXi vSphere Installation Bundle (VIB) driver file for vSGA from NVIDIA or the appropriate NVIDIA Windows drivers to use vDGA.

You get the ESXi 5.5 driver at [VMware vSphere ESXi 5.5 Driver](#).

The following GPU cards are supported:

- NVIDIA Quadro 4000
- NVIDIA Quadro 5000
- NVIDIA Quadro 6000
- NVIDIA GRID K1
- NVIDIA GRID K2
- NVIDIA M2070Q

Additional cards might be supported in the future. Refer to [NVIDIA](#) for a full list of supported graphics cards.

This guide covers how to deploy only vSGA. To deploy vDGA, refer to the instructions in [Deploying Hardware-Accelerated Graphics with View Virtual Desktops in Horizon 6](#). It is recommended that you follow all the other exercises in the guide to get your View environment fully configured before you set up a vDGA-enabled View desktop.

Remote Desktop Session Host Requirements for App Remoting

If you do not have an RDSH server that is already configured, prepare a virtual desktop with Windows Server 2012 R2 installed and configure an RDSH server using the [Remote Desktop Session Host Configuration](#) exercises. If you already have an RDSH server configured, use it when configuring app remoting in subsequent exercises.

Hardware Requirements

Table 4 shows the minimum and recommended hardware requirements for View components.

COMPONENT	VIRTUAL CPUS	RAM
View Connection Server	Minimum: 2 vCPUs Recommended: 4 vCPUs	Minimum: 4 GB Recommended: 10 GB
View Composer Server	Minimum: 2 vCPUs Recommended: 4 vCPUs	Minimum: 4 GB Recommended: 8 GB
View security server	Minimum: 2 vCPUs Recommended: 4 vCPUs	Minimum: 4 GB Recommended: 10 GB

Table 4: Hardware Requirements

Operating System Requirements

Table 5 shows the operating system requirements for a View deployment.

OPERATING SYSTEM	VERSION	EDITION	MINIMUM DISK SPACE
Windows Server 2008 R2	64-bit	Standard and Enterprise	40 GB
Windows Server 2008 R2 SP1	64-bit	Standard and Enterprise	40 GB
Windows Server 2012 R2	64-bit		40 GB

Table 5: Operating System Requirements

Create Virtual Machines for View Components

You must create three virtual machines that meet the requirements listed in the previous tables, one for each View component:

- View Connection Server
- View security server
- View Composer Server

For each virtual machine, gather the information listed in Table 6.

VIEW CONNECTION SERVER	CONFIGURATION INFORMATION
Static IP address configured	
Virtual machine joined to the domain	
Virtual machine host name FQDN in DNS with reverse lookup records defined	
Windows Firewall turned on	
VIEW SECURITY SERVER	CONFIGURATION INFORMATION
Static IP address configured	
Virtual machine joined to the domain (optional)	
Virtual machine host name FQDN in DNS with reverse lookup records defined	
Windows Firewall turned on	
VIEW COMPOSER SERVER	CONFIGURATION INFORMATION
Static IP address configured	
Virtual machine joined to the domain	
Virtual machine host name FQDN in DNS with reverse lookup records defined	
Windows Firewall turned on (optional)	
ODBC driver installed for your database	

Table 6: Virtual Machine Information

Download the View Installer Files

The first step is to download the installation files and prepare for installation. For the purposes of this exercise, a utility is used to create an ISO image with all the installers on it. Alternatively, you can upload the View installer files to a network file share that is accessible by the target virtual machines where you will install your View components.

1. Verify that you have at least 700 MB of space to download the installers.
2. Go to [VMware Downloads](#), and download the following installers:
 - View Connection Server (64-bit)
 - View Composer Server
 - View Agent (32-bit or 64-bit)
 - View Agent Direct Connect (32-bit or 64-bit)
 - View Client (32-bit or 64-bit)

When you have downloaded the installation files, proceed to the next exercise to gather component data.

Complete the Prerequisite Worksheet

After downloading the View installer files, gather the data that you need to set up your View instance.

1. Complete the component worksheet.

COMPONENT	HOST NAME	FQDN	IP	CREDENTIALS
View Connection Server				
View security server				
View Composer Server				
vCenter Server Appliance				

2. Complete the database worksheet.

DATABASE	FQDN	IP	INSTANCE NAME	DATABASE NAME	CREDENTIALS FOR USER WITH DBO ACCESS: USER NAME / PASSWORD
View Composer Server database					

After you have gathered the data to set up your View instance, prepare the ESXi host for vSGA 3D graphics if you are using vSGA.

Prepare the ESXi Host for vSGA 3D Graphics

This is an optional exercise if you plan on taking advantage of vSGA-enabled 3D graphics. You can complete the rest of the exercises if you skip this exercise.

Before beginning, verify that you have a graphics card physically installed on your ESXi host and that the card is configured to work with your host. The [VIB driver](#) must be uploaded to a datastore accessible to your ESXi host.

Important: Installing a VIB driver and configuring the device requires that you reboot the ESXi host.

1. Upload the ESXi VIB driver file for your video card to a datastore on your ESXi host.
2. Prepare your host for the VIB installation and ESXi host reboot, and gracefully shut down all virtual machines and place the host in maintenance mode.
3. Use SSH to access your ESXi host console, and run the following command:

```
esxcli software vib install -v /vmfs/volumes/datastore/NVIDIA-VMware-xxxxxxx.x86_64.vib
```

When the installation of the VIB has completed, the results are displayed.

Installation Result

Message: Host is changed.

Reboot Required: true

VIBs Installed: NVIDIA_bootbank_NVIDIA-VMware_ESXi™_5.1_Host_Driver_304.59-10EM.510.0.0.802205

VIBs Removed:

VIBs Skipped:

Note: For additional information on installing ESXi VIB drivers, see [Installing async drivers on ESXi 5.x](#).

4. Run the following command to verify that the VIB was installed.

```
esxcli software vib list
```

Name	Version	Vendor	Acceptance Level	Install Date
NVIDIA-VMware_ESXi_5.1_Host_Driver	304.59-10EM.510.0.0.802205	NVIDIA	VMwareAccepted	2013-02-13
ata-pata-amd	0.3.10-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-atiixp	0.4.6-4vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-cmd64x	0.2.5-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-hpt3x2n	0.3.4-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-pdc2027x	1.0-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-serverworks	0.4.3-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-sil680	0.4.8-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ata-pata-via	0.3.3-2vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
block-cciss	3.6.14-10vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ehci-ehci-hcd	1.0-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
esx-base	5.1.0-0.5.838463	VMware	VMwareCertified	2013-02-04
esx-dvfilter-generic-fastpath	5.1.0-0.0.799733	VMware	VMwareCertified	2013-02-04
esx-tboot	5.1.0-0.0.799733	VMware	VMwareCertified	2013-02-04
esx-xlibs	5.1.0-0.0.799733	VMware	VMwareCertified	2013-02-04
esx-xserver	5.1.0-0.0.799733	VMware	VMwareCertified	2013-02-04
ima-qla4xxx	2.01.31-1vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ipmi-ipmi-devintf	39.1-4vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ipmi-ipmi-msghandler	39.1-4vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
ipmi-ipmi-si-drv	39.1-4vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
misc-cnic-register	1.1-1vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
misc-drivers	5.1.0-0.0.799733	VMware	VMwareCertified	2013-02-04
net-be2net	4.1.255.11-1vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-bnx2	2.0.15g.v50.11-7vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-bnx2x	1.61.15.v50.3-1vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-cnic	1.10.2j.v50.7-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-e1000	8.0.3.1-2vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-e1000e	1.1.2-3vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-enic	1.4.2.15a-1vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04
net-forcedeth	0.61-2vmw.510.0.0.799733	VMware	VMwareCertified	2013-02-04

5. Note the name of the VIB module.

You need the VIB module name to verify later that this driver loaded successfully.

6. Follow proper vSphere shutdown procedures, and then reboot your ESXi host from one of the following:

- vSphere Client
- Command line by entering **reboot**

Important: Do not reboot until you have followed proper vSphere shutdown procedures. After rebooting ESXi, connect to your host with the vSphere Client and initiate proper virtual machine power-on procedures to return your environment to the previous state.

7. When your host has powered back on, use SSH to access the ESXi console.
8. Run the following command to verify that the driver modules can load successfully.

```
Esxcli system module load --module nameofmodule
```

For further instructions or troubleshooting for configuring vSGA, see the guide [Deploying Hardware-Accelerated Graphics with View Virtual Desktops in Horizon 6](#). You have completed the initial prerequisite exercises. You are now ready to install View.

Installing View Components

This section provides hands-on exercises to help you evaluate the installation process of the View components.

- [Install View Connection Server](#)
- [Install a View security server](#)
- [Install View Composer Server](#)

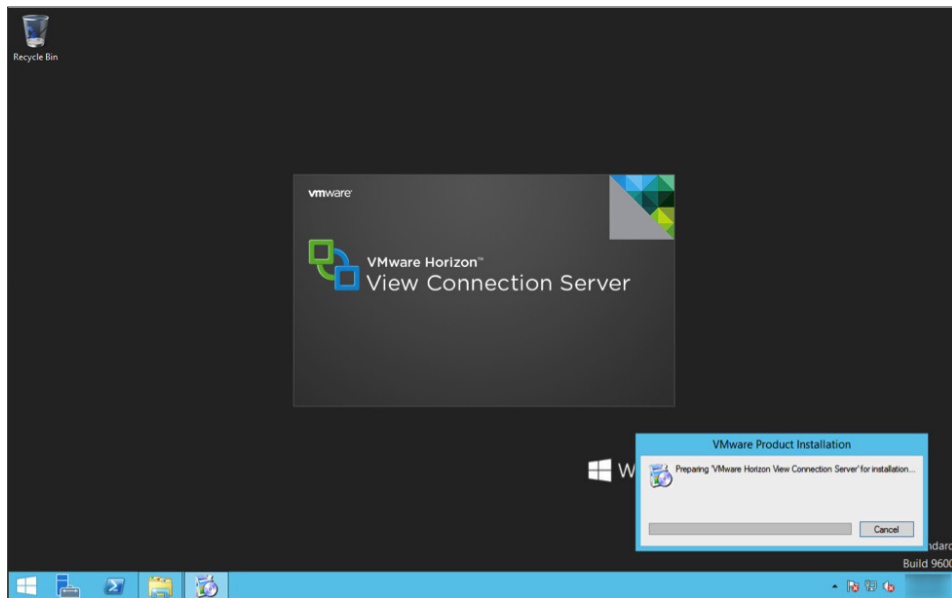
The exercises are sequential and build on one another, so make sure to complete each exercise in this section before going to the next.

Install View Connection Server

View Connection Server acts as a broker for client connections by authenticating and directing incoming user desktop requests. View Administrator, installed when you install View Connection Server, is the Web-based administrative UI for the management, provisioning, and deployment of virtual desktops. As an administrator, you can centrally manage thousands of virtual desktops from a single View Administrator console.

1. Log in to the virtual machine that you prepared as the target for installing View Connection Server.
The virtual machine must meet the requirements detailed in the Installation Prerequisites.
2. Verify that the 64-bit View Connection Server installer is accessible by the operating system of the target virtual machine.

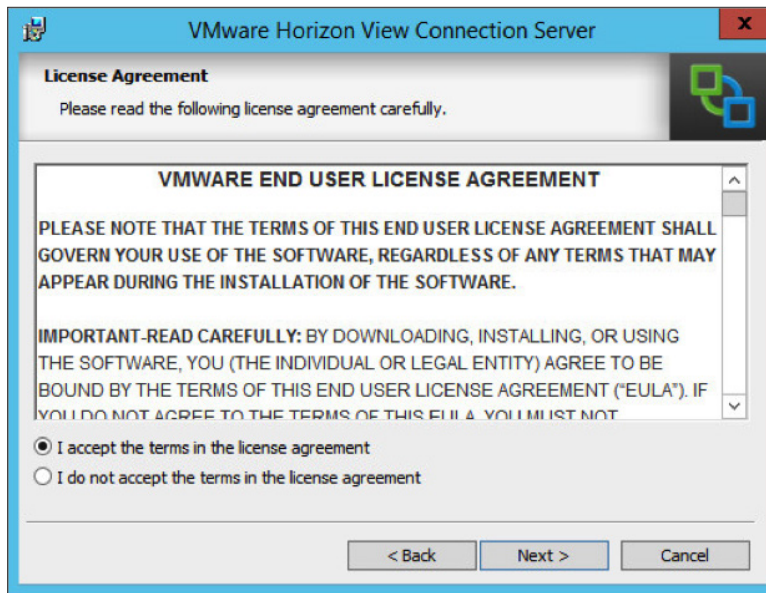
3. Launch and load the View Connection Server installer.



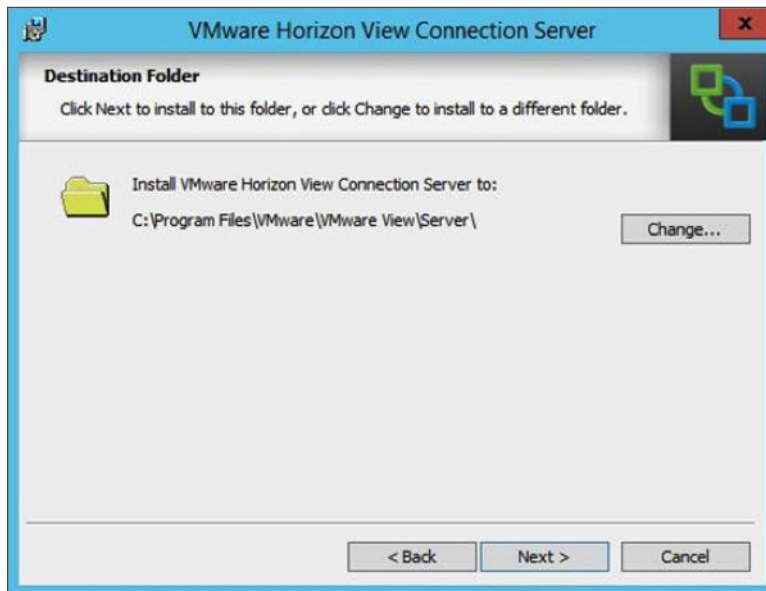
4. When the installer finishes loading, click **Next**.



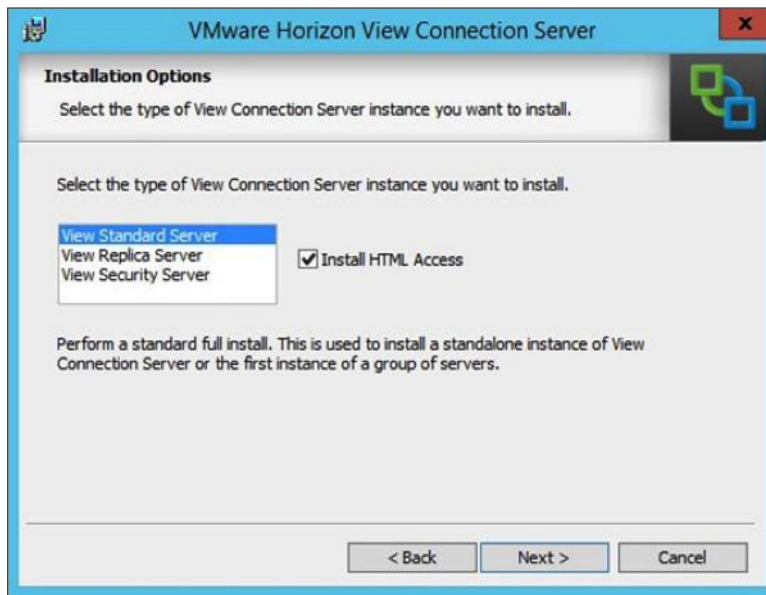
5. Review the license agreement, accept the terms and conditions, and click **Next**.



6. Choose where you want to install View Connection Server, and click **Next**.



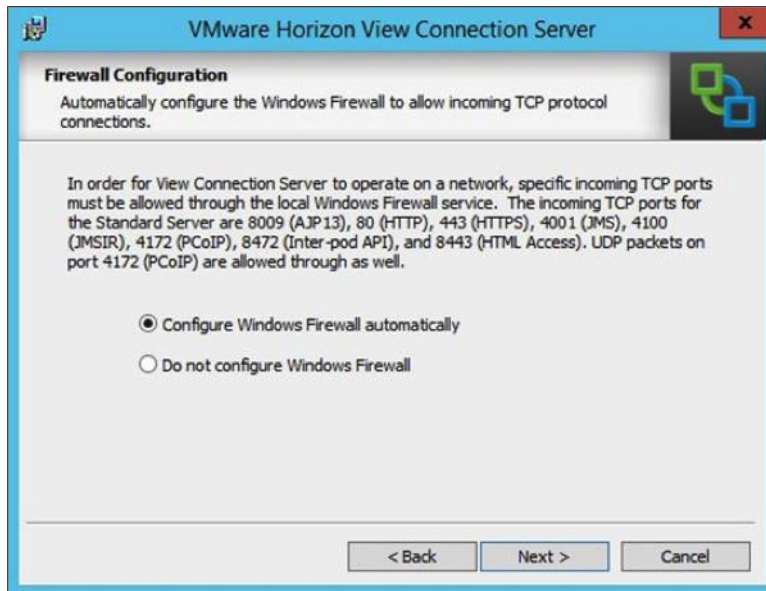
7. Select **View Standard Server**, select the **Install HTML Access** check box, and click **Next**.



8. Create a password to protect data backups, and click **Next**.

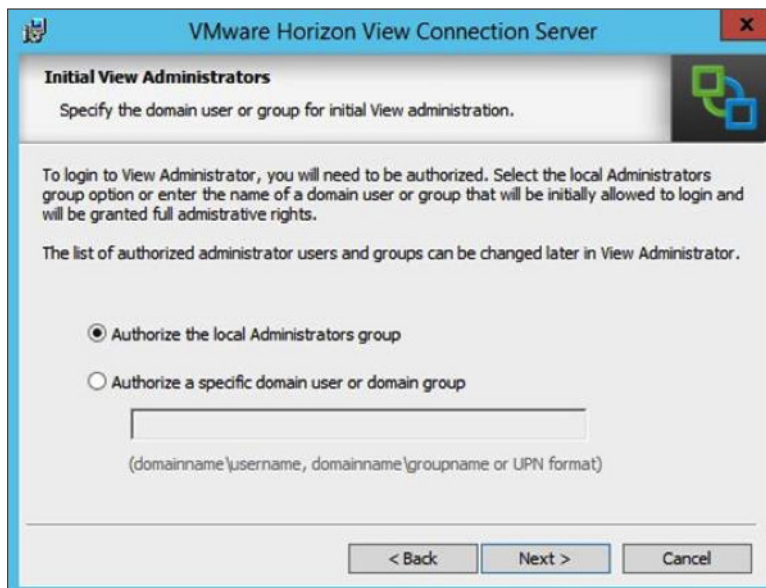


9. Choose whether to configure Windows Firewall automatically, and click **Next**.

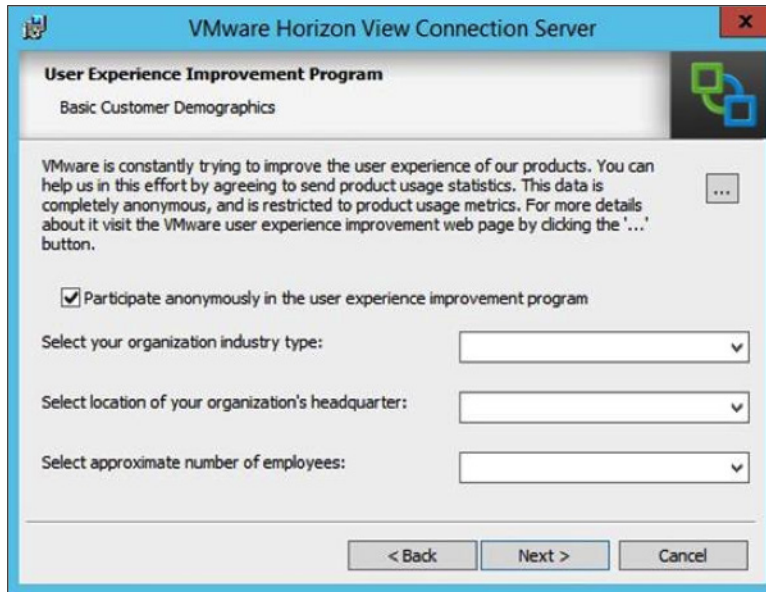


Note: The Windows Firewall ports are required for View Connection Server to function correctly. For the purposes of this exercise, **Configure Windows Firewall automatically** is selected. If you want to configure the ports manually, complete the required port configuration before proceeding to the next step.

10. Select which administrators group or specific administrator user you want to authorize to manage View Connection Server, and click **Next**.

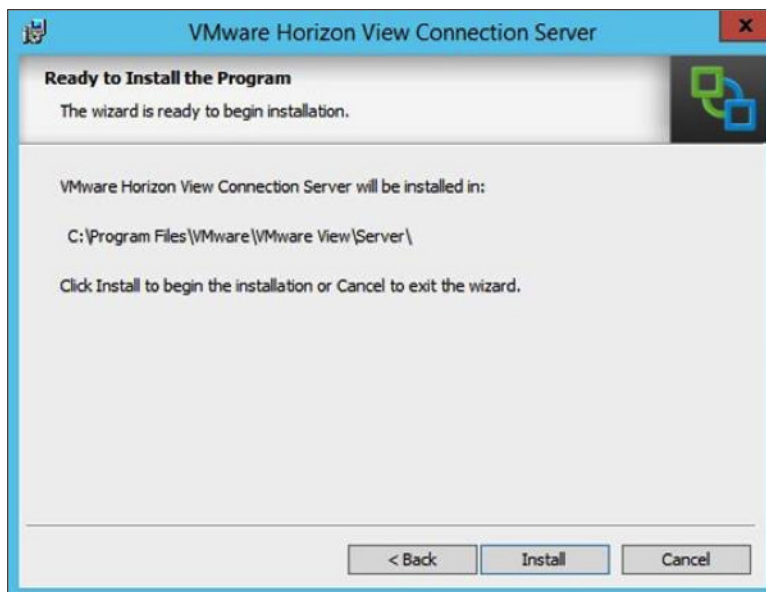


11. Choose whether to participate anonymously in the user experience improvement program, and, if so, select your answers from the drop-down menus, and click **Next**.



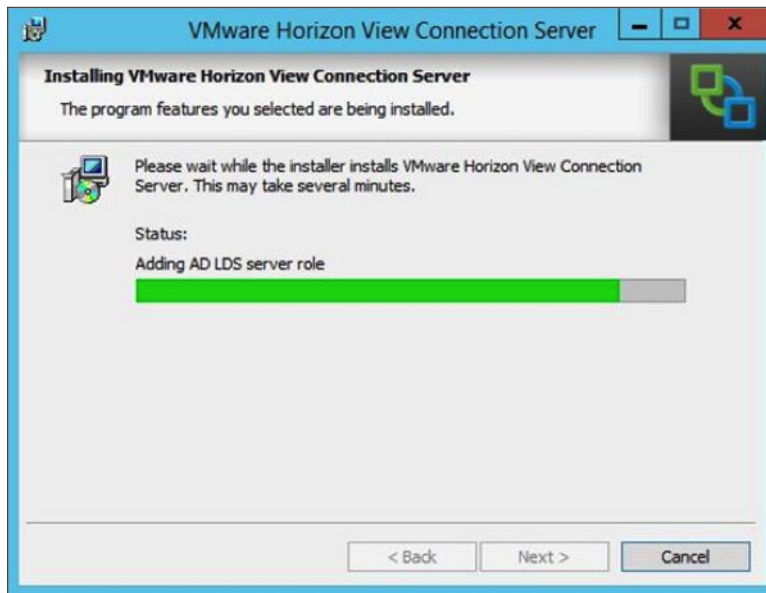
The screenshot shows a window titled "VMware Horizon View Connection Server" with a close button (X) in the top right corner. The window contains a section titled "User Experience Improvement Program" with a sub-header "Basic Customer Demographics". Below this, there is a paragraph of text explaining the program and a button with three dots (...). A checkbox is checked, labeled "Participate anonymously in the user experience improvement program". Below the checkbox are three drop-down menus: "Select your organization industry type:", "Select location of your organization's headquarter:", and "Select approximate number of employees:". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

12. Review or modify your selections by clicking **Back**, and when you are ready to proceed, click **Install**.

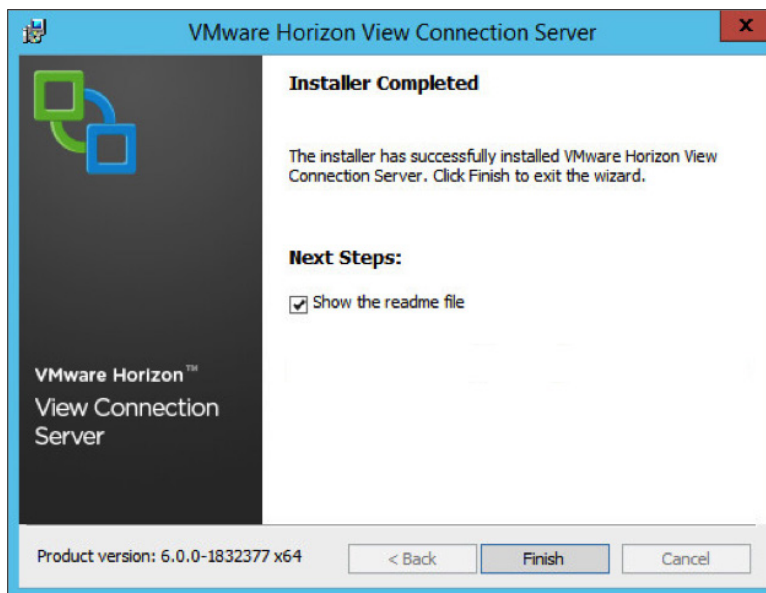


The screenshot shows a window titled "VMware Horizon View Connection Server" with a close button (X) in the top right corner. The window contains a section titled "Ready to Install the Program" with a sub-header "The wizard is ready to begin installation.". Below this, there is a paragraph of text stating "VMware Horizon View Connection Server will be installed in:" followed by the path "C:\Program Files\VMware\VMware View\Server\". Below the path is a paragraph of text stating "Click Install to begin the installation or Cancel to exit the wizard.". At the bottom of the window are three buttons: "< Back", "Install", and "Cancel".

You can monitor your installation status as it progresses.



13. When the Installer Completed window appears, indicate whether to open the readme file, and click **Finish** to close the View Connection Server installer.



You have now completed installing View Connection Server and can proceed to the next exercise to install a View security server.

Install a View Security Server

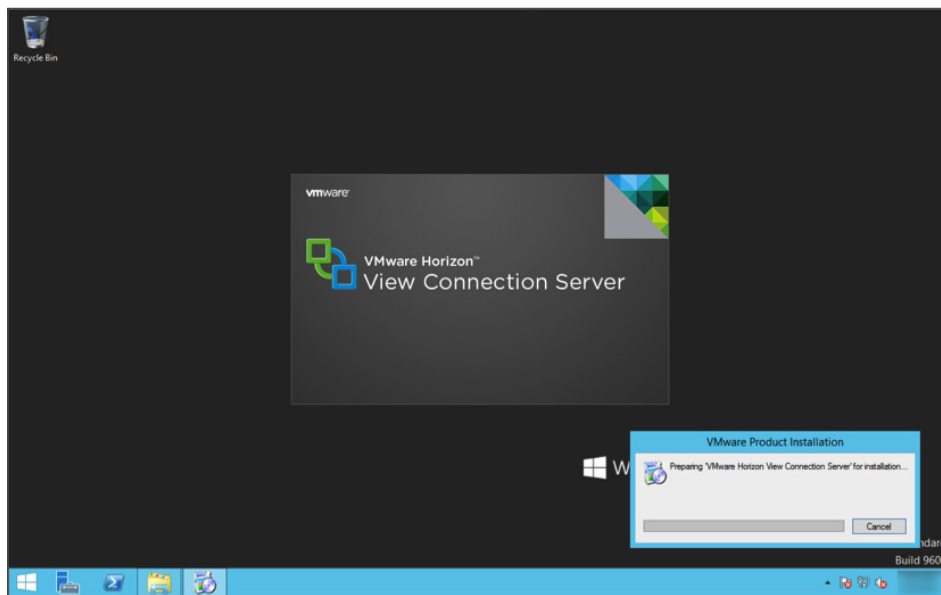
A View security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. Security servers ensure that the only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.

1. Log in to the virtual machine that you prepared as the target for installing View security server.

The virtual machine must meet the requirements detailed in the Installation Prerequisites.

2. Verify that the 64-bit View Connection Server installer is accessible by the operating system of the target virtual machine.
3. Launch and load the View Connection Server installer in the virtual machine.

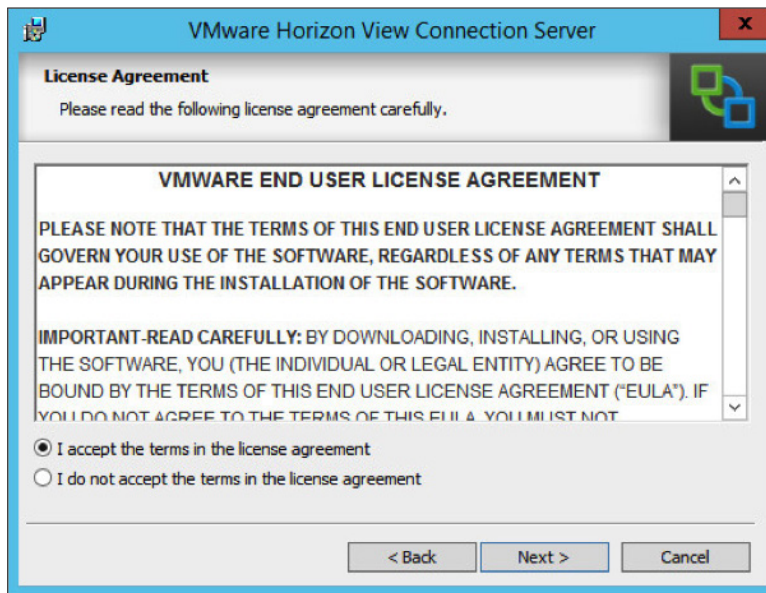
Note: The View security server is an installation option within the View Connection Server installer.



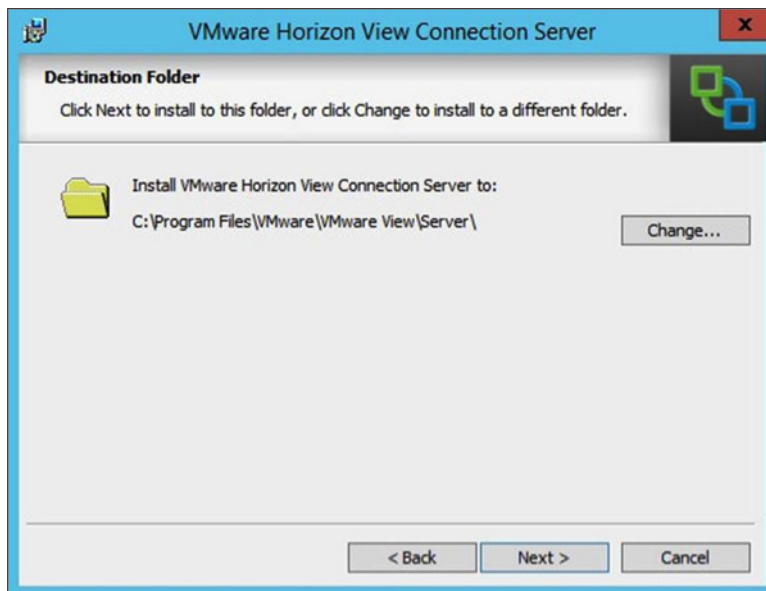
4. When the installer finishes loading, click **Next**.



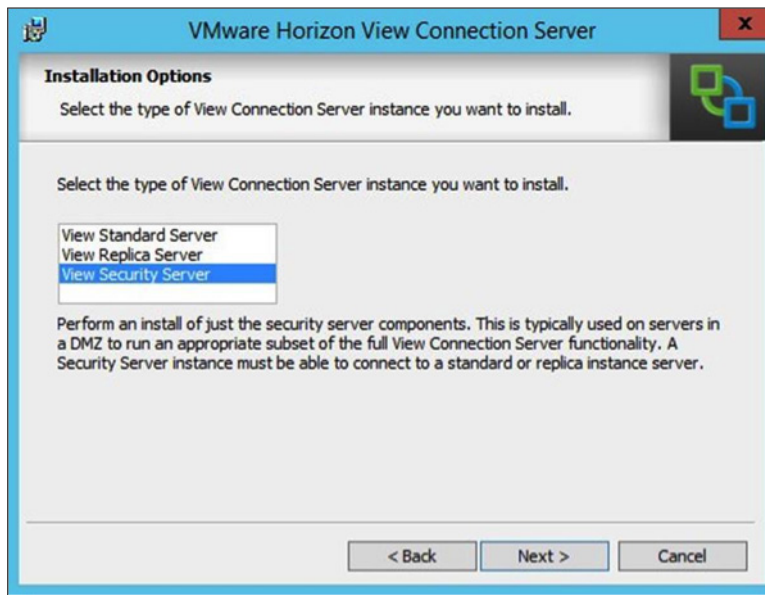
5. Review the license agreement, accept the terms and conditions, and click **Next**.



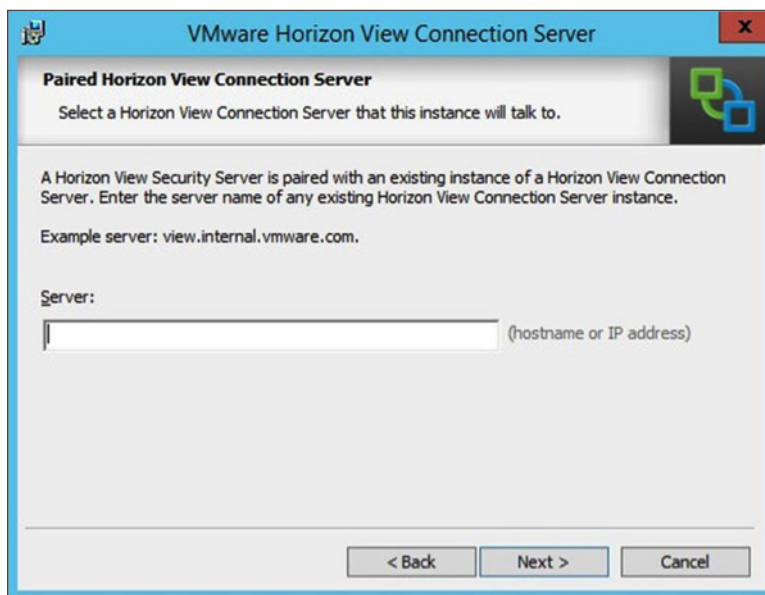
6. Choose where to install the View security server, and click **Next**.



7. Select **View Security Server**, and click **Next**.



8. In the Server text box, enter the FQDN of the View Connection Server you installed, to pair to the View security server.



You enter the FQDN in this format:

```
https://<fqdn-of-view-connection-server>/admin
```

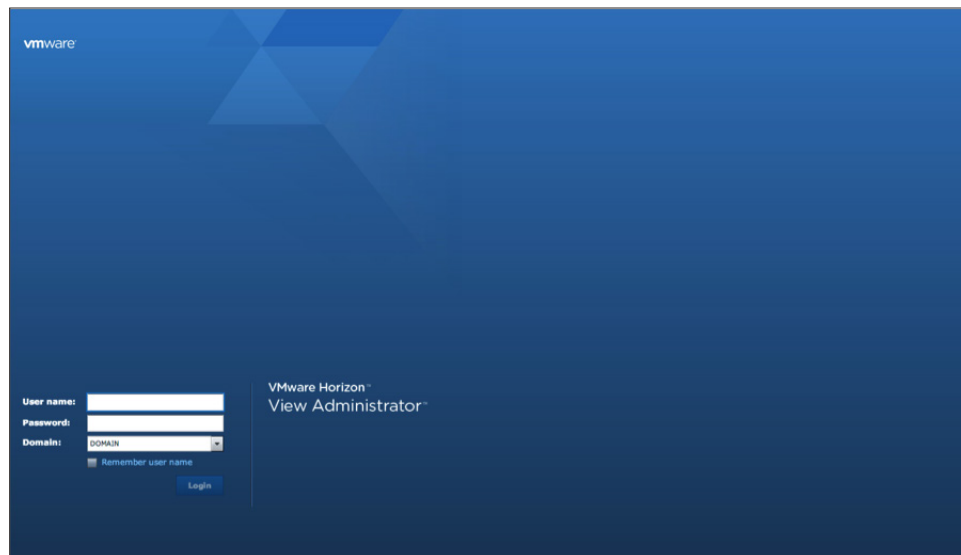
where **fqdn-of-view-connection-server** is the fully qualified domain name or the IP address of the View Connection Server.

9. Click **Next**.
10. Go to the View Administrator console to create a one-time pairing password for this session.



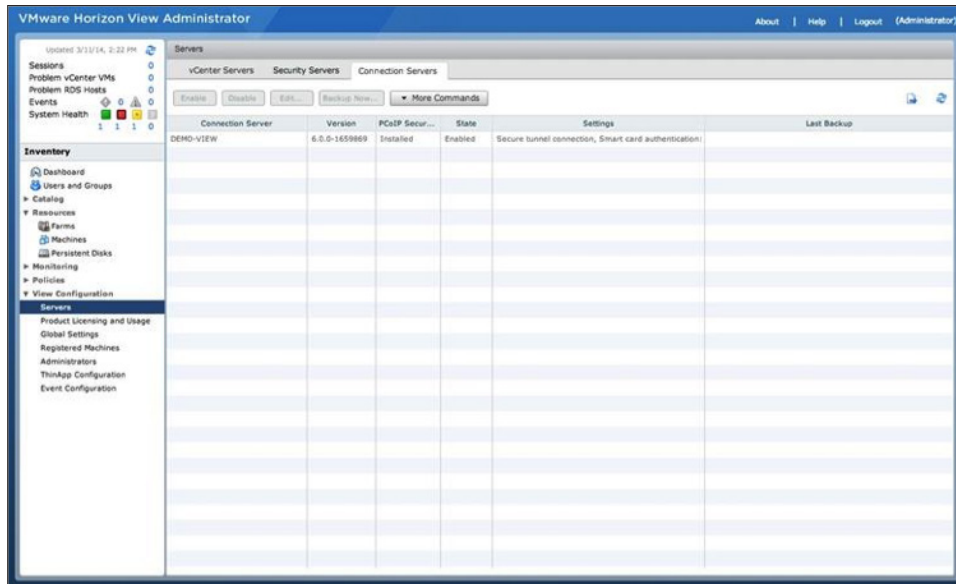
The screenshot shows a Windows-style dialog box titled "VMware Horizon View Connection Server". The main heading is "Paired Horizon View Connection Server Password". Below the heading, it says "Enter a password to pair with the Horizon View Connection Server." There is a paragraph of instructional text: "A password is required to pair this Security Server with a Connection Server. First specify the Pairing Password for the Connection Server in View Administrator. This password is set in View Administrator in 'View Configuration' > 'Servers'. Select the specified Connection Server and go to 'More Commands' > 'Specify Security Server Pairing Password'." Below this text is a text input field labeled "Password:". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

11. Log in to the View Administrator console using the credentials that you established in Install View Connection Server.

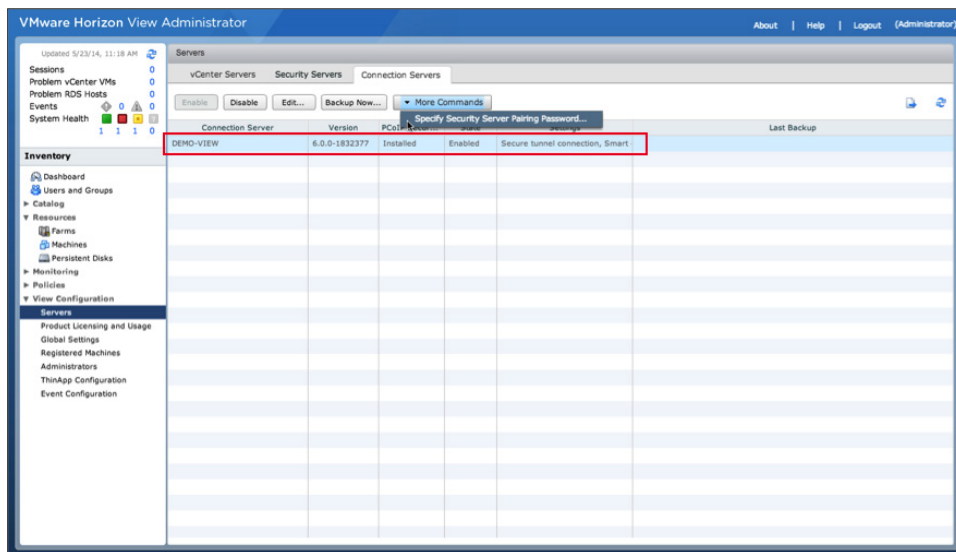


The screenshot shows the VMware Horizon View Administrator login interface. It has a dark blue background with the VMware logo in the top left. On the left side, there are three input fields: "User name:", "Password:", and "Domain:". Below the "Domain:" field is a checkbox labeled "Remember user name". To the right of these fields is a "Login" button. On the right side of the screen, the text "VMware Horizon View Administrator" is displayed.

12. In the View Administrator console
 - a. In the left menu, under View Configuration, click **Servers**.
 - b. In the Servers window, select the **Connection Servers** tab.

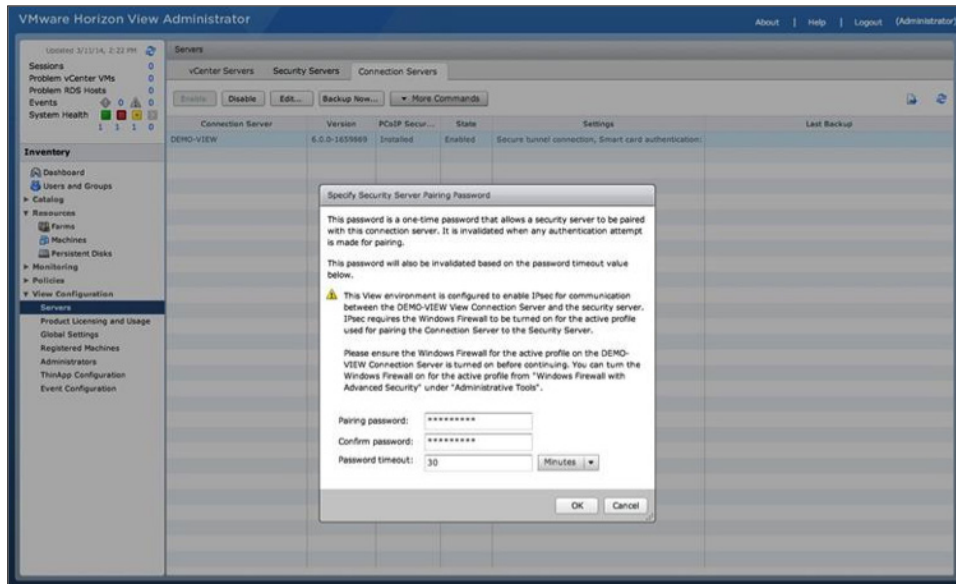


13. Select the View Connection Server that you installed in Exercise 1, and from the More Commands drop-down menu, select **Specify Security Server Pairing Password**.



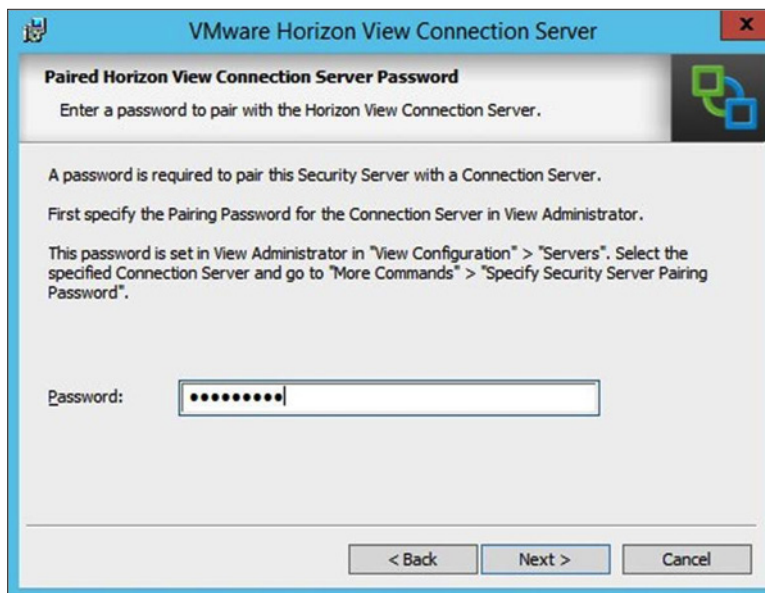
14. Specify a pairing password and a timeout value, and click **OK**.

Note: The security-server pairing password is a one-time password that permits a security server to be paired with a View Connection Server instance. As a security measure, the password becomes invalid after you provide it to the View Connection Server installation program.



When you finish setting the pairing password, stay logged in to the View Administrator console because you need to return to it to verify the security server installation.

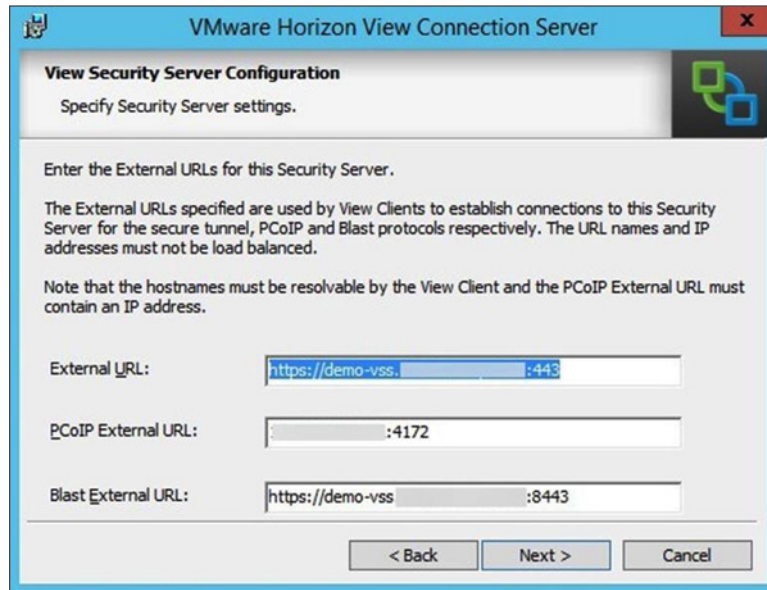
15. In the virtual machine where you are installing the View security server, enter the security-server pairing password, and click **Next**.



Note: This step initiates the pairing process, which can take a few minutes to complete.

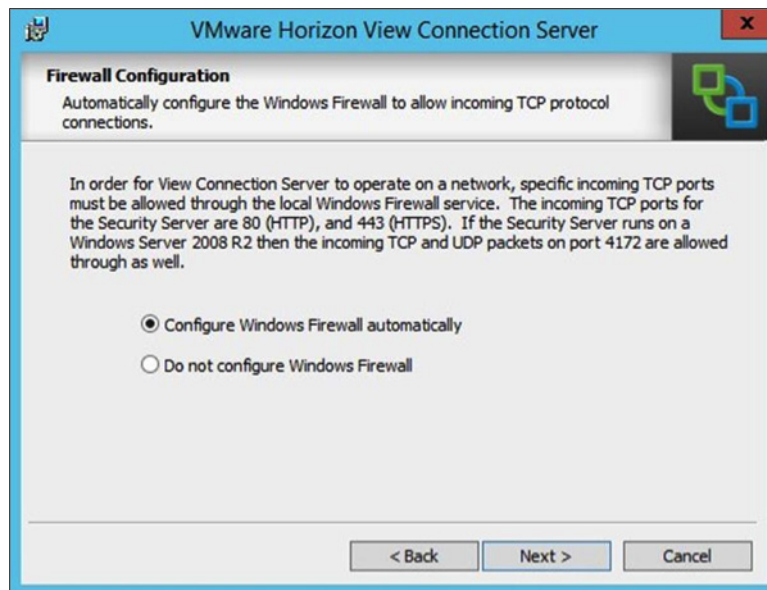
16. In the View Security Server Configuration dialog box, accept the default values for the external URLs or modify them, and click **Next**.

Note: The PCoIP External URL must contain an IP address and not a FQDN. You can change these values later in the View Administrator console.



The screenshot shows the 'View Security Server Configuration' dialog box. It has a title bar 'VMware Horizon View Connection Server' and a subtitle 'View Security Server Configuration'. Below the subtitle is the instruction 'Specify Security Server settings.' and a VMware logo. The main text area contains instructions: 'Enter the External URLs for this Security Server.', 'The External URLs specified are used by View Clients to establish connections to this Security Server for the secure tunnel, PCoIP and Blast protocols respectively. The URL names and IP addresses must not be load balanced.', and 'Note that the hostnames must be resolvable by the View Client and the PCoIP External URL must contain an IP address.' There are three text input fields: 'External URL:' with the value 'https://demo-vss.:443', 'PCoIP External URL:' with the value ':4172', and 'Blast External URL:' with the value 'https://demo-vss.:8443'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

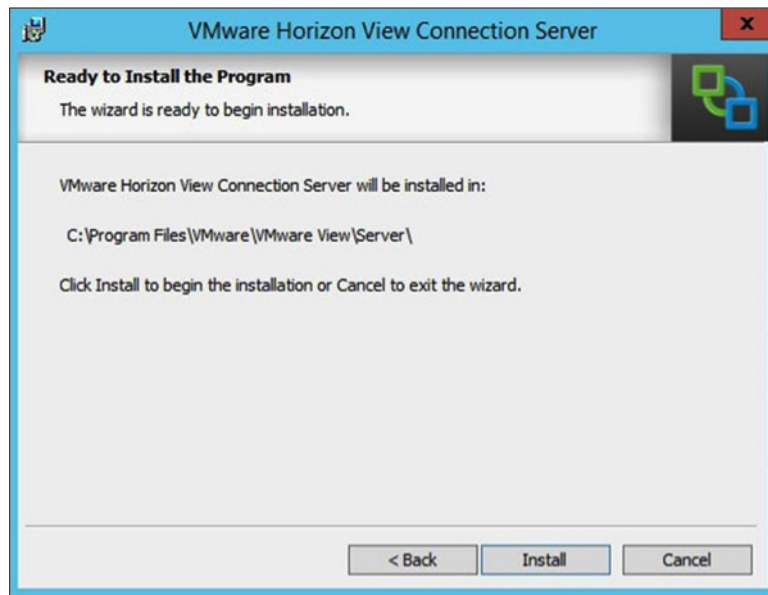
17. Choose whether to configure the Windows Firewall automatically, and click **Next**.



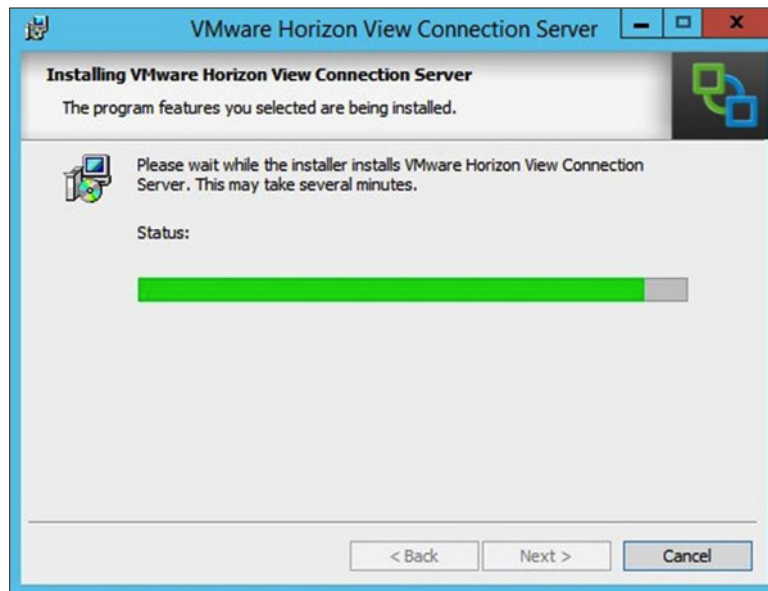
The screenshot shows the 'Firewall Configuration' dialog box. It has a title bar 'VMware Horizon View Connection Server' and a subtitle 'Firewall Configuration'. Below the subtitle is the instruction 'Automatically configure the Windows Firewall to allow incoming TCP protocol connections.' and a VMware logo. The main text area contains a paragraph: 'In order for View Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Security Server are 80 (HTTP), and 443 (HTTPS). If the Security Server runs on a Windows Server 2008 R2 then the incoming TCP and UDP packets on port 4172 are allowed through as well.' There are two radio button options: 'Configure Windows Firewall automatically' (which is selected) and 'Do not configure Windows Firewall'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Note: The Windows Firewall ports are required for the View security server to function correctly. For the purposes of this exercise, **Configure Windows Firewall automatically** was selected. If you want to configure the ports manually, complete the port configuration required before going to the next step.

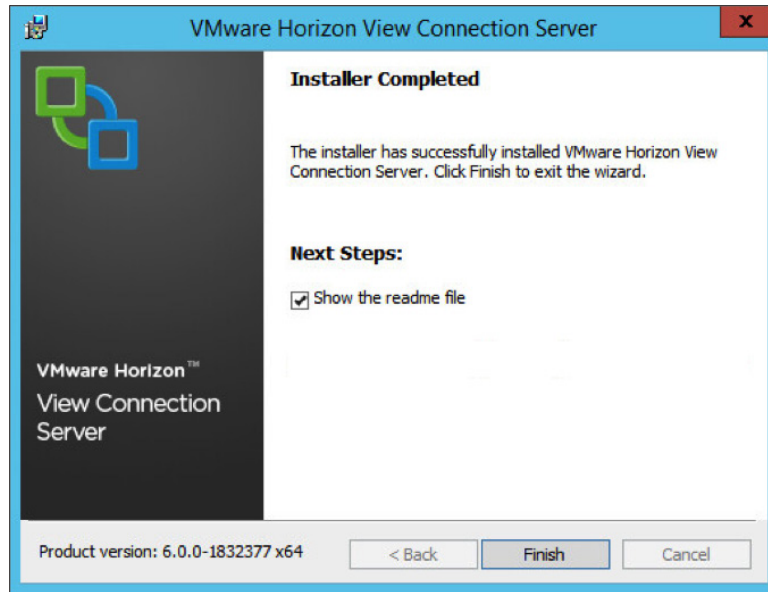
18. Click **Install** to complete the installation.



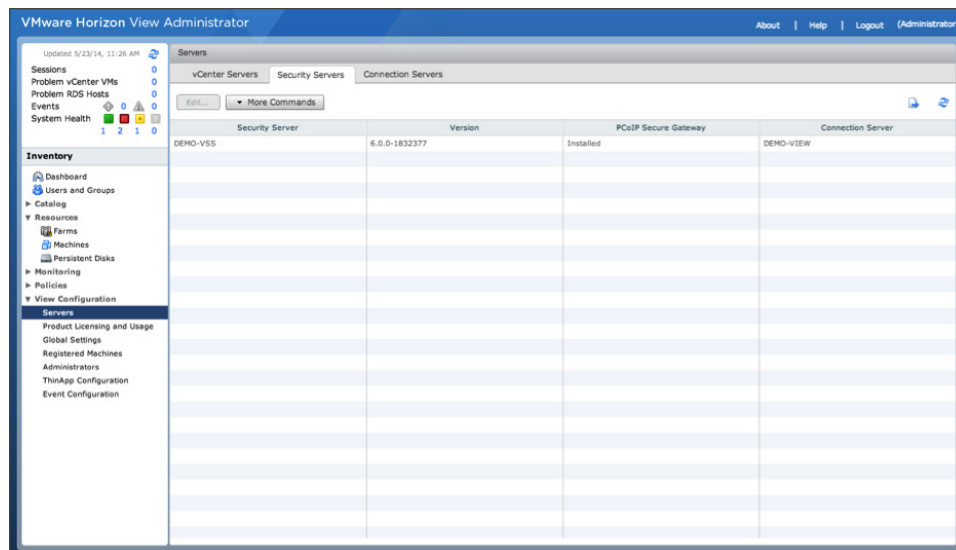
You can monitor the installation as it progresses.



19. When the Installer Completed window appears, indicate whether to automatically open the readme file, and click **Finish** to close the installer.



20. To verify the View security server installation and pairing, go to the View Administrator console:
- Under **View Configuration > Servers**, click the **Security Servers** tab.
 - Verify the host name of the View security server and the host name of the View Connection Server that it is paired to.



You have now completed installing the View security server and pairing it to the View Connection Server. You can now proceed to the next exercise and install the View Composer Server.

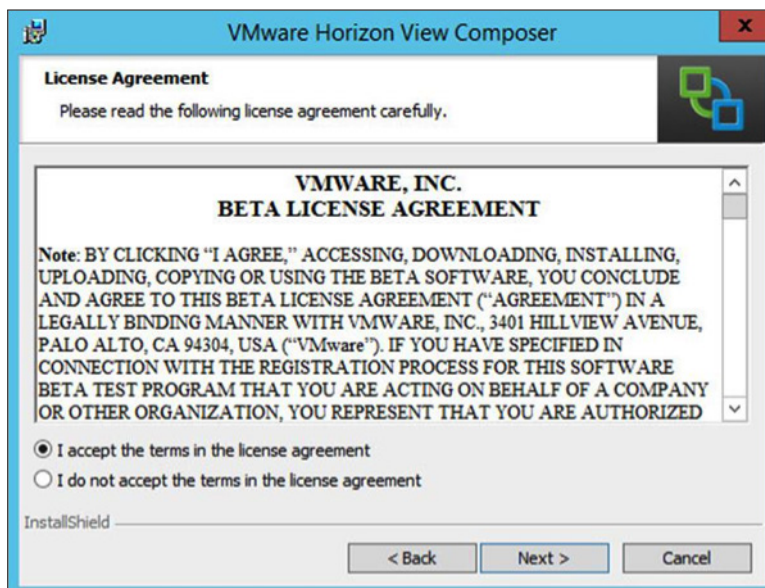
Install View Composer Server

View Composer Server is an optional service that enables you to manage pools of similar desktops, called *linked-clone desktops*. Linked-clone desktop images can optimize your use of storage space and facilitate updates.

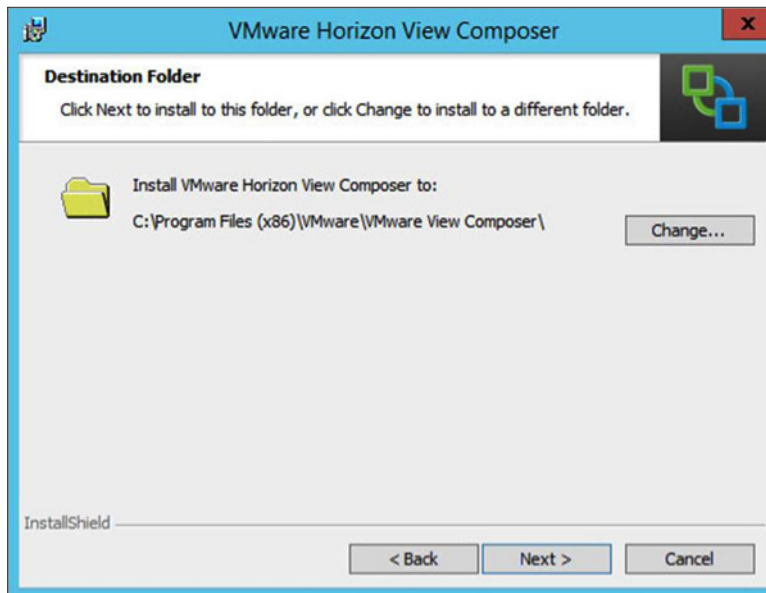
1. Log in to the virtual machine that you prepared as the target for installing View Composer Server.
Verify that the virtual machine meets the prerequisites listed in [Installation Prerequisites](#) and that the appropriate native SQL driver is installed for your database.
2. Verify that the 64-bit VMware View Composer Server installer is accessible by the operating system of the target virtual machine.
3. Launch and load the View Composer Server installer, and click **Next**.



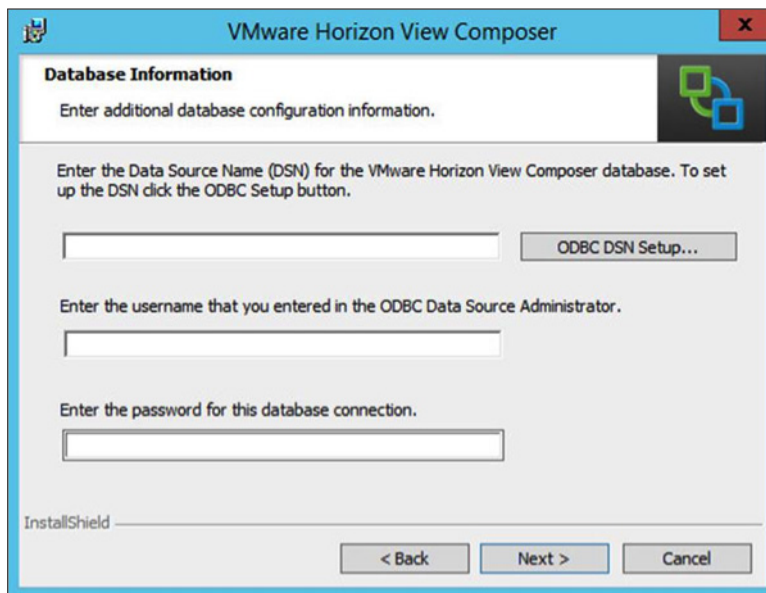
4. Review the license agreement, accept the terms and conditions, and click **Next**.



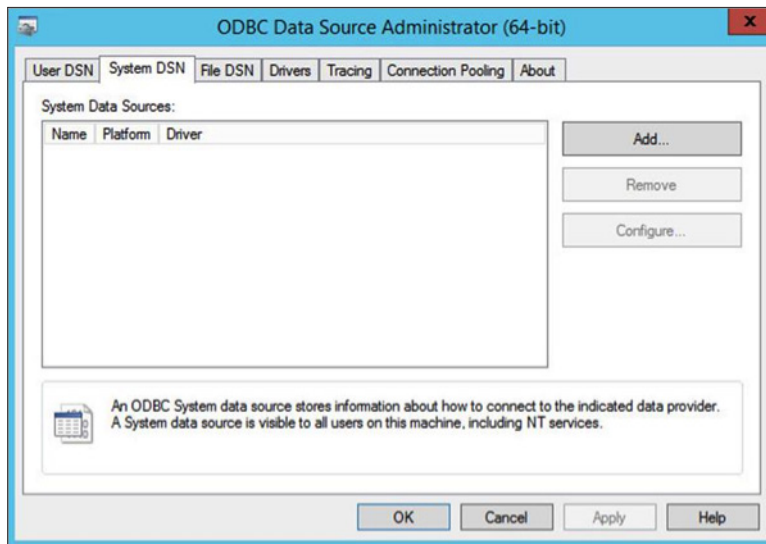
5. Choose where you want to install the View Composer Server, and click **Next**.



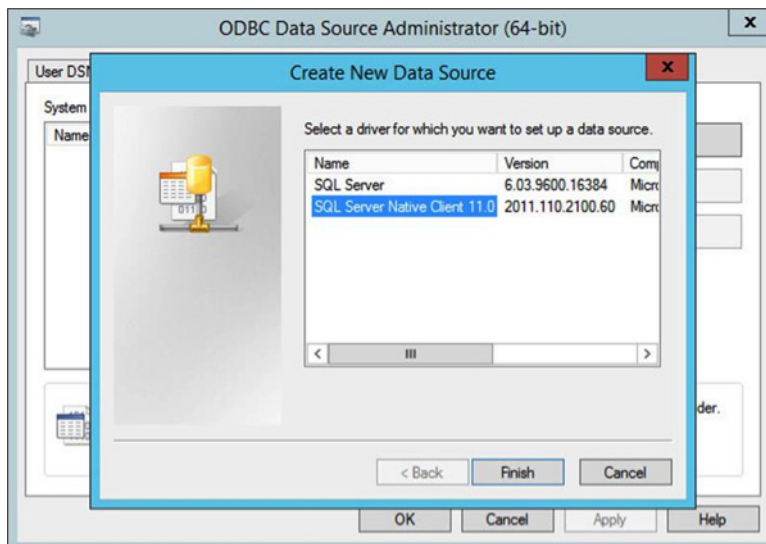
6. Click **ODBC DSN Setup** to establish a new Data Source Name (DSN) to define the connection between View Composer Server and your database.



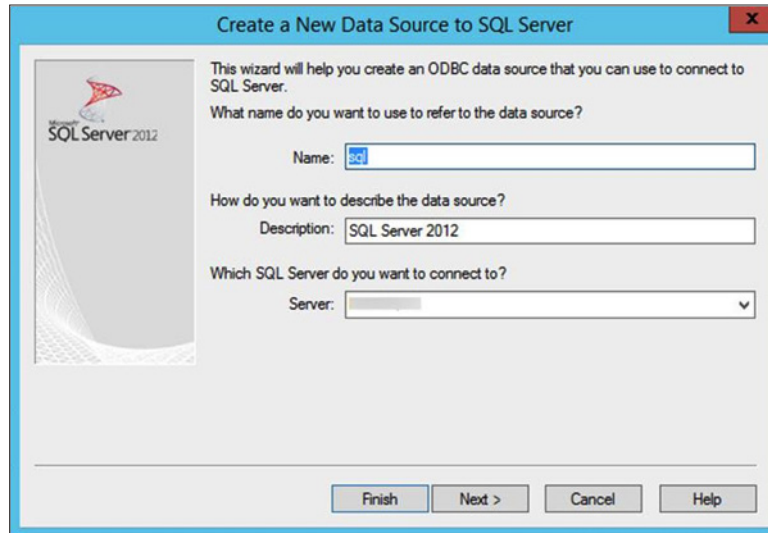
7. In the ODBC Data Source Administrator dialog box, click the **System DSN** tab, and click **Add**.



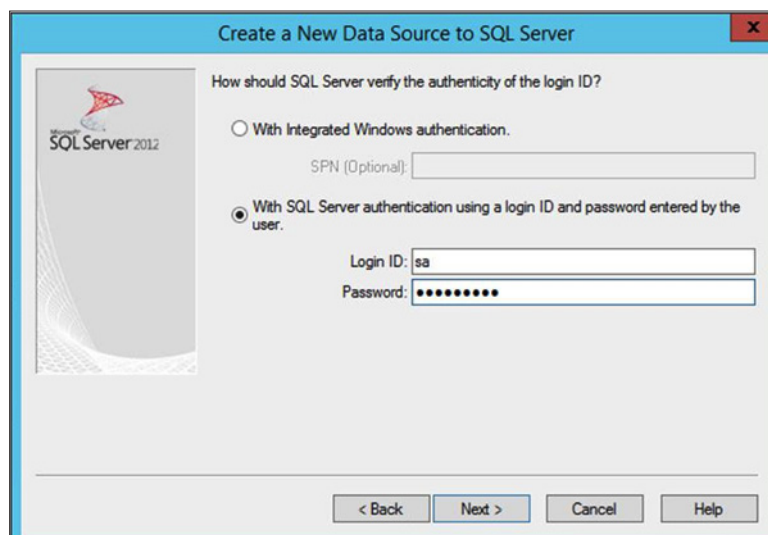
8. Select the driver for your database, and click **Finish**.
For the purposes of this exercise, SQL Server Native Client 11.0 was selected.



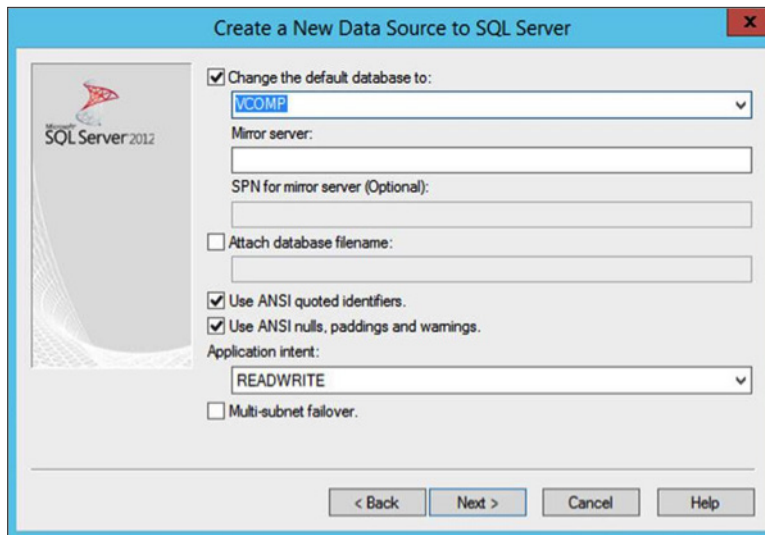
9. In the Create a New Data Source to SQL Server dialog box, enter the required information for your data source:
 - a. **Name:** Unique name that refers to the data source that you are connecting to
 - b. **Description:** Optional
 - c. **Server:** Address of your SQL Server in the format **FQDN/<SQLInstanceName>** or **IP/<SQLInstanceName>**.



10. Click **Next**.
11. Enter the SQL Server **Login ID** and **Password**, and click **Next**.



12. Select the **Change the default database to** check box, and from the drop-down menu, select the database that you created for View Composer Server data, and click **Next**.



Create a New Data Source to SQL Server

☒ Change the default database to:
 VCOMP

Mirror server:

SPN for mirror server (Optional):

☐ Attach database filename:

☒ Use ANSI quoted identifiers.
☒ Use ANSI nulls, paddings and warnings.

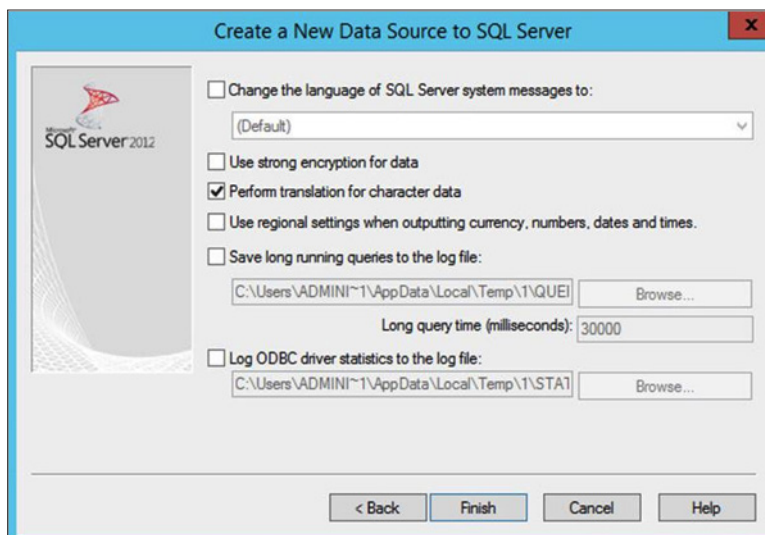
Application intent:
 READWRITE

☐ Multi-subnet failover.

< Back Next > Cancel Help

13. After selecting the database options that you want (optional), click **Finish**.

Additional database options are available, but not required, for the View Composer Server database.



Create a New Data Source to SQL Server

☐ Change the language of SQL Server system messages to:
 (Default)

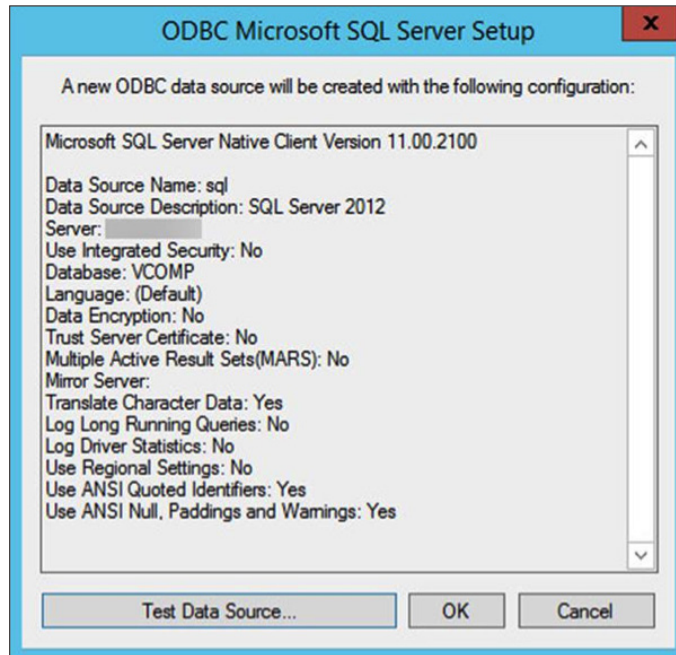
☐ Use strong encryption for data
☒ Perform translation for character data
☐ Use regional settings when outputting currency, numbers, dates and times.

☐ Save long running queries to the log file:
 C:\Users\ADMINI~1\AppData\Local\Temp\1\QUEI Browse...
 Long query time (milliseconds): 30000

☐ Log ODBC driver statistics to the log file:
 C:\Users\ADMINI~1\AppData\Local\Temp\1\STA1 Browse...

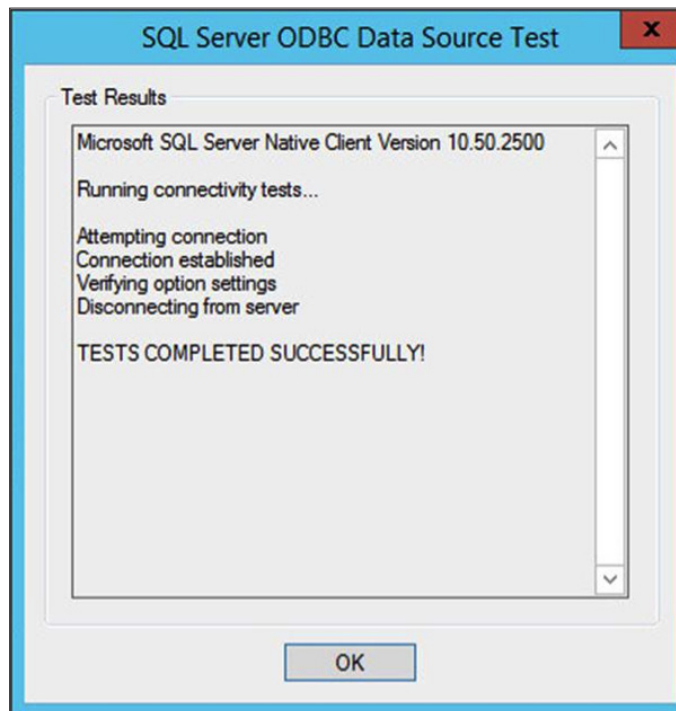
< Back Finish Cancel Help

14. When the summary of DSN options displays, click **Test Data Source** to verify the connection to the database.



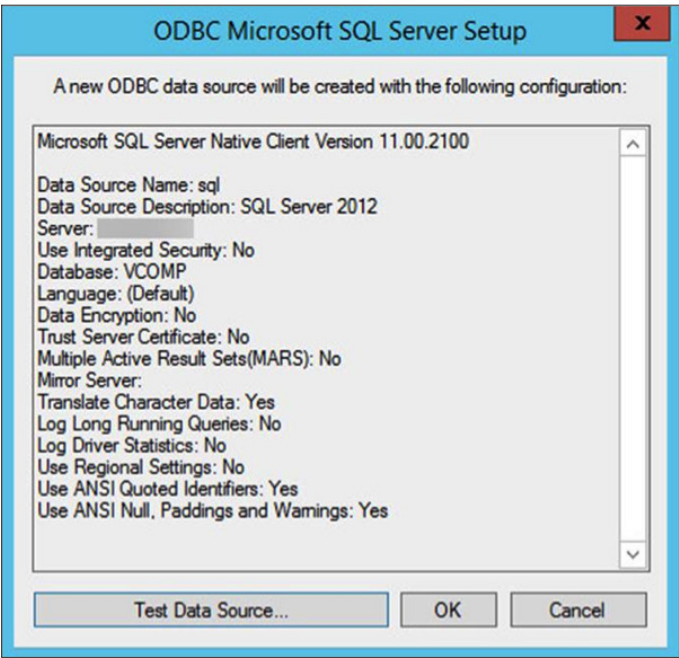
15. Verify that the test completed successfully:

- If your connection test completed successfully, click **OK** to continue.

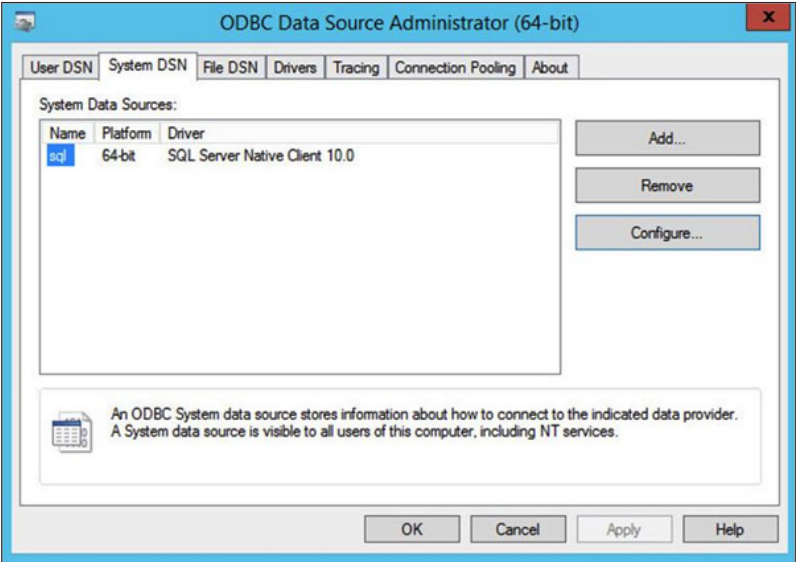


- If your connection test was unsuccessful, click **OK**, and in the next window, click **Cancel** to go back and change the parameters in the previous windows. Retest until the test results are successful.

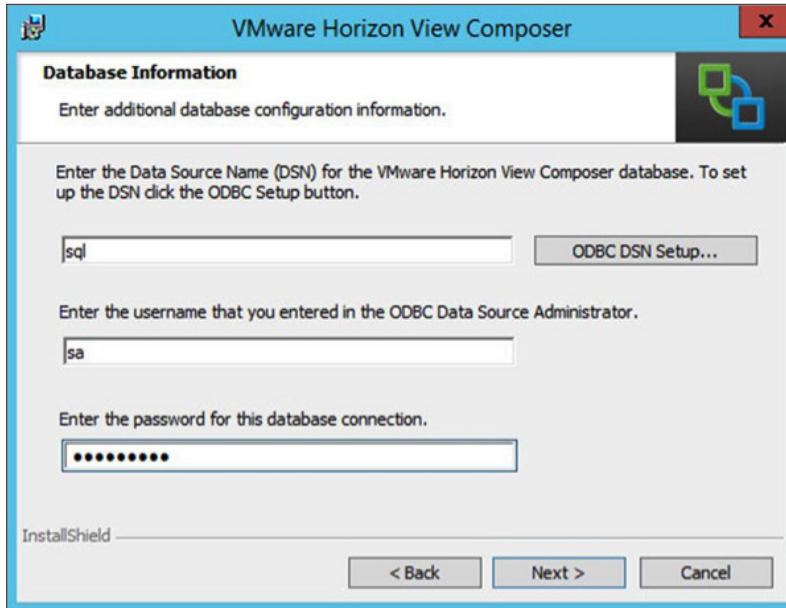
16. Click **OK** to add the System DSN to your ODBC Data Source Administrator List.



17. When the System DSN tab displays the System Data Sources, select the new System DSN name, and click **OK**.

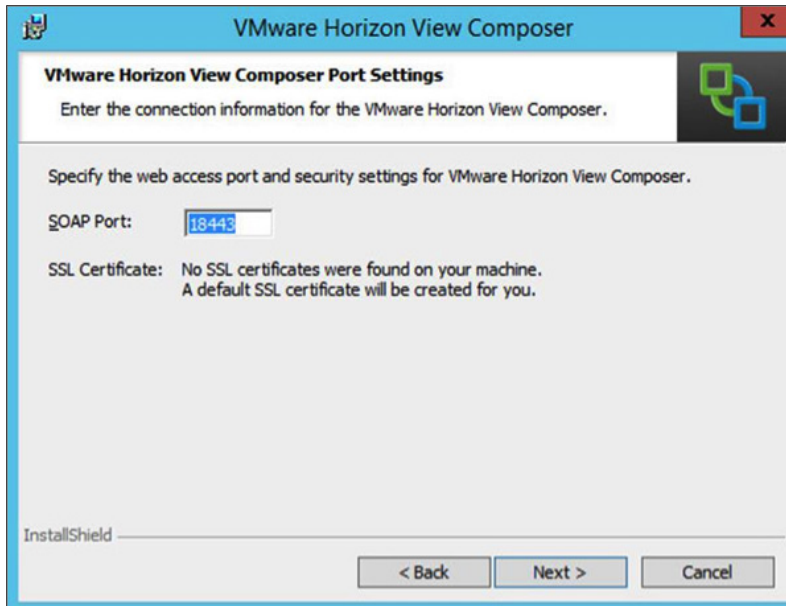


18. After the System DSN is created, and the Setup Wizard brings you back to the VMware Horizon View Composer Server installer, enter the System DSN name, user name, and password, and click **Next**.



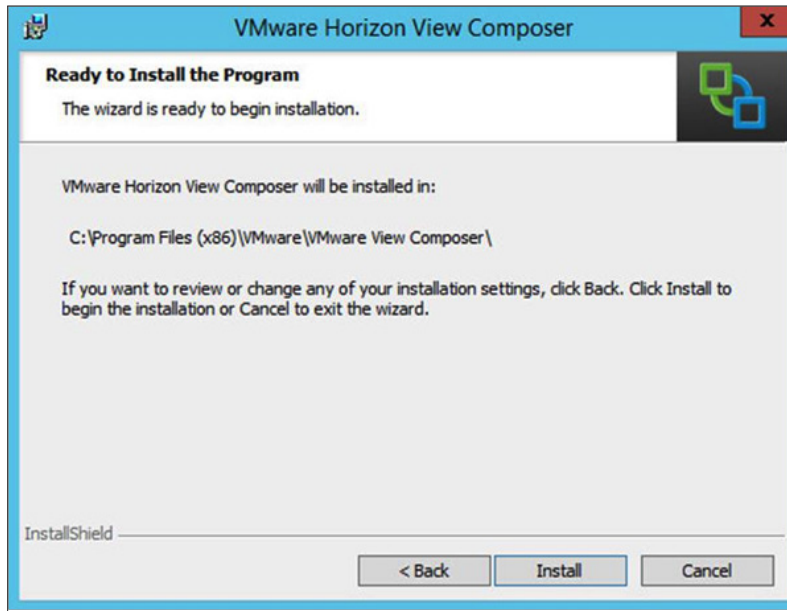
The screenshot shows the "VMware Horizon View Composer" window with the "Database Information" tab selected. The window has a blue title bar and a red close button. The main area is white with a blue header bar. The text "Enter additional database configuration information." is displayed. Below this, there is a text box for the Data Source Name (DSN) containing "sql", a button labeled "ODBC DSN Setup...", a text box for the username containing "sa", and a password field with masked characters. At the bottom, there are buttons for "< Back", "Next >", and "Cancel".

19. Specify a **SOAP Port** for View Composer Server communication by either accepting the default value or entering a preferred port, and click **Next**.



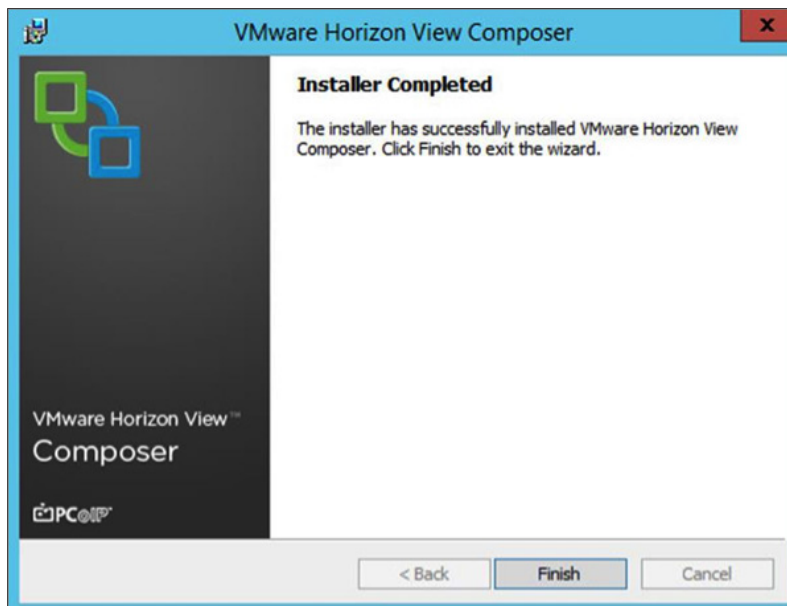
The screenshot shows the "VMware Horizon View Composer" window with the "VMware Horizon View Composer Port Settings" tab selected. The window has a blue title bar and a red close button. The main area is white with a blue header bar. The text "Enter the connection information for the VMware Horizon View Composer." is displayed. Below this, there is a text box for the SOAP Port containing "18443", and a section for the SSL Certificate stating "No SSL certificates were found on your machine. A default SSL certificate will be created for you." At the bottom, there are buttons for "< Back", "Next >", and "Cancel".

20. Review your selections and modify them, if necessary, by clicking **Back**. When you are ready to proceed, click **Install**.

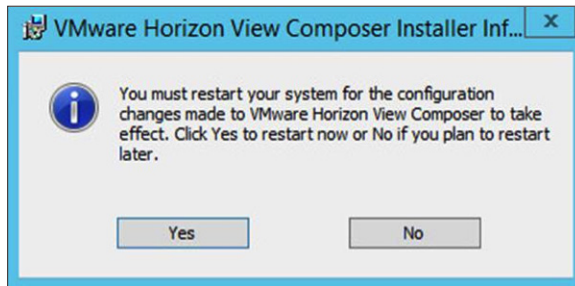


You can monitor the installation progress.

21. When the Installer Completed window appears, click **Finish**.



22. To finalize the installation, click **Yes** to reboot the virtual machine.



You are now ready proceed to set up a Remote Desktop Session Host (RDSH) server to use for application and desktop remoting.

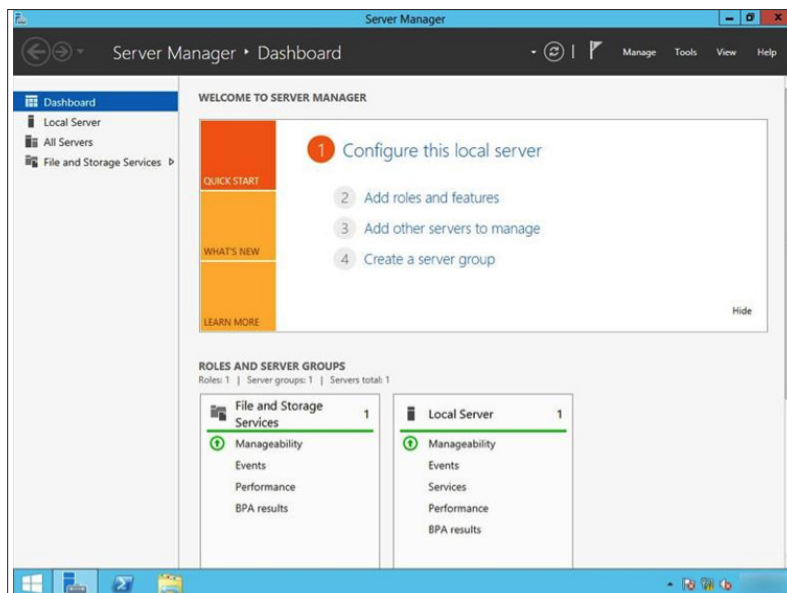
Remote Desktop Session Host Configuration

After installing the View components, you can set up an RDSH server. The host is required for setting up RDSH desktop and application pools. If you have an existing RDSH server that is already configured, you can skip the set-up exercises and proceed to [Install View Agent on the RDSH Server](#) and [Configure Group Policy Settings for RDSH](#). This section contains the following exercises:

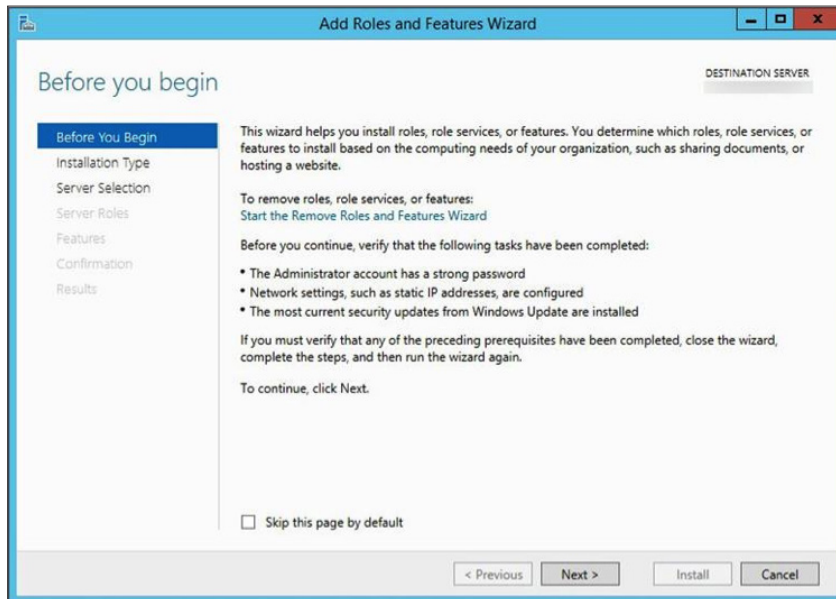
- [Set Up an RDSH server on Windows Server 2012 R2](#)
- [Install View Agent on the RDSH server](#)
- [Configure Group Policy settings for RDSH](#)

Set Up an RDSH Server on Windows Server 2012 R2

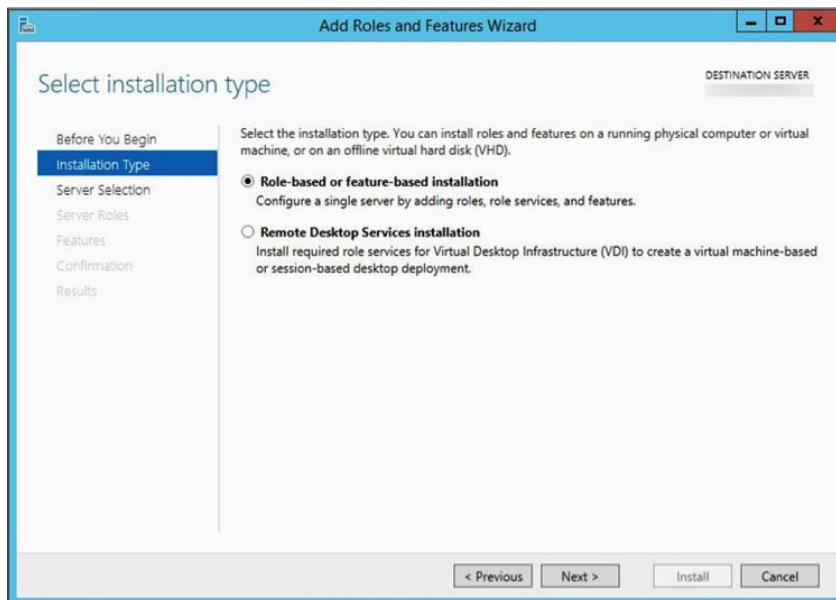
1. Log in as the administrator to the virtual machine that you prepared as your target RDSH server and start the Server Manager tool.
2. Click **Add roles and features**.



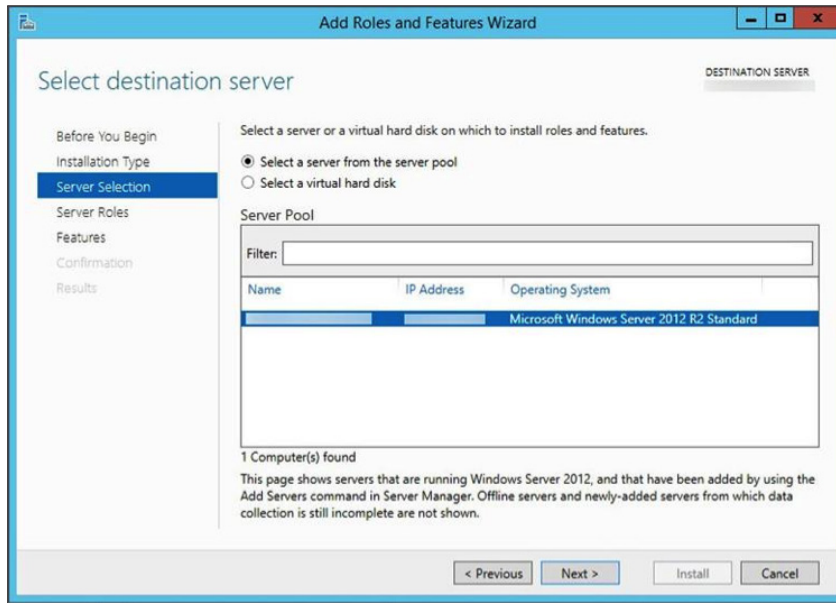
3. To start the Add Roles and Features wizard, click **Next**.



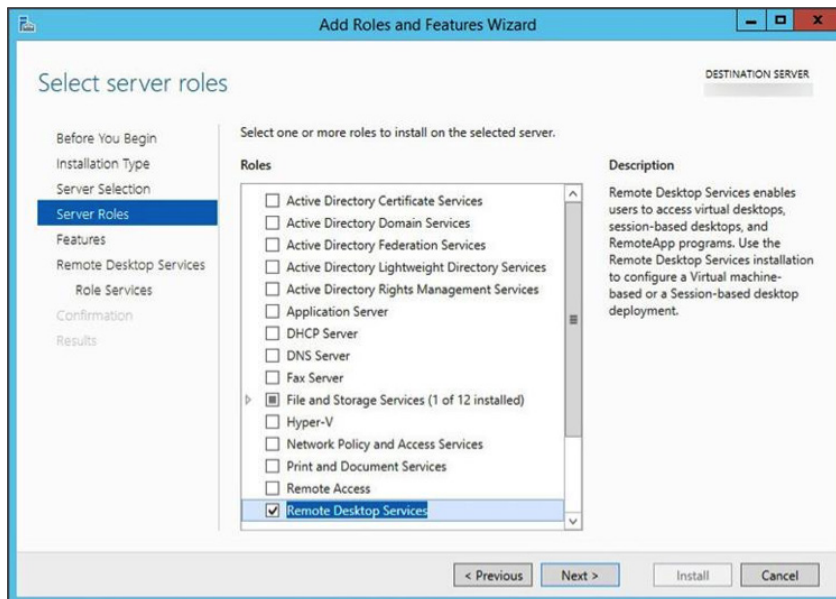
4. To install the RDSH role to your server, select **Role-based or feature-based installation**, and click **Next**.



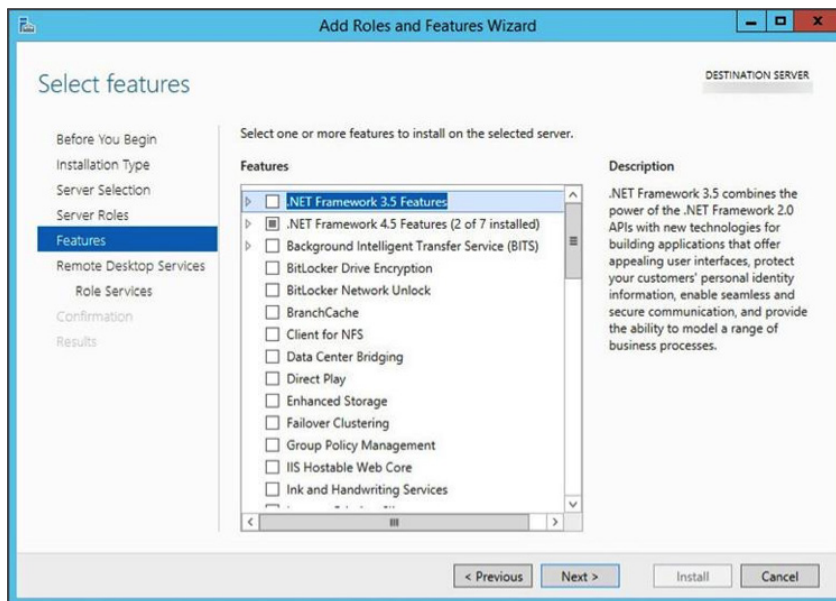
5. Select where to add the role:
 - a. Because you are installing this role on the server on which you are running the wizard, choose **Select a server from the server pool**.
 - b. Click the name of the server that you are logged in to, and click **Next**.



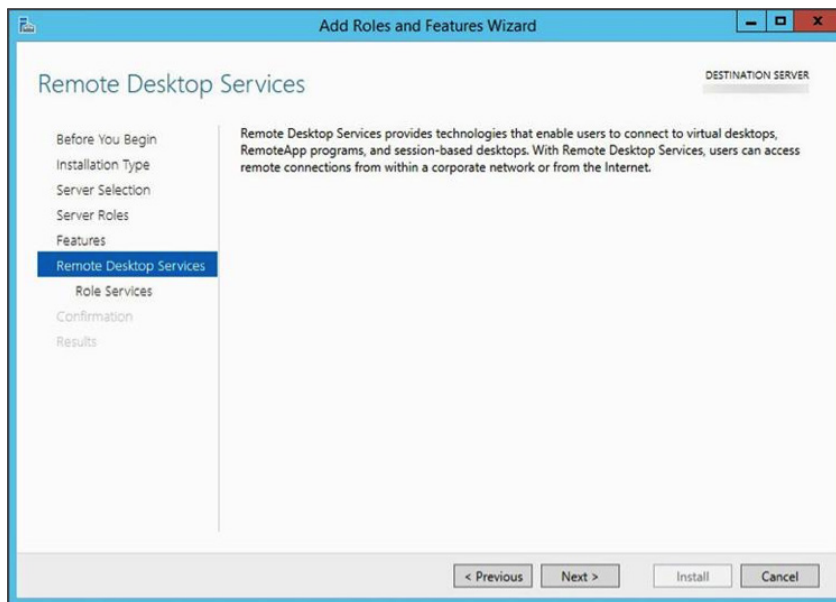
6. In the Roles list, select **Remote Desktop Services**, and click **Next**.



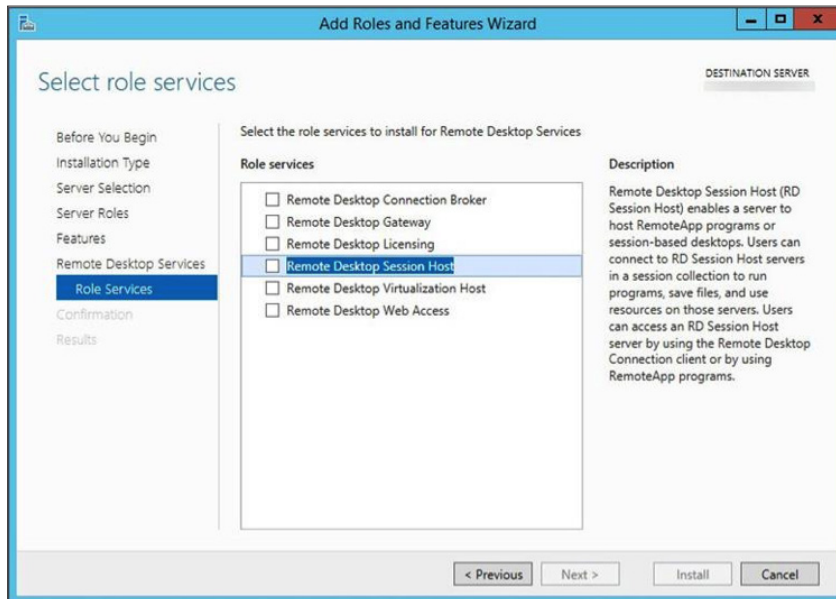
7. On the Select Features page, accept the default features by clicking **Next**.



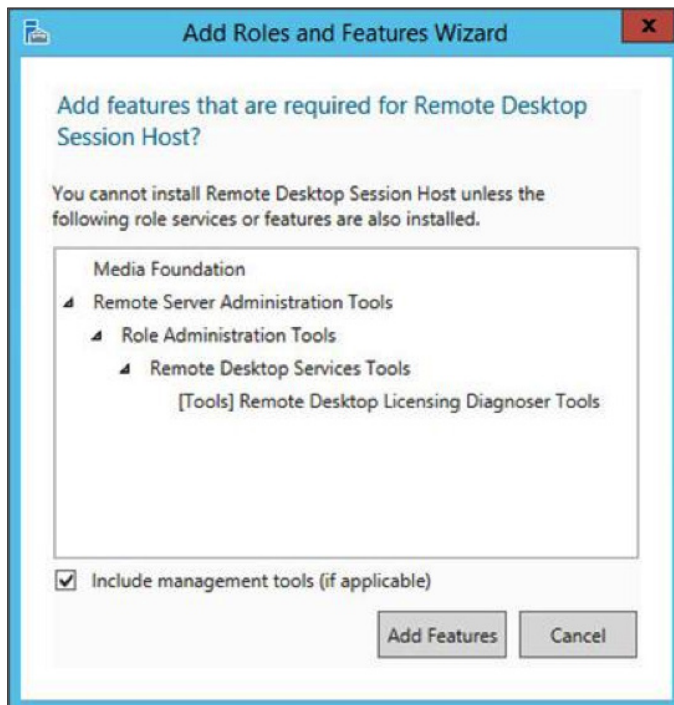
8. Review the Remote Desktop Services role, and click **Next**.



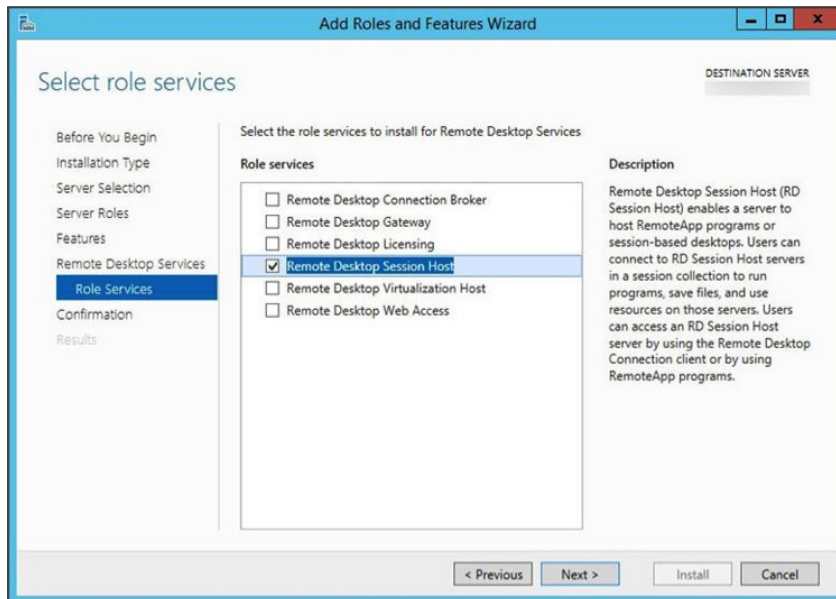
9. In the Role Services list, click **Remote Desktop Session Host**.



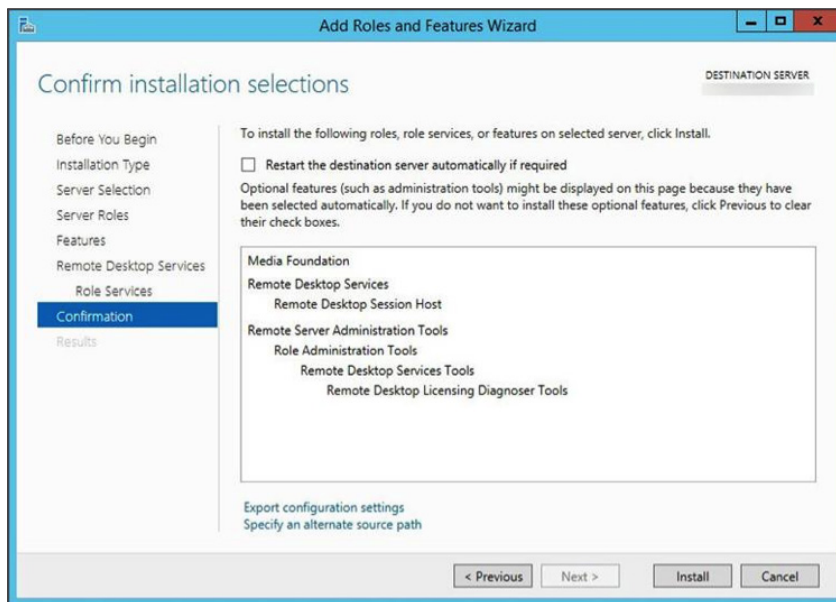
10. In the Add Roles and Features Wizard dialog box, click **Add Features**.



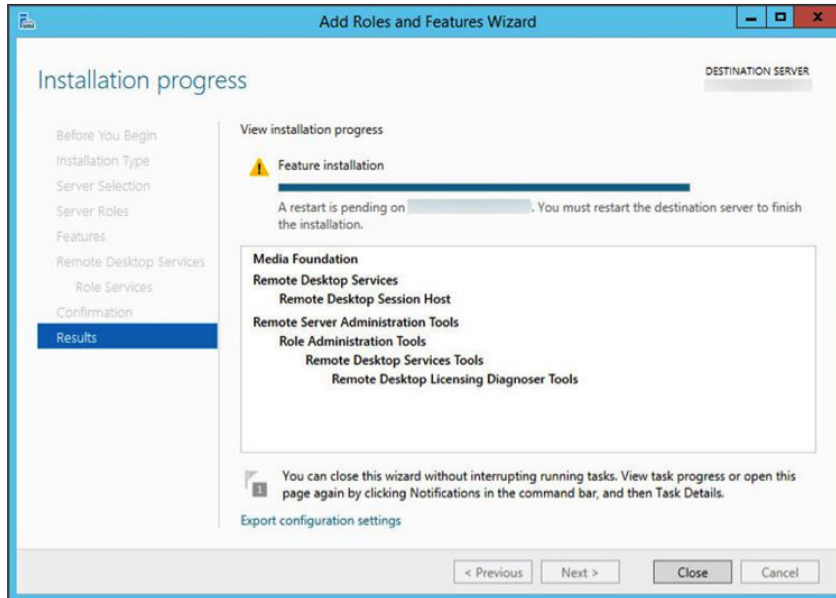
11. In the Select Role Services page with Remote Desktop Session Host selected, click **Next**.



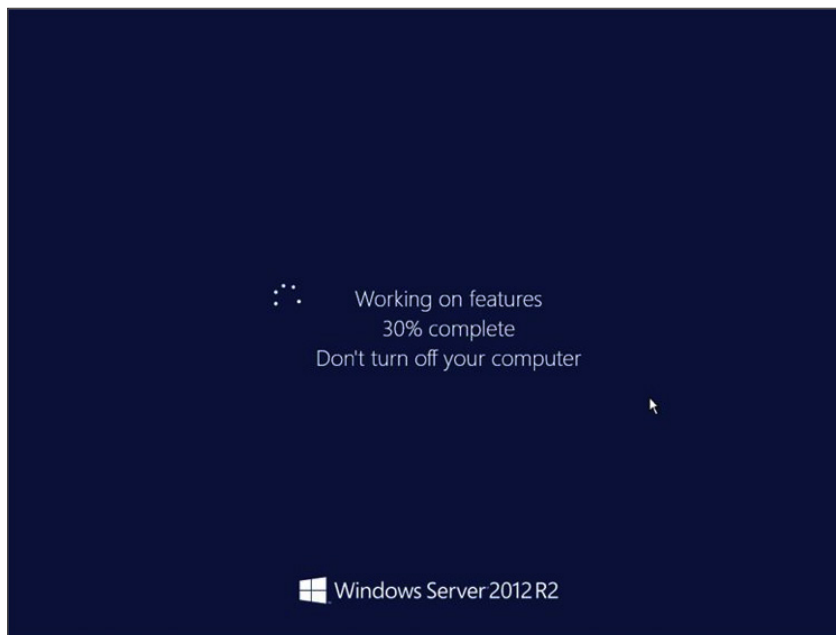
12. Review your selections, and click **Previous** to make changes or, if acceptable, click **Install**.



You can monitor the installation progress. When the installation is complete, you are prompted to manually reboot the system.



13. Do not turn off your computer while the system is completing the installation.

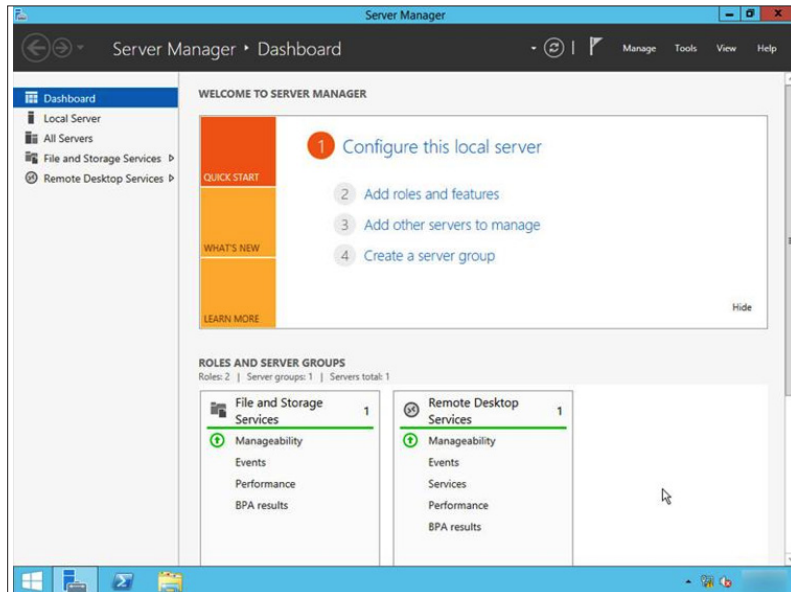


14. When the installation is finished:

- a. Log in to your system as administrator.
- b. Launch the Server Manager to confirm that your installation has completed successfully.

The Remote Desktop Services role now appears in the Server Manager dashboard.

Note: Be sure to properly license your host. See the article on RD Session Host Licensing: [Specify the Remote Desktop Licensing Mode on an RD Session Host Server](#).



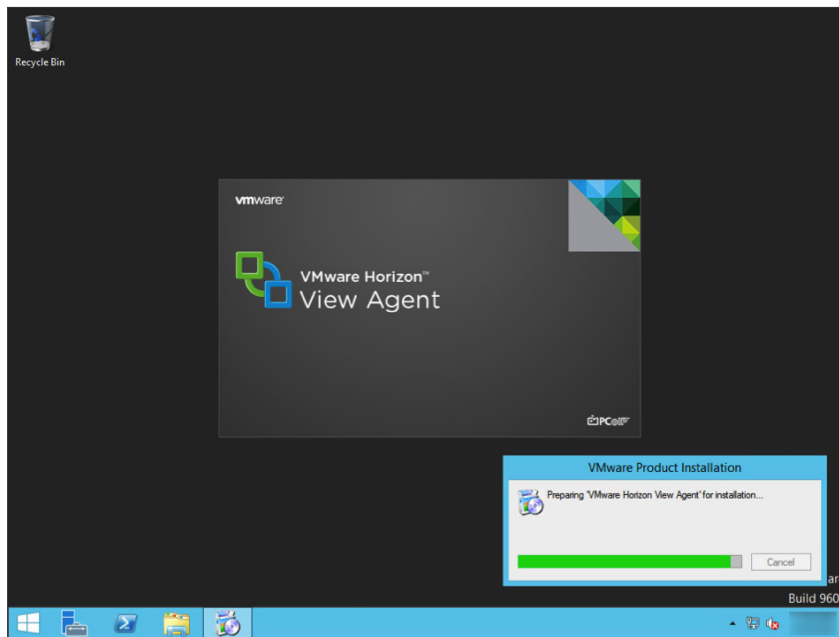
You have successfully configured your RDSH server. The next step is to install View Agent on the RDSH server.

Install View Agent on the RDSH Server

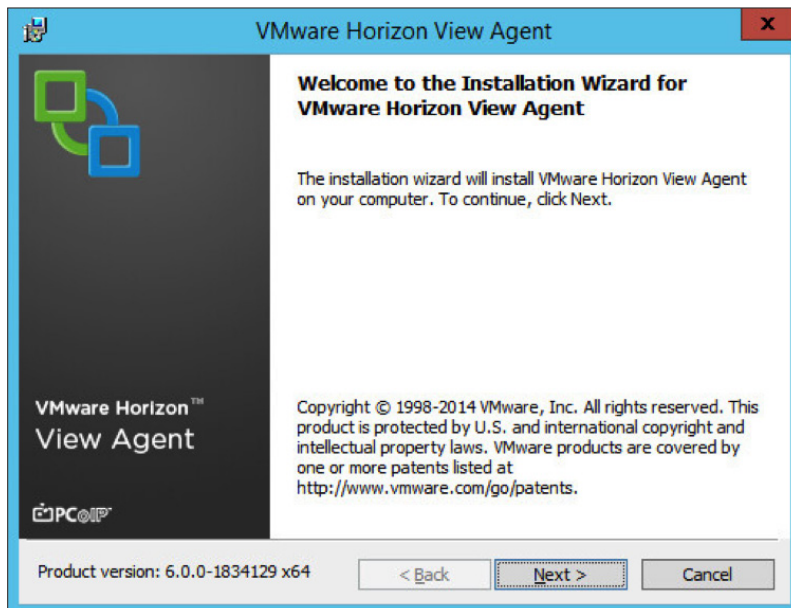
You must install the View Agent service on all virtual machines managed by vCenter Server so that View Connection Server can communicate with them. View Agent also provides features such as connection monitoring, virtual printing, persona management, and access to locally connected USB devices.

1. Launch the VMware View Agent installer with the Run As Administrator option.

You must be able to access the installer from your virtual machine.



2. When the installer has loaded, click **Next**.

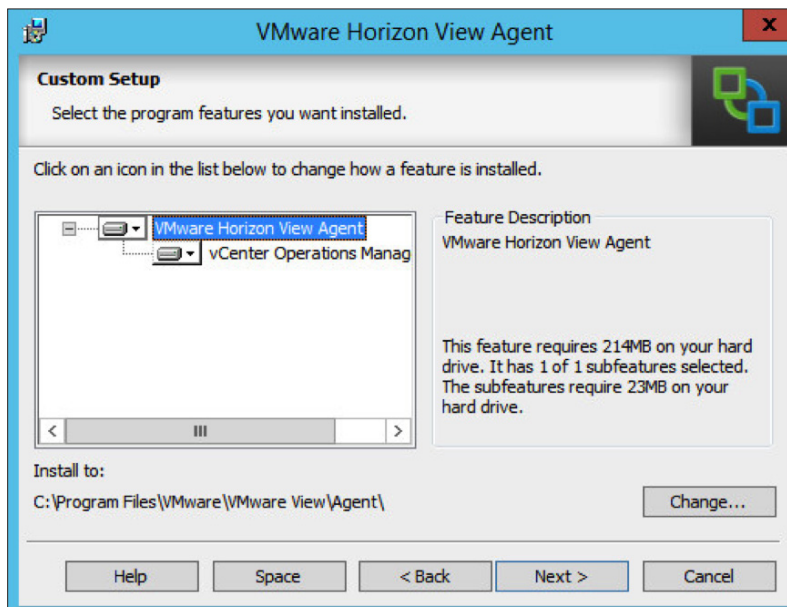


3. Read the license agreement, accept the terms and conditions, and click **Next**.

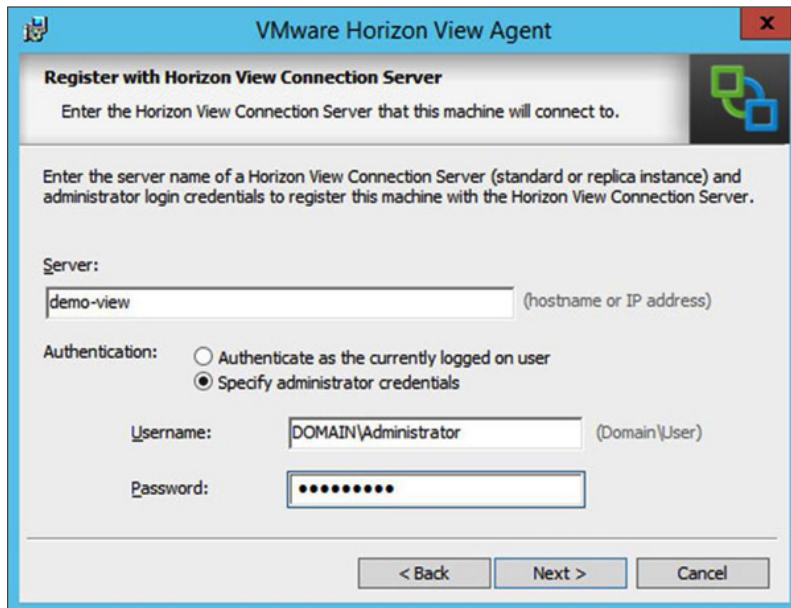


The Custom Setup window lists the features that you can install for View Agent. You can use the default settings.

4. Select the features you want installed in View Agent, and click **Next**.



5. Register the RDSH server with your View Connection Server:
 - a. In the Server text box, enter the View Connection Server host name.
 - b. Select an authentication method. If you select **Specify administrator credentials**, enter the user name and password.
 - c. Click **Next**.

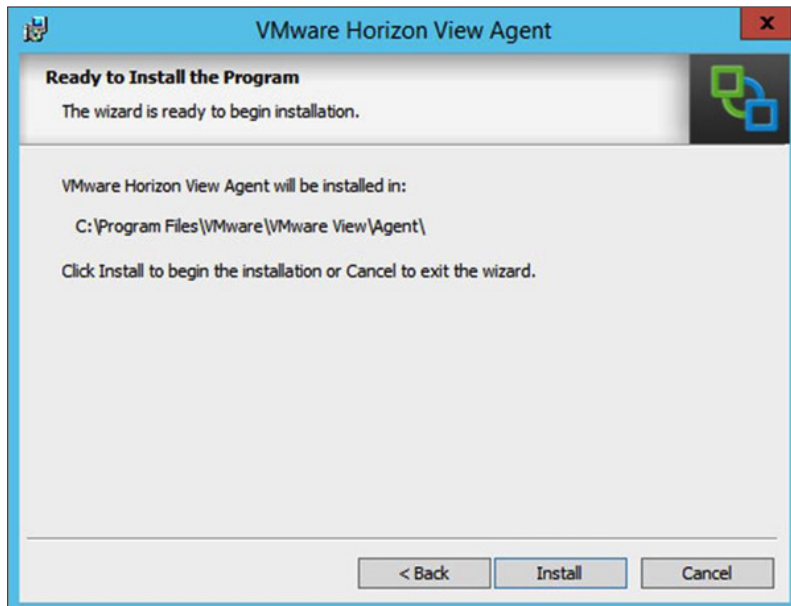


The screenshot shows the 'Register with Horizon View Connection Server' dialog box. The title bar reads 'VMware Horizon View Agent'. The main heading is 'Register with Horizon View Connection Server' with a sub-instruction: 'Enter the Horizon View Connection Server that this machine will connect to.' Below this, a larger instruction states: 'Enter the server name of a Horizon View Connection Server (standard or replica instance) and administrator login credentials to register this machine with the Horizon View Connection Server.'

The 'Server:' label is followed by a text box containing 'demo-view' and a hint '(hostname or IP address)'. Under the 'Authentication:' section, there are two radio buttons: 'Authenticate as the currently logged on user' (unselected) and 'Specify administrator credentials' (selected). Below these, the 'Username:' label is followed by a text box containing 'DOMAIN\Administrator' and a hint '(Domain\User)'. The 'Password:' label is followed by a masked password field represented by ten dots.

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

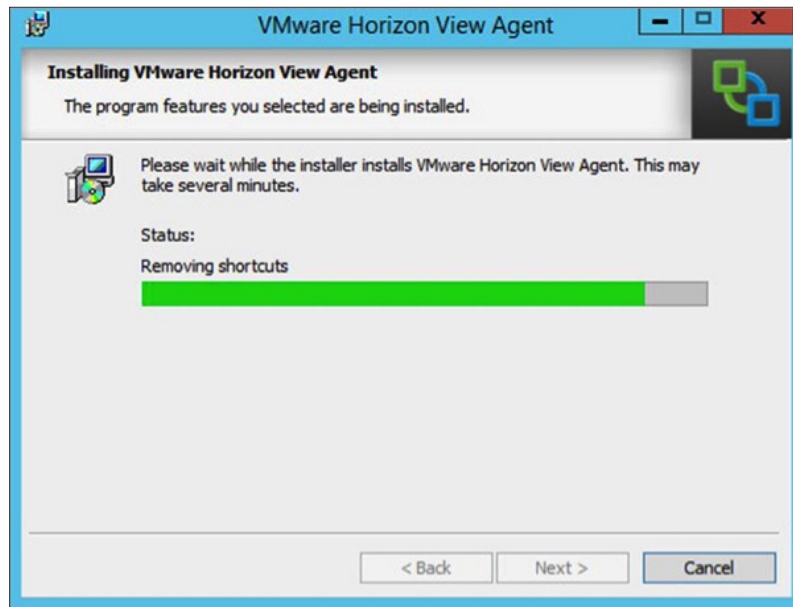
6. To install the View Agent, click **Install**.



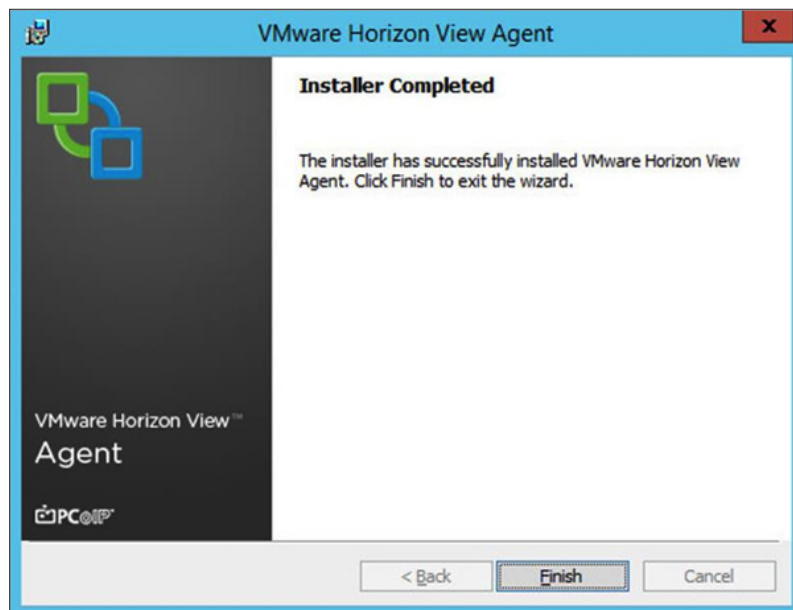
The screenshot shows the 'Ready to Install the Program' dialog box. The title bar reads 'VMware Horizon View Agent'. The main heading is 'Ready to Install the Program' with a sub-instruction: 'The wizard is ready to begin installation.' Below this, the text states: 'VMware Horizon View Agent will be installed in: C:\Program Files\VMware\VMware View\Agent\'. A final instruction says: 'Click Install to begin the installation or Cancel to exit the wizard.'

At the bottom, there are three buttons: '< Back', 'Install', and 'Cancel'.

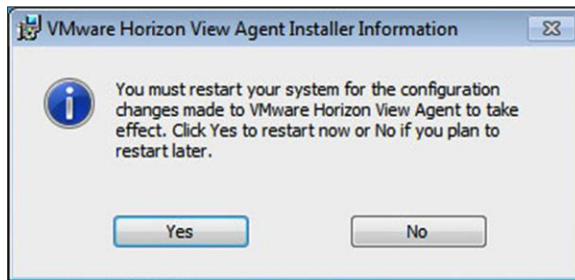
7. Monitor your installation status as it progresses.



8. In the Installer Completed window, click **Finish**.



9. To complete the installation, click **Yes** to initiate the restart of the operating system.

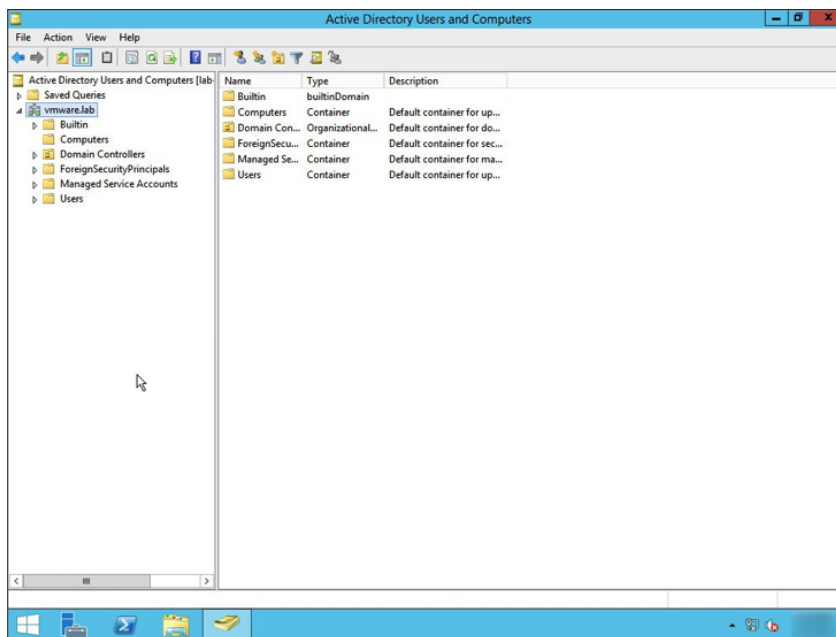


You have now completed installing the RDSH server. The next series of exercises walks you through configuring Group Policy Settings for user access to Remote Desktop Session Host services.

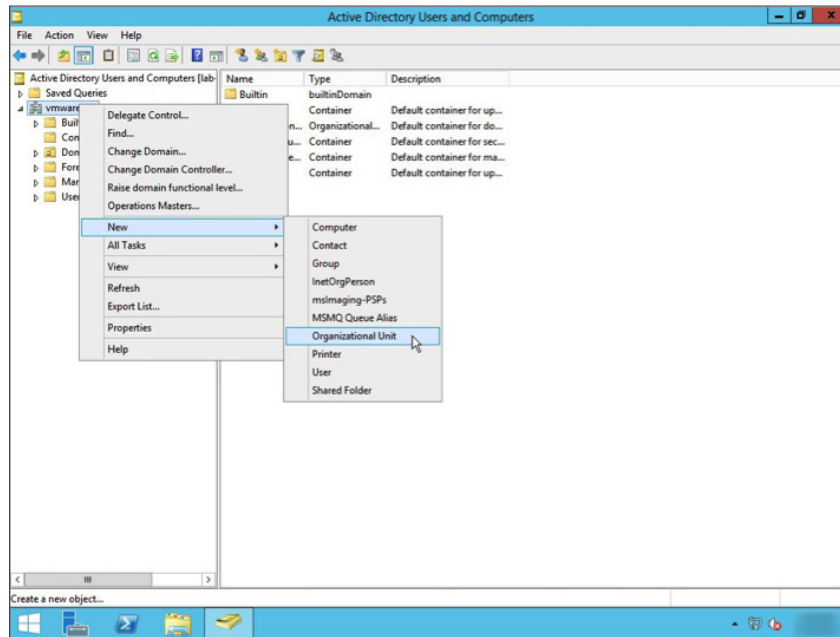
Configure Group Policy Settings for RDSH

After you have deployed and configured your Remote Desktop Session Host, you must configure user security and access settings for Remote Desktop Session Host services. Define these settings as a Group Policy Object.

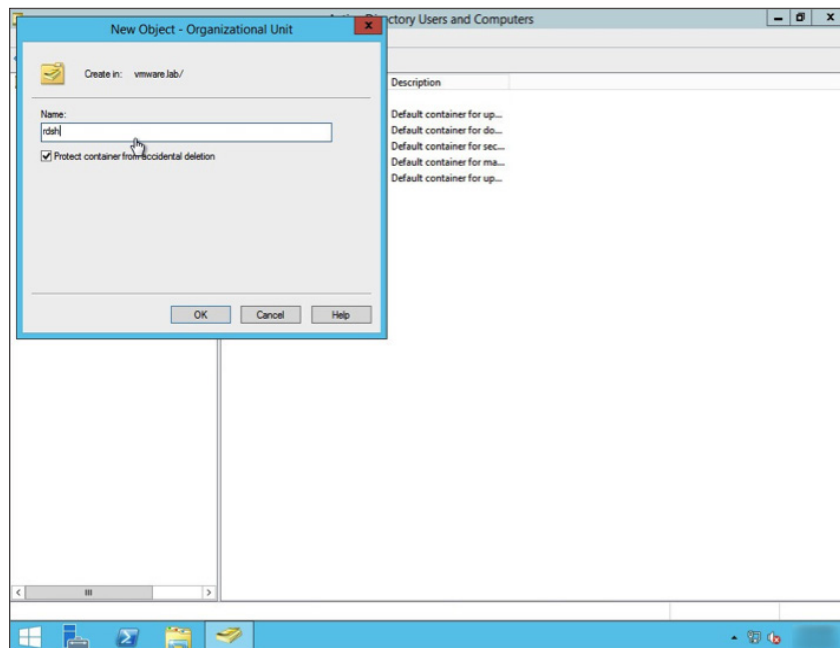
1. Create an Organizational Unit (OU) for the RD Session Hosts:
 - a. Log in as the administrator to your Active Directory Domain Controller.
 - b. Launch Active Directory Users and Computers and highlight the domain.



- Right-click your target domain and go to **New > Organizational Unit**.



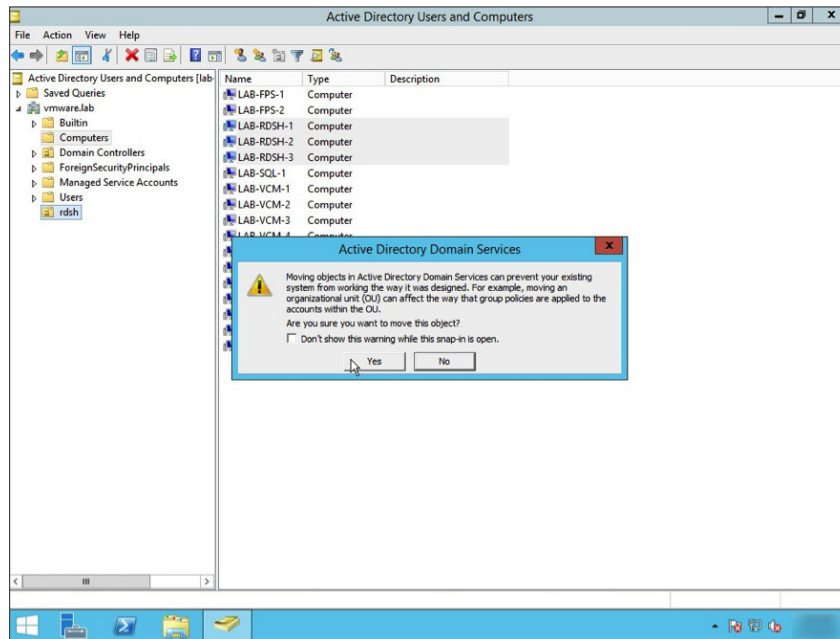
- Enter a name for your Organizational Unit, and click **OK**.



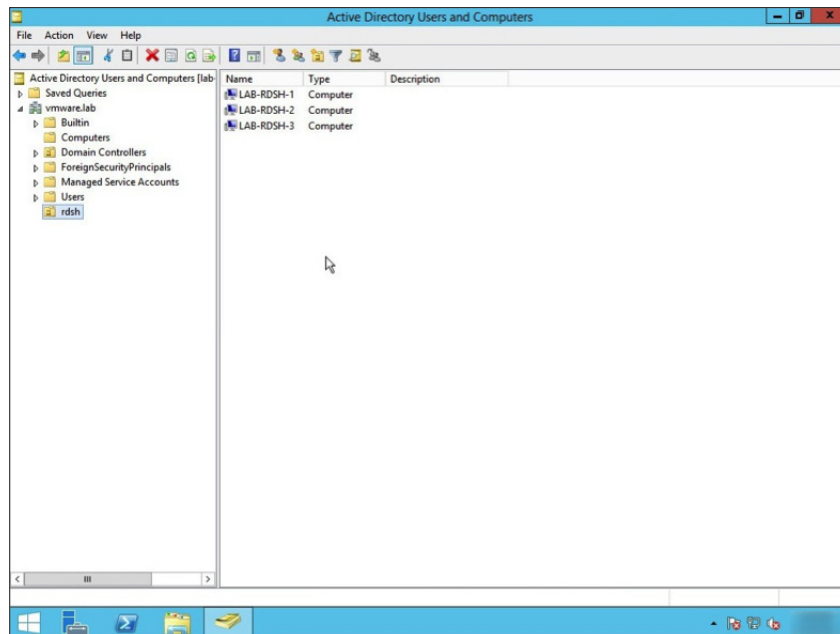
Under your domain, you see that the OU Group has been created.

- Click the **Computers** folder for your domain, highlight the computer names for your RD Session Hosts, and drag and drop them to your new OU Group.

5. In the warning message dialog box, click **Yes**.

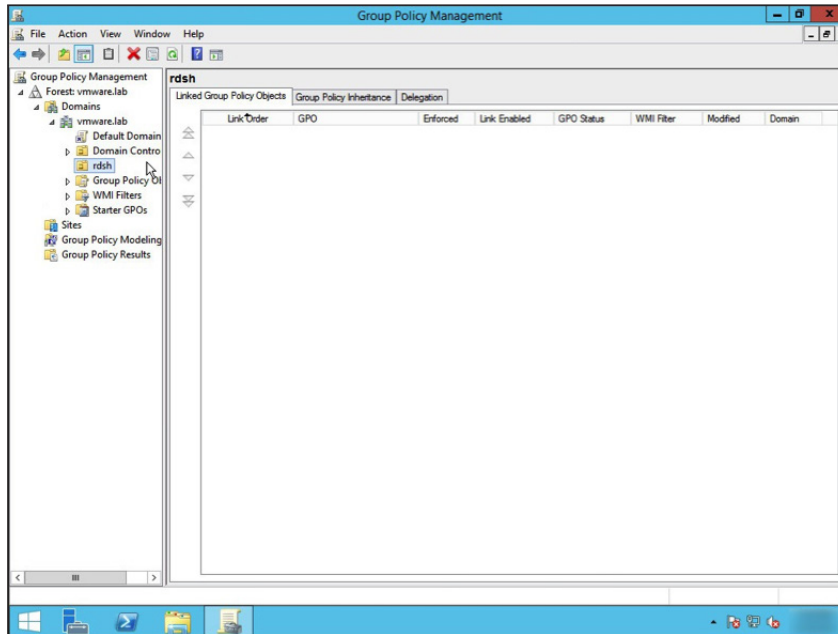


6. Click the Organizational Unit (OU) Group that you created to verify that all your Remote Desktop Session Hosts are now part of the OU Group.

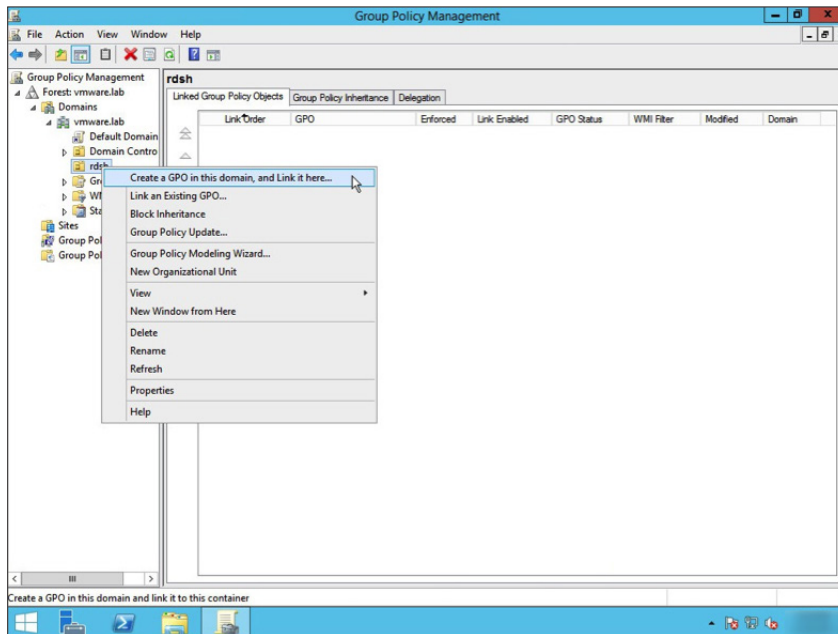


7. Launch the Group Policy Management utility.

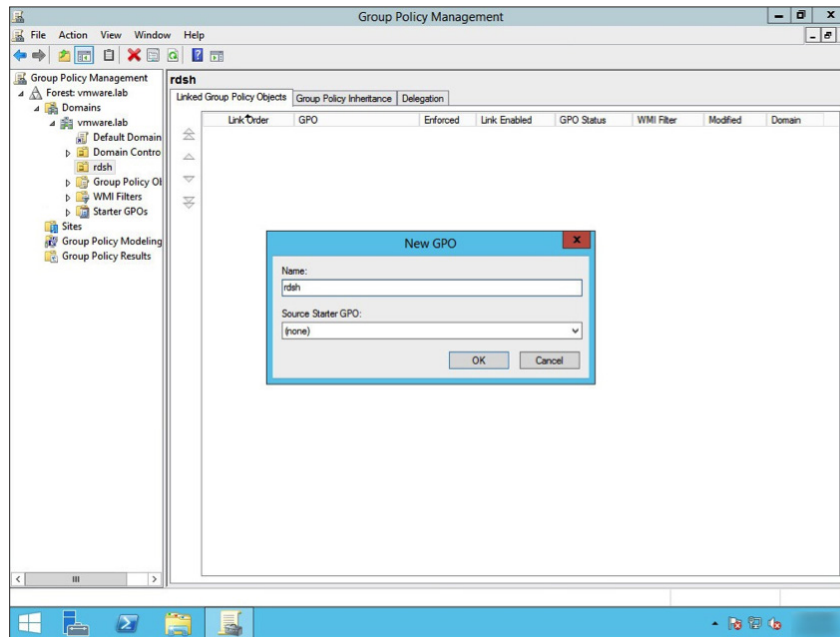
8. Expand the tree hierarchy for your domain and highlight the RDSH Organizational Unit (OU) Group that you created in the previous steps.



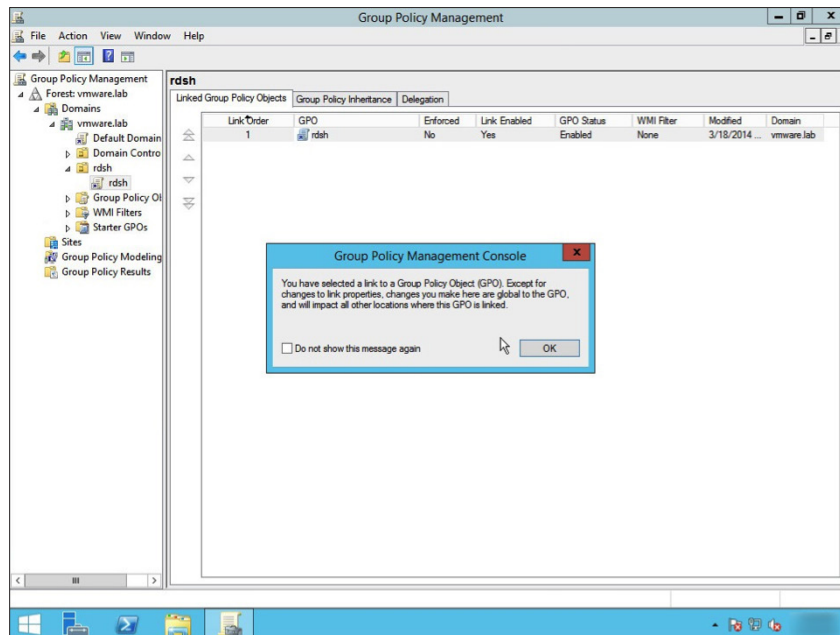
9. Right-click the OU Group and select **Create a GPO in this domain, and Link it here.**



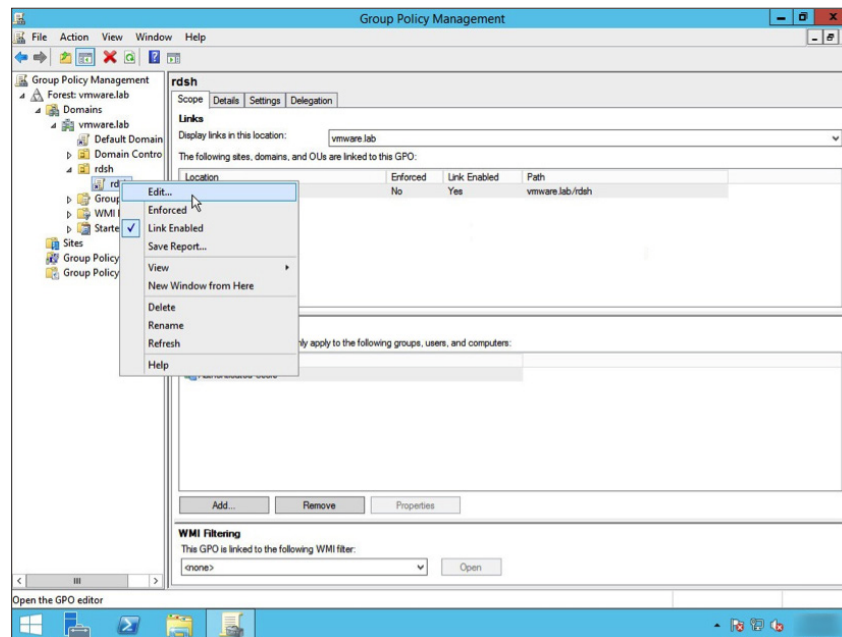
10. Enter a **Name** for the new GPO and click **OK**.



11. In the Group Policy Management Console warning dialog box (about GPO links), click **OK**.



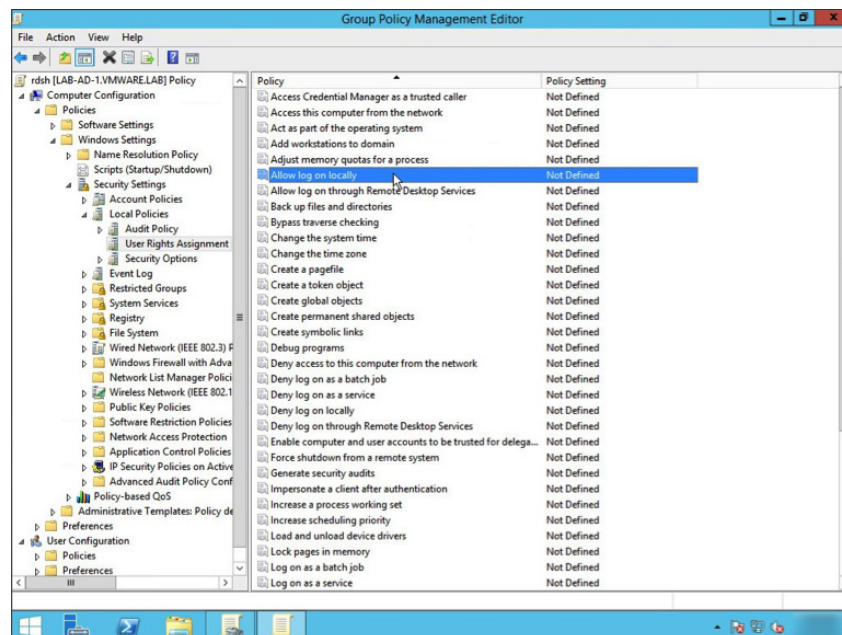
12. Right-click your Group Policy Object, and click **Edit**.



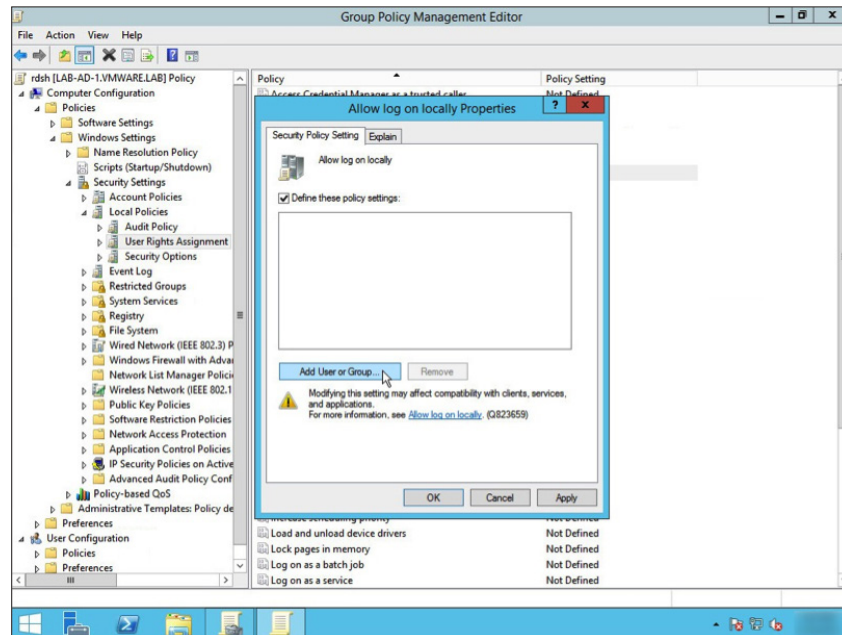
You are now in the Group Policy Management Editor for your Remote Desktop Session Host policy.

13. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.

14. Click **Allow log on locally**.

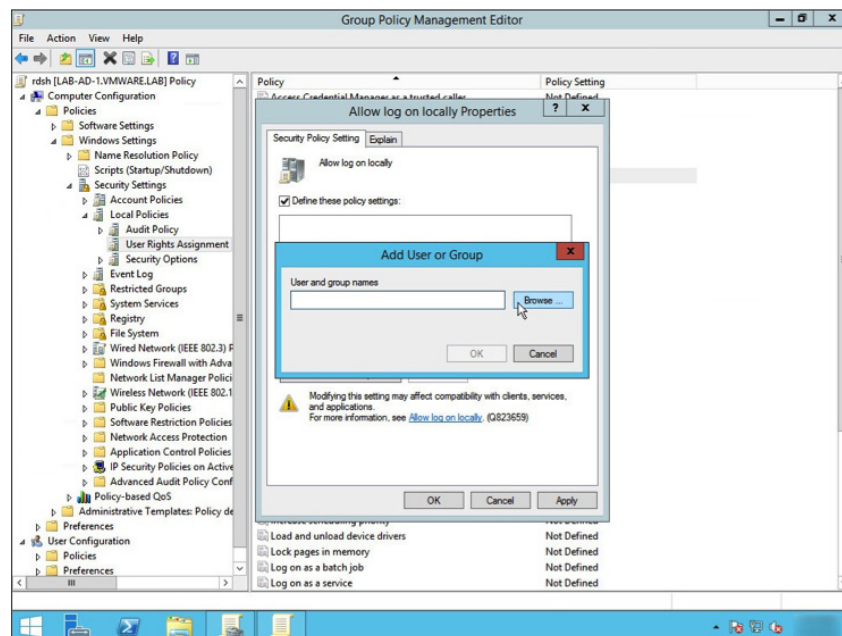


15. In the Allow Log On Locally Properties dialog box, ensure that the check box for **Define these policy settings** is selected, and click **Add User or Group**.

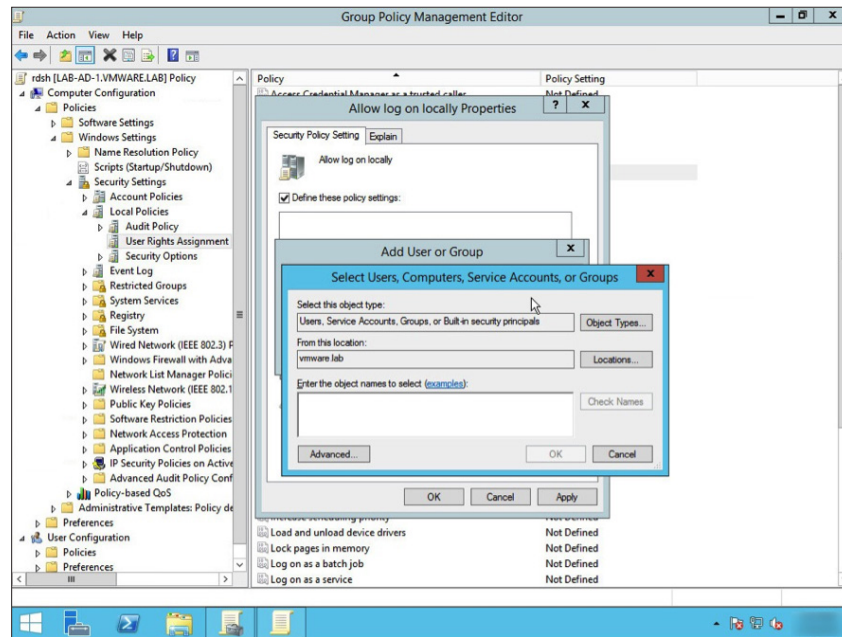


You now define which users or groups you will give access to allow local login.

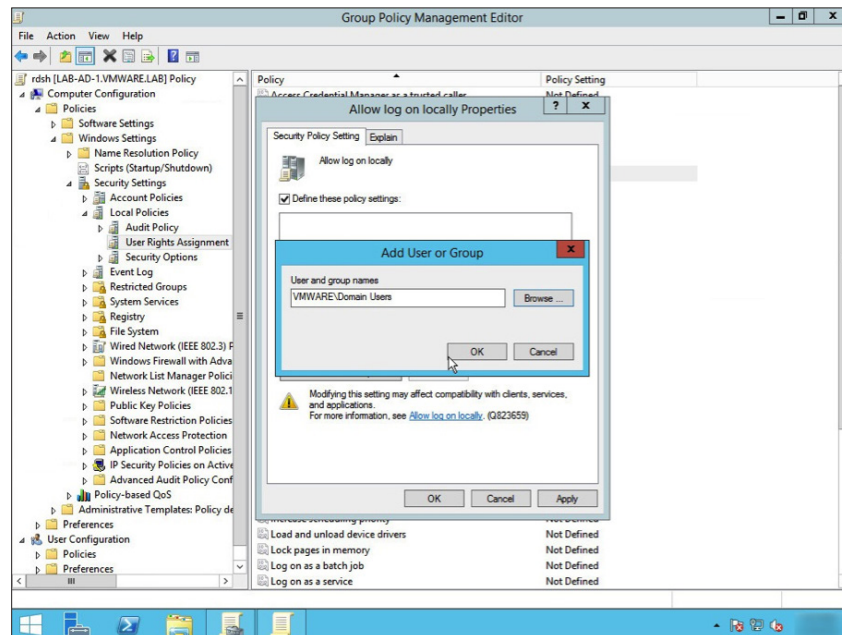
16. In the Add User or Group dialog box, click **Browse**.



17. In the Select Users, Computers, Service Accounts, or Groups dialog box:
 - a. In the **Enter the object names to select** field, enter the names of the user or groups for which you will allow access.
 - b. Click **OK**.

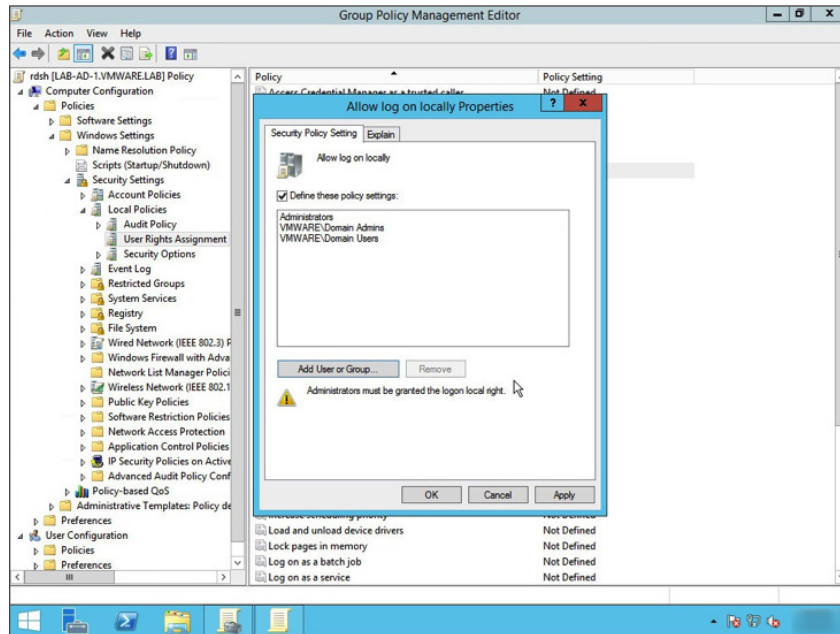


18. In the Add User or Group dialog box, verify that you are adding the correct users or groups, and click **OK**.

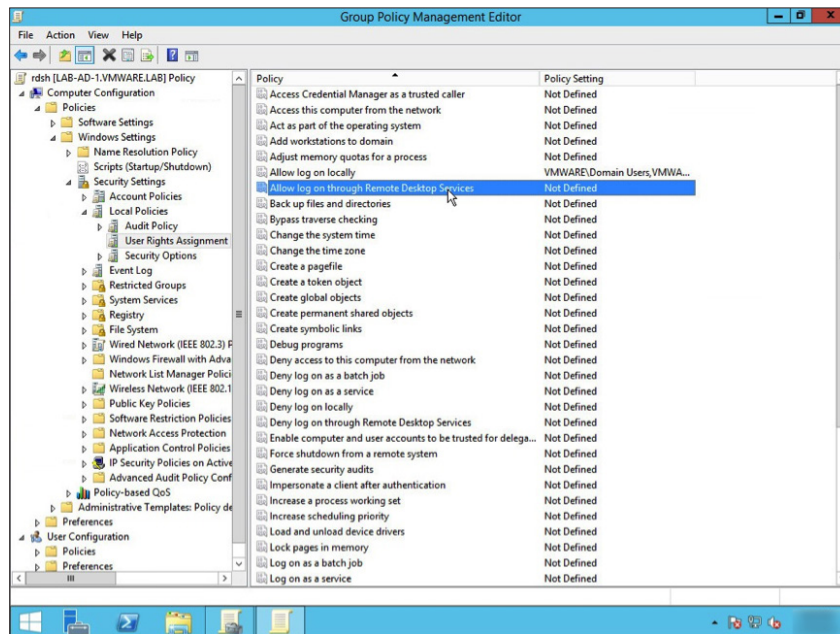


19. Verify that you have added all the users or groups you wish to authorize and click **OK**.

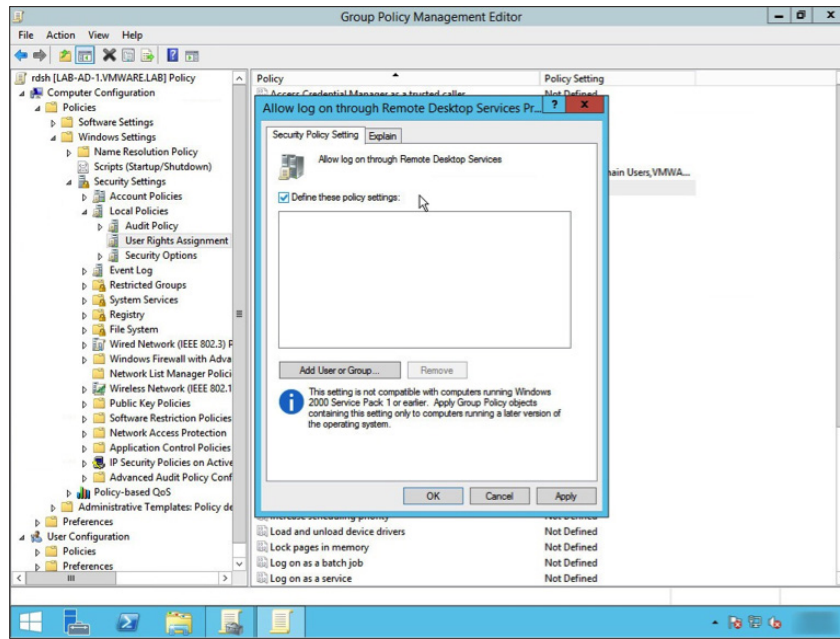
If you need to add additional users or groups, click **Add User or Group** to repeat the previous steps and make the necessary changes.



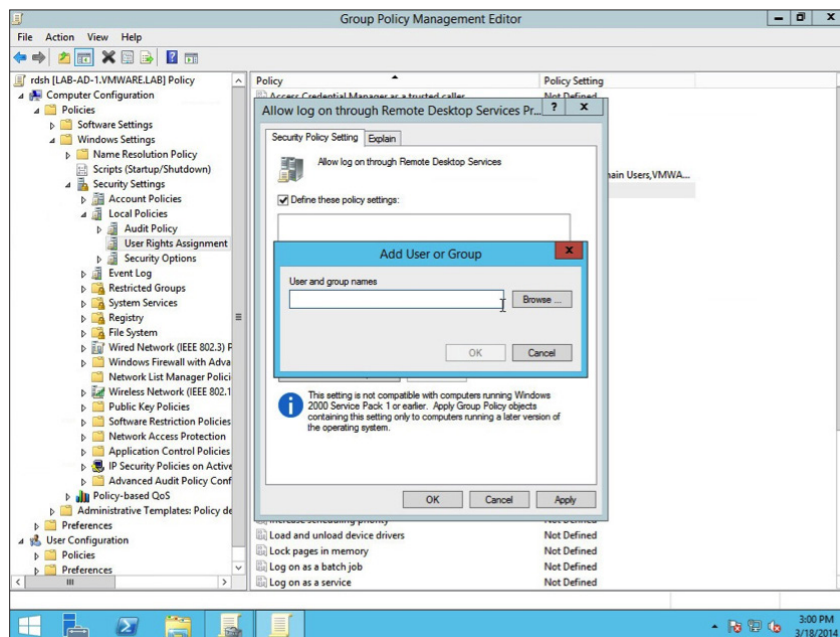
20. In the Group Policy Management Editor, click the policy **Allow log on through Remote Desktop Services**.



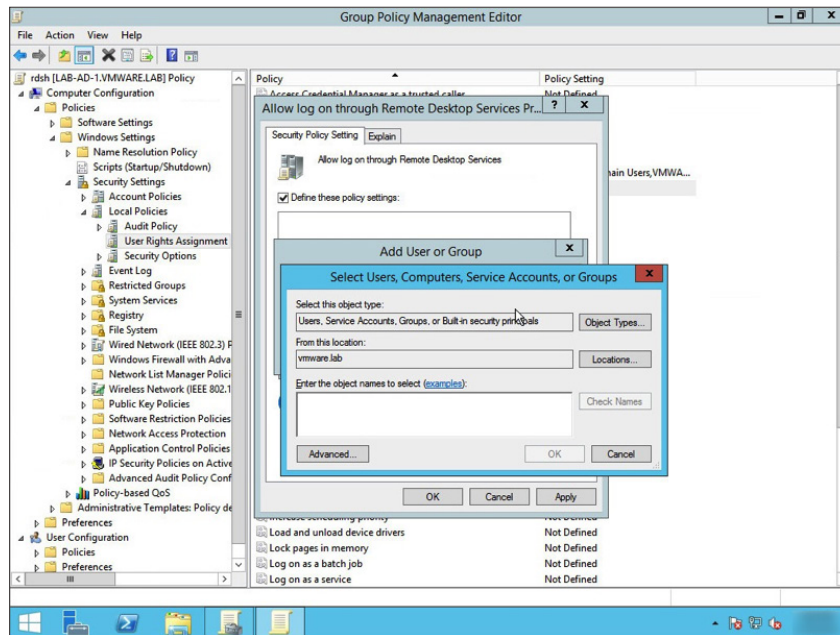
21. In the Allow Log On Through Remote Desktop Services Properties dialog box:
 - a. Ensure the check box for **Define these policy settings** is selected.
 - b. Click **Add User or Group**.



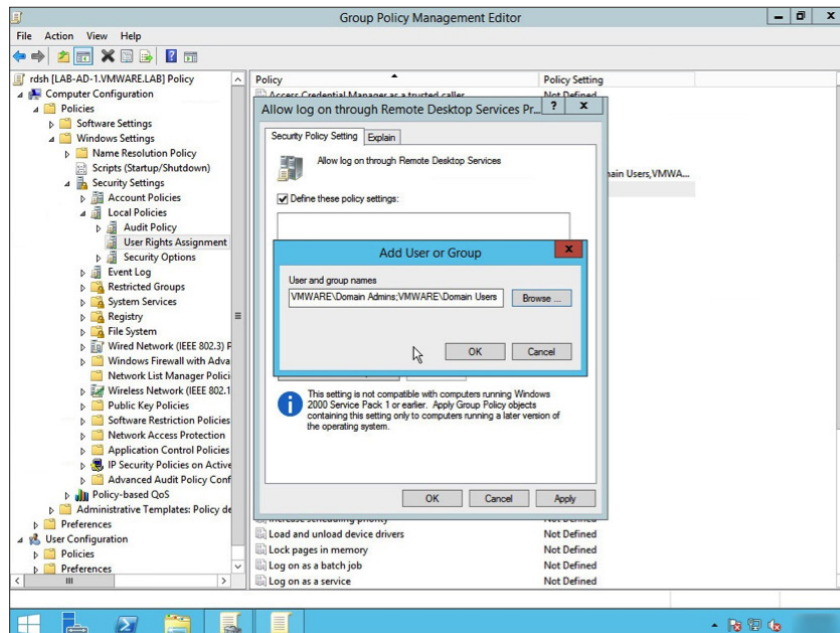
22. In the Add User or Group dialog box:
 - a. Define the users or groups to allow for this policy.
 - b. Click **Browse**.



23. In the Select Users, Computers, Service Accounts, or Groups dialog box:
- In the **Enter the object names to select** field, enter the names of the user or groups for which you will allow access.
 - Click **OK**.

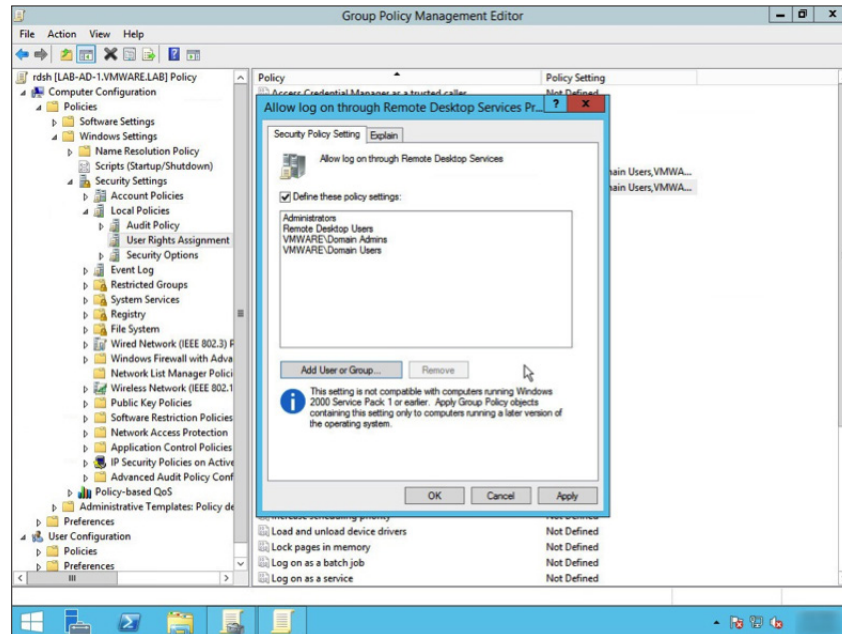


24. Verify that you are adding the correct users or groups, and click **OK**.



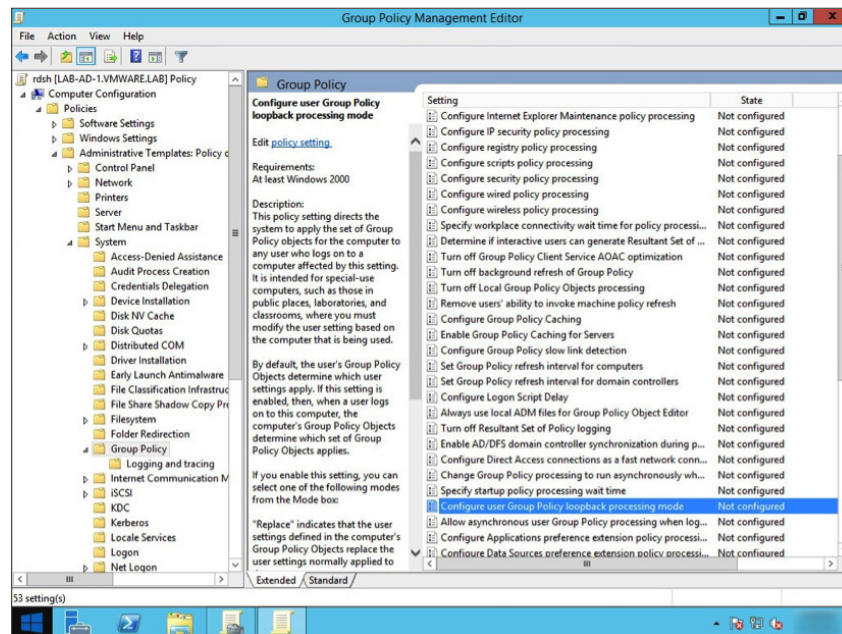
25. Verify that you have added all the users or groups you wish to authorize, and click **OK**.

If you need to add additional users or groups, click **Add User or Group** to repeat the previous steps and make the necessary changes.



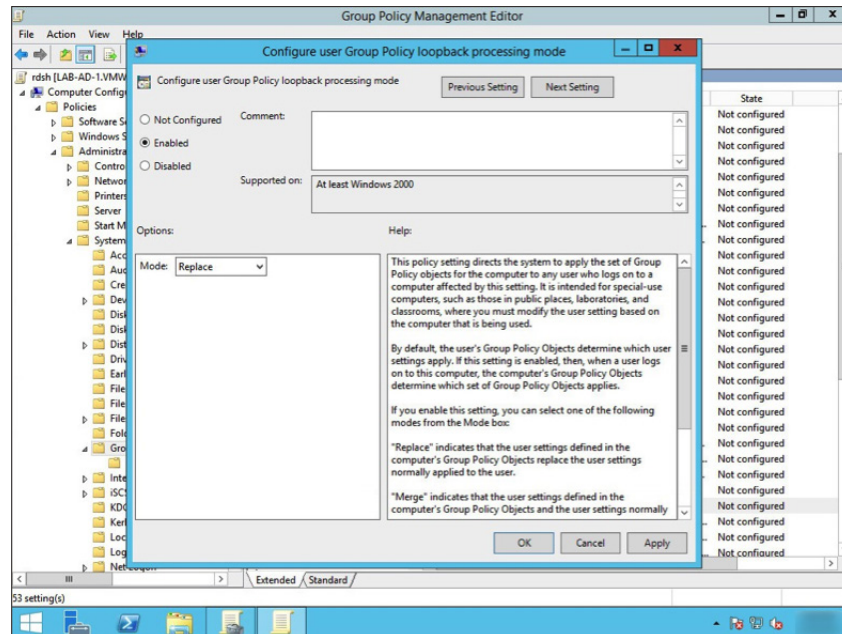
26. In the Group Policy Management Editor:

- Navigate to **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > System > Group Policy**.
- Click the policy **Configure user Group Policy loopback processing mode**.

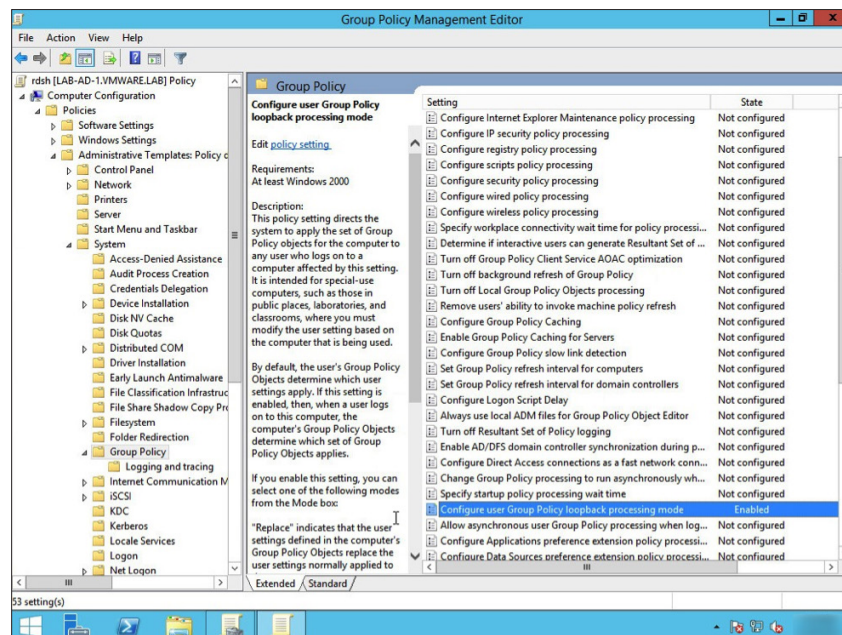


27. In the Configure User Group Policy Loopback Processing Mode dialog box:

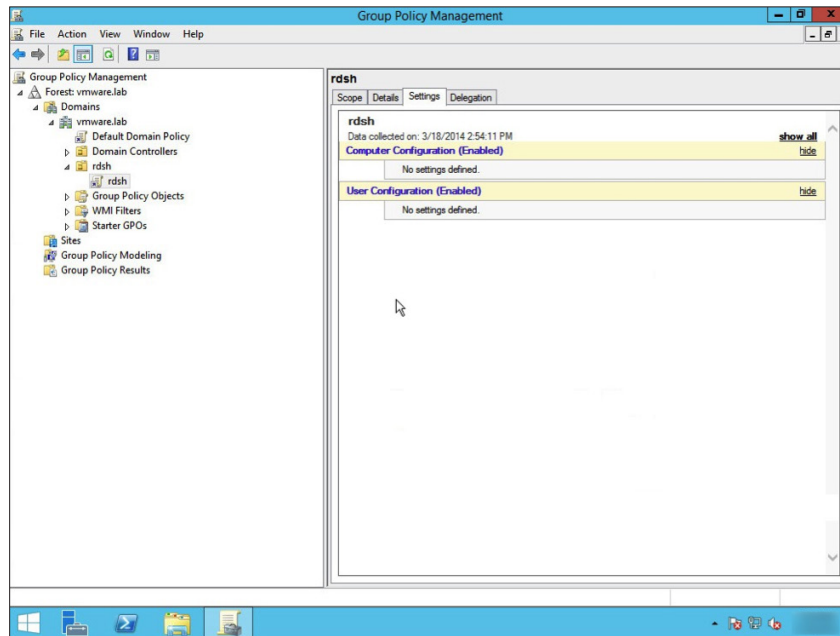
- Select **Enabled** to enable this policy.
- Click **OK**.



28. In the Group Policy Management Editor, verify that your policy is enabled by ensuring that the value in the State column for the policy has changed to Enabled.



29. Close the window for the Group Policy Management Editor to return to the Group Policy Management window.



You have successfully configured the Group Policy Settings for user access to Remote Desktop Session Host services.

Configuring View

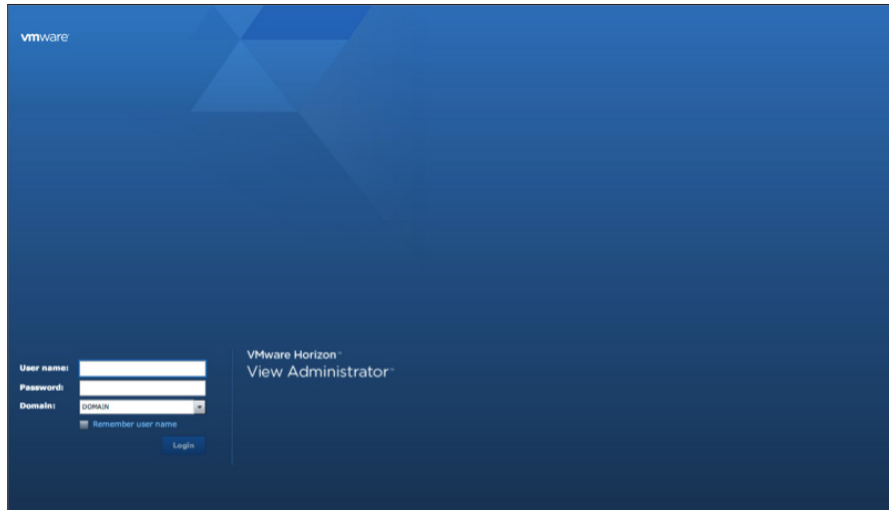
After you have installed the View component servers and set up RDSH, you are ready to configure View. This section contains the following exercises:

- [Add a License](#)
- [Connect vCenter Server Appliance and Configure the View Composer Settings](#)
- [Configure Persona Management Administrative Templates in Active Directory](#)
- [Adjust PCoIP Settings for PCoIP Tuning](#)
- [Configure Syslog Event Logging](#)
- [Enable Windows Server 2008 R2 SP1](#)
- [Create a Farm for Remote Desktop Session Hosts](#)

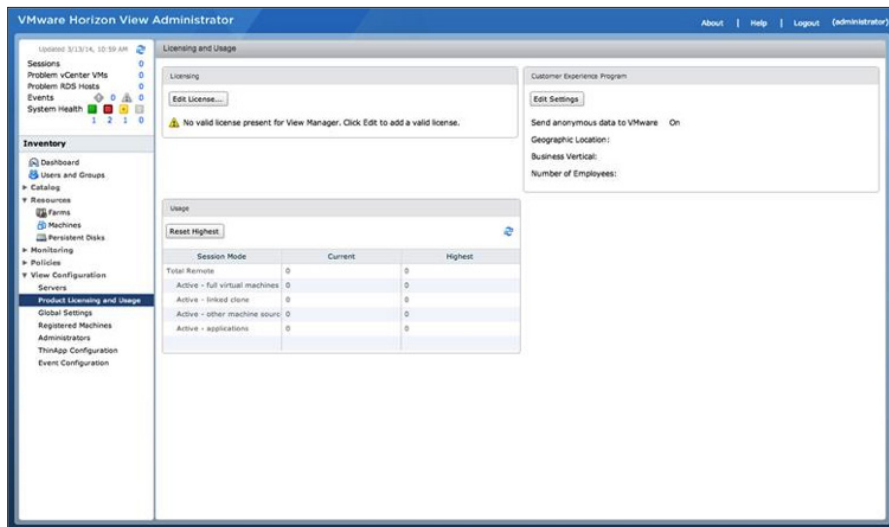
Add a License

You must have a valid license to use View.

1. Log in to the View Administrator console as an administrator.



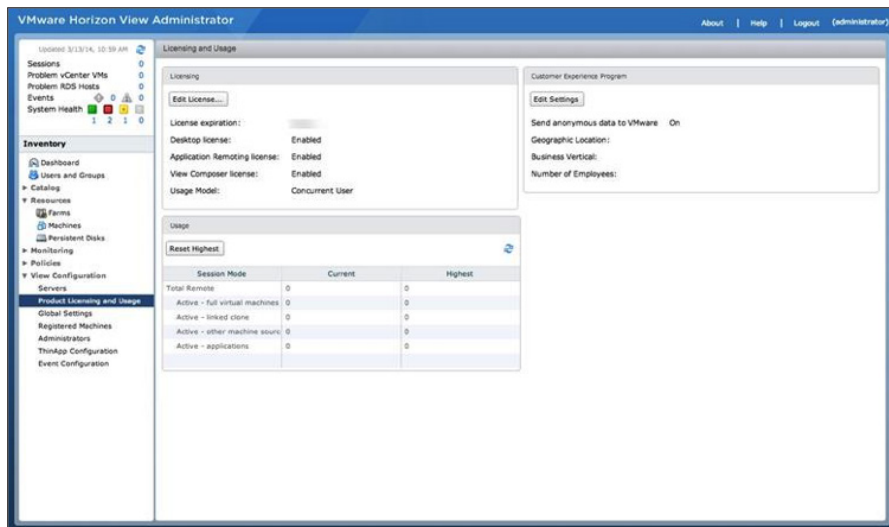
2. In the View Administrator window:
 - a. In the left pane, under View Configuration, click **Product Licensing and Usage**.
 - b. In the Licensing panel, click **Edit License**.



3. Enter a valid License serial number, and click **OK**.



4. In the Licensing section, verify your license information.

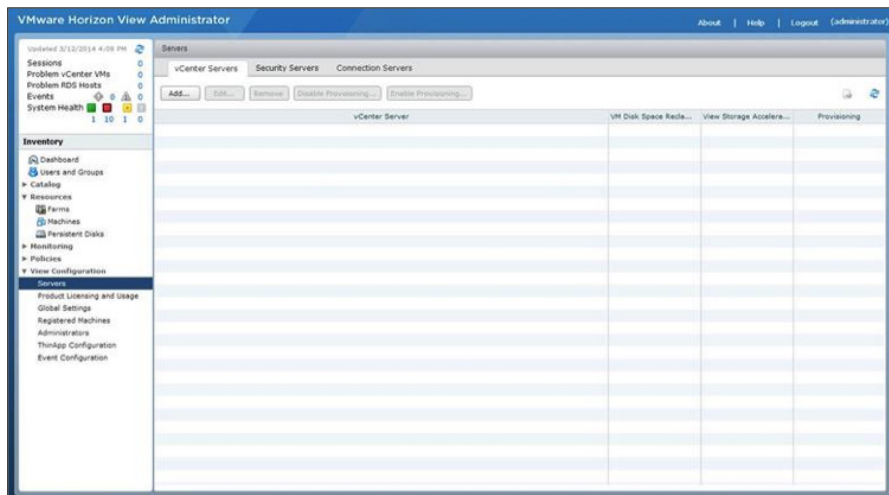


Now that you have a valid license, you can connect the vCenter Server Appliance and configure the View Composer Server settings.

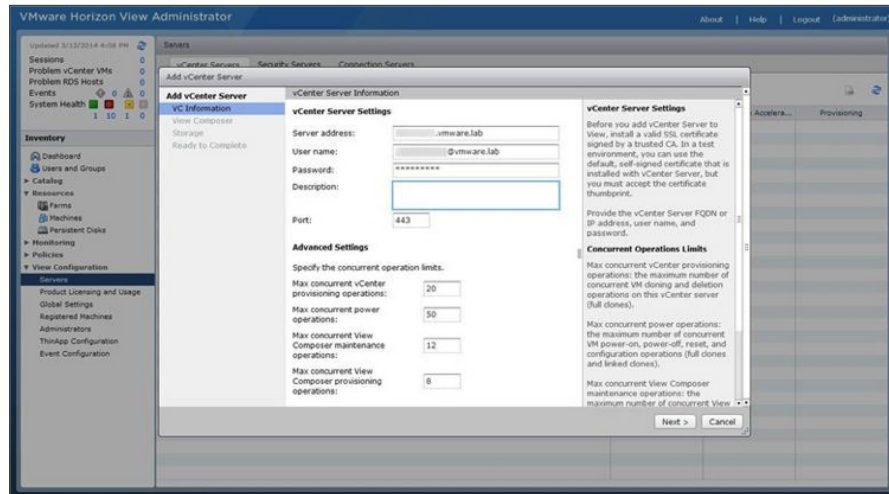
Connect vCenter Server Appliance and Configure the View Composer Settings

Follow these steps:

1. From the Inventory panel on the left of View Administrator, select **View Configuration > Servers**.
2. On the vCenter Servers tab in the main Servers panel, click **Add**.

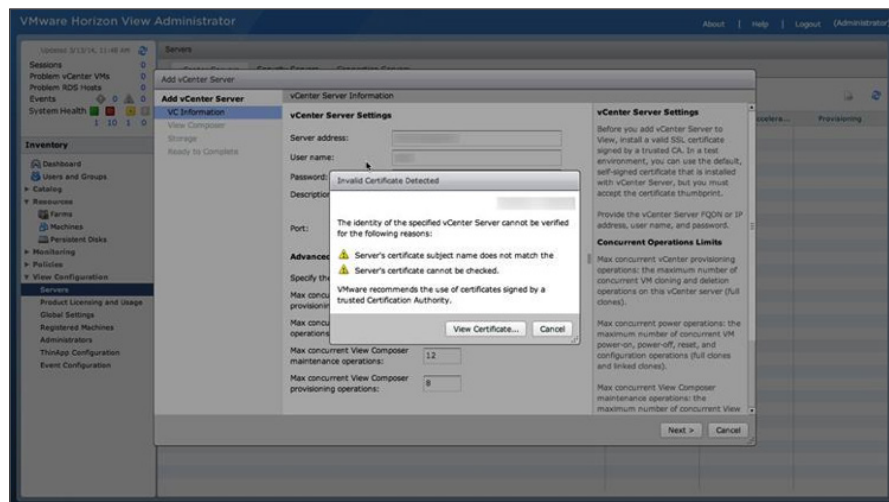


3. In the Add vCenter Server dialog box:
 - a. In the **Server address** field, enter the fully qualified domain name or IP address of your vCenter Server.
 - b. Accept or modify the default values for the other settings, and click **Next**.

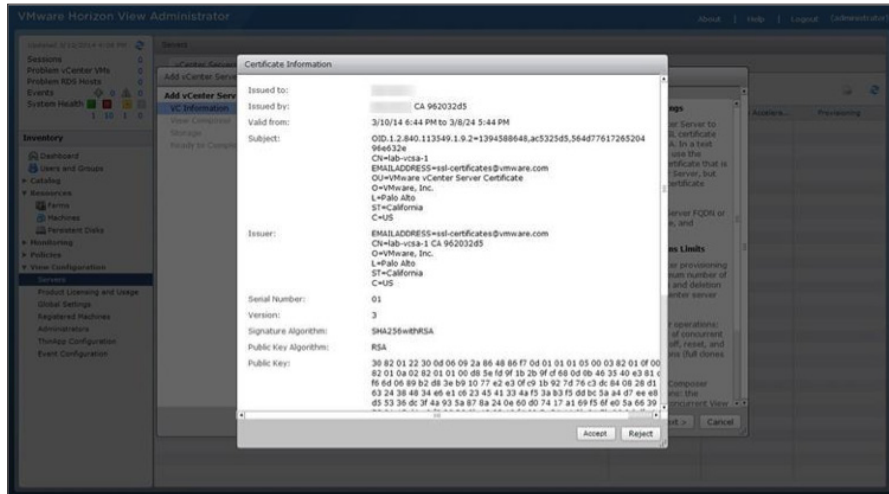


4. In the Invalid Certificate Detected dialog box, click **View Certificate** to see the vCenter Server SSL certificate.

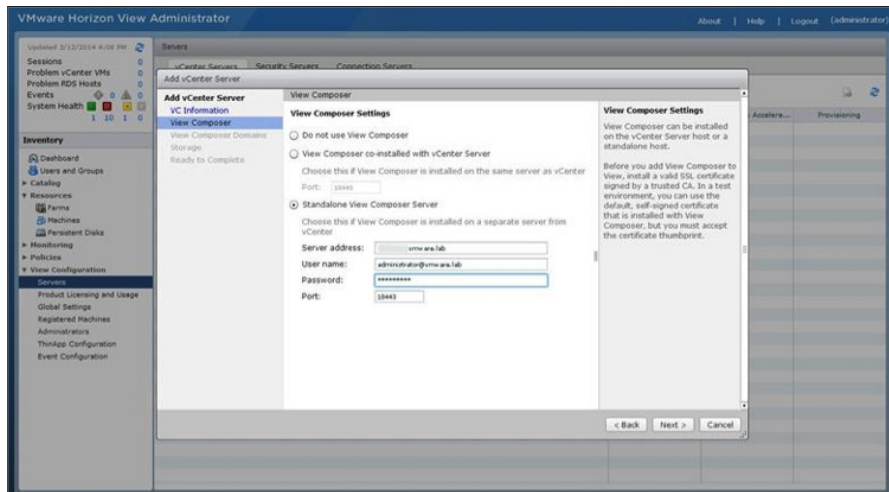
In an evaluation environment, you can use a default self-signed certificate, but for a production environment, it is recommended that you replace the self-signed certificate with an approved certificate from a Certificate Authority.



5. In the Certificate Information dialog box:
 - a. Verify the self-signed certificate generated by the default installation of the vCenter Server Appliance.
 - b. Click **Accept** to approve.



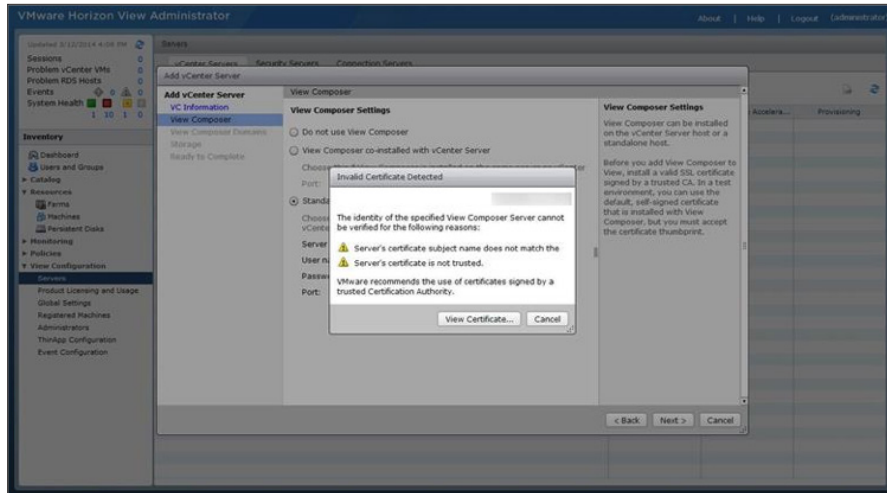
6. In the Add vCenter Server dialog box, configure the View Composer Settings:
 - a. Select **Standalone View Composer Server**.
 - b. Enter the required **Server address**, either the FQDN or IP address, of your View Composer Server virtual machine.
 - c. Enter the **User name** and **Password** of the server.
 - d. Modify the **Port** value only if you modified it during the View Composer Server installation. Otherwise, use the default.



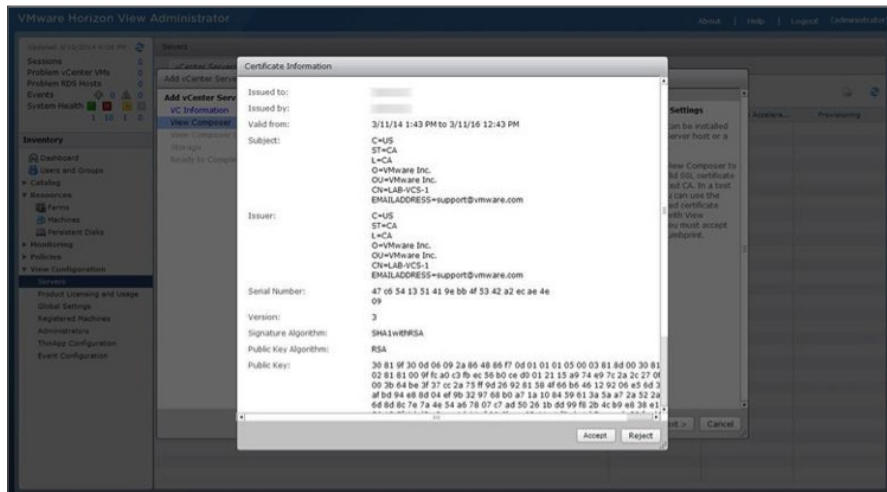
7. Click **Next**.

8. In the Invalid Certificate Detected dialog box, click **View Certificate** to see the View Composer SSL certificate.

In an evaluation environment, you can use a default self-signed certificate. In a production environment, it is recommended that you replace the self-signed certificate with an approved certificate from a Certificate Authority.

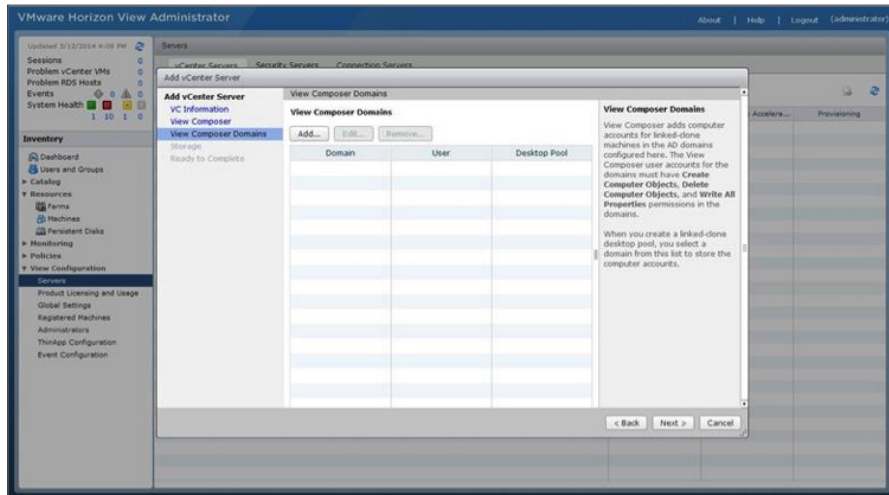


9. In the Certificate Information dialog box, verify the self-signed certificate generated by the default installation of the View Composer Server, and click **Accept** to approve.



10. In the Add vCenter Server dialog box:

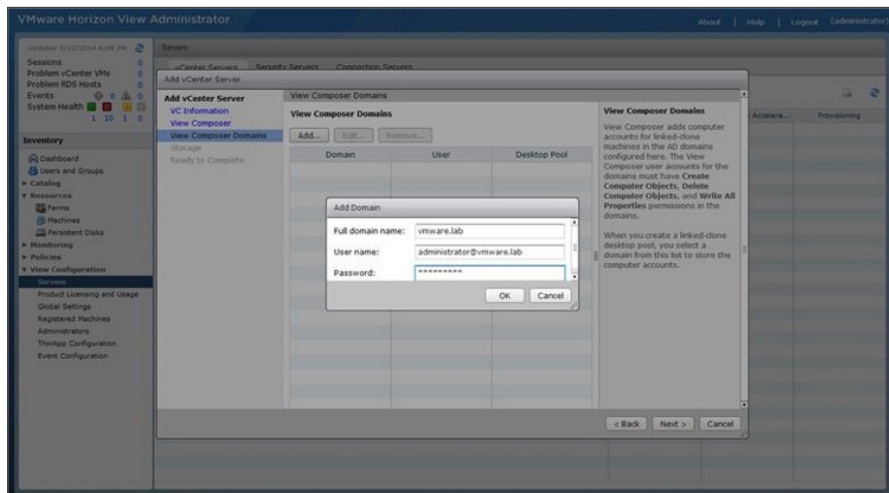
- Select **View Composer Domains**.
- Click **Add**.



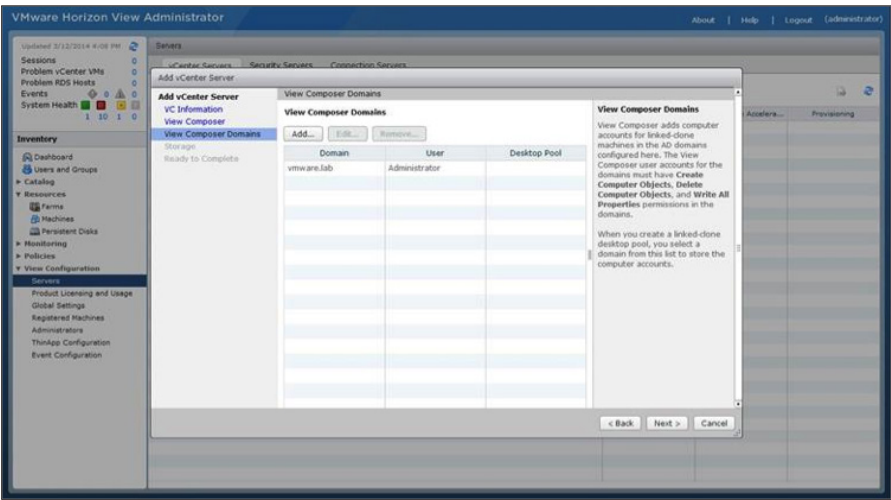
11. In the Add Domain dialog box:

- Enter the **Full domain name**, **User name**, and **Password**.
- Click **OK**.

The user name and password are the credentials for your domain. This account must have permission to create computer objects, delete computer objects, and write properties in the domain.

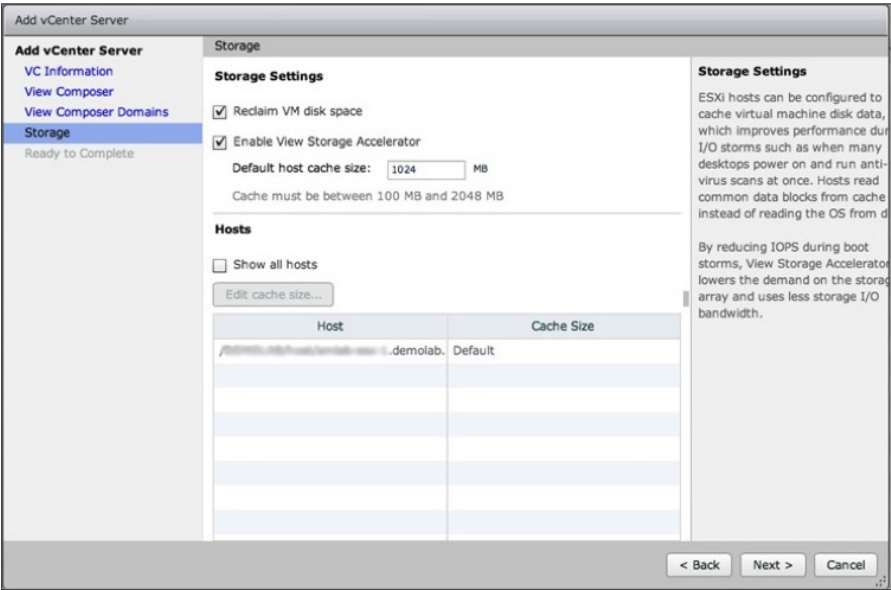


12. Review the information, and click **Next**.



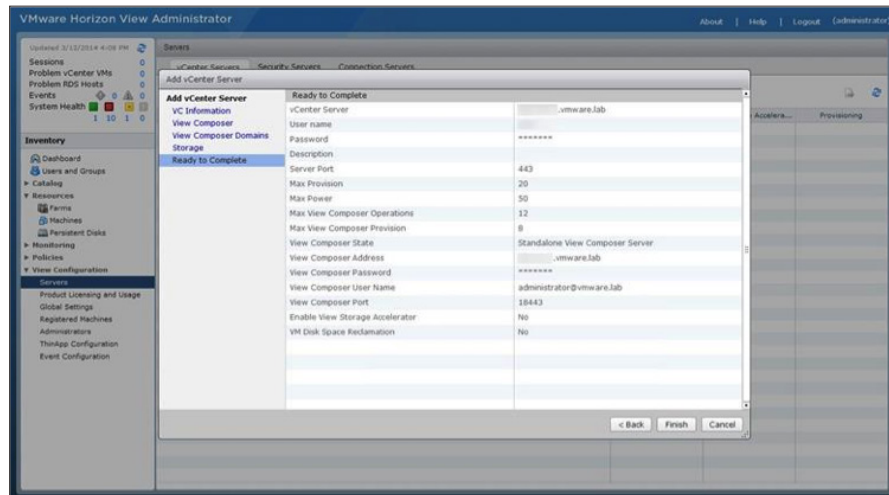
13. Configure the storage options for your vCenter Server, and click **Next**.

If you enabled View Storage Accelerator, enter the host cache size. The default is 1024 MB. You can use any valid value.



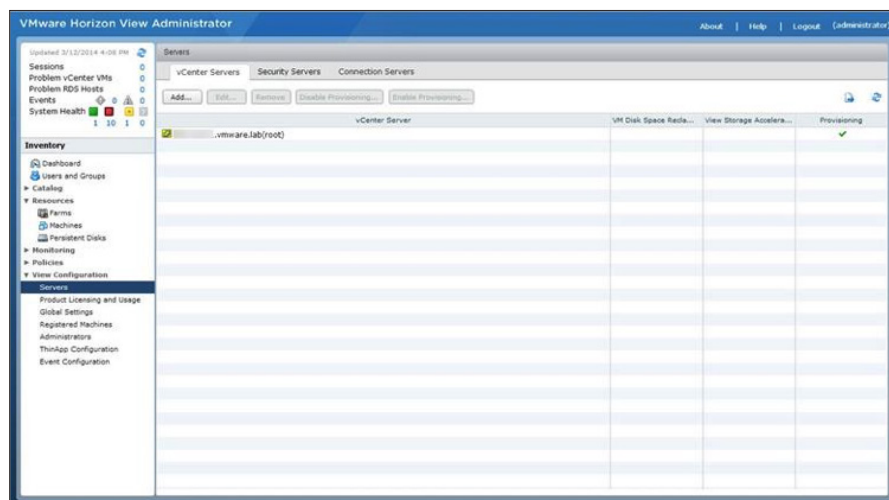
14. Review the vCenter Server information, and click **Finish** to accept these values and to add the vCenter Server to your View environment.

To modify any settings, click **Back**.



15. In the vCenter Servers tab, view the vCenter Server added to your View environment.

To make changes to the connection information or settings, select a vCenter Server and click **Edit**.



You have now connected to the vCenter Server Appliance and configured View Composer Server.

Configure Persona Management Administrative Templates in Active Directory

You can choose to skip this exercise and return to it after completing the rest of the exercises in this document.

It is recommended that you configure Persona Management Administrative Templates. They provide persistent, dynamic user profiles across user sessions on different desktops. User profile data is downloaded as needed to speed up login and logout time. New user settings are automatically sent to the user profile repository during desktop use.

For instructions on importing and tuning the Persona Administrative Template in Active Directory Group Policy, see the [VMware View Persona Management Guide](#).

Adjust PCoIP Settings for PCoIP Tuning

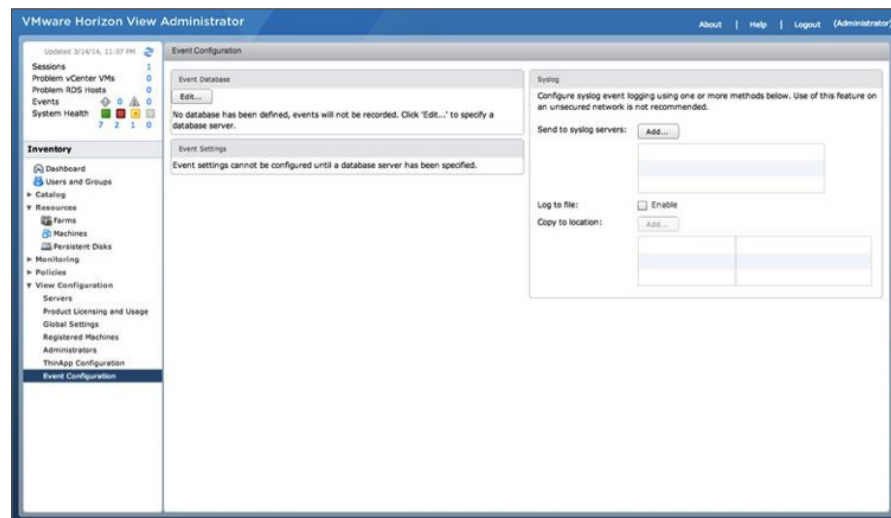
You can choose to skip this exercise and return to it after completing the rest of the exercises in this document.

It is recommended that you adjust the PCoIP settings to ensure the best user experience. For instructions on tuning PCoIP, see the blog post [Horizon 6 with PCoIP—Up to 30% Bandwidth Savings out of the Box!](#) and [VMware View with 5 PCoIP Network Optimization Guide](#).

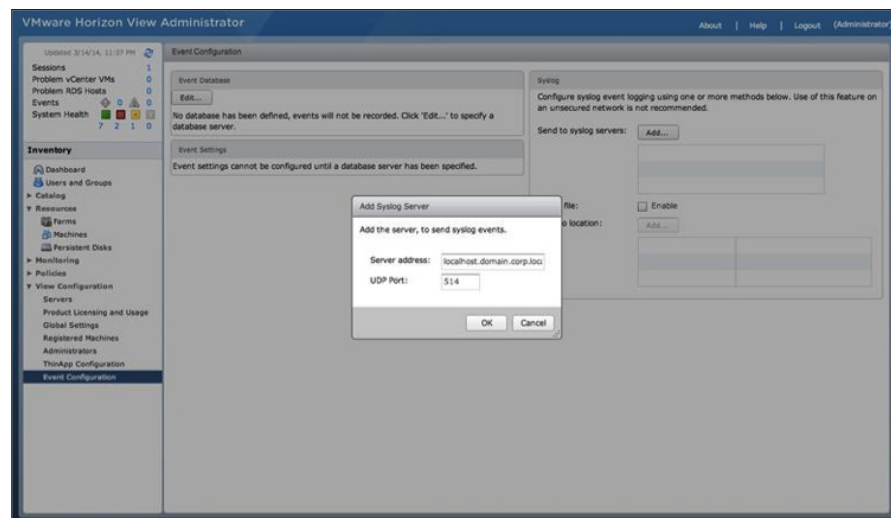
Configure Syslog Event Logging

You can use the Syslog feature to send View events to a Syslog server.

1. In the View Administrator console:
 - a. In the left pane, select **View Configuration > Event Configuration**.
 - b. In the Syslog panel, click **Add**.



2. In the Add Syslog Server dialog box, enter the Server address and UDP Port for your target Syslog server, and click **OK**.

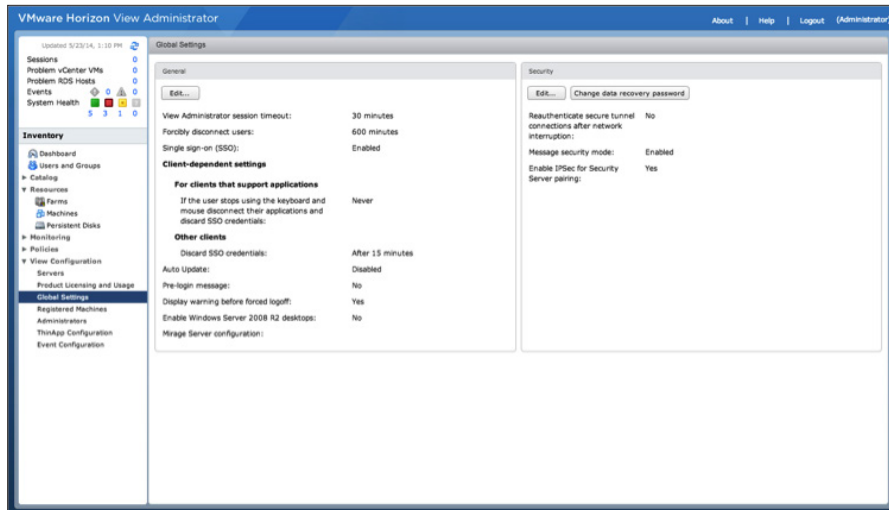


You have now set up Syslog collection for View events.

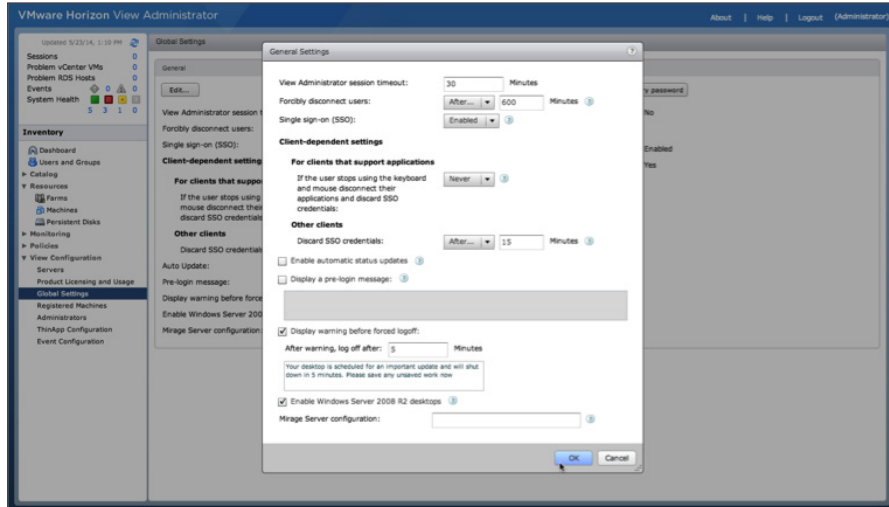
Enable Windows Server 2008 R2 SP1

You can enable Windows Server 2008 R2 with SP1 to use for desktop deployment on View Connection Server.

1. In the View Administrator console, from the left pane, select **View Configuration > Global Settings** and in the General pane, click **Edit**.



2. In the General Settings dialog box, select the check box **Enable Windows Server 2008 R2 desktops**, and click **OK**.

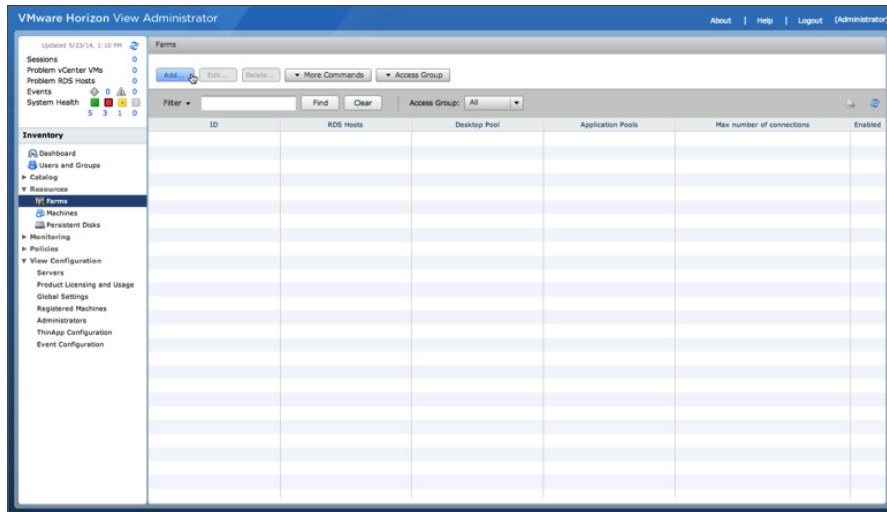


You have enabled Windows Server 2008 R2 SP1 View desktop support. You are now ready to create a farm for Remote Desktop Session Hosts.

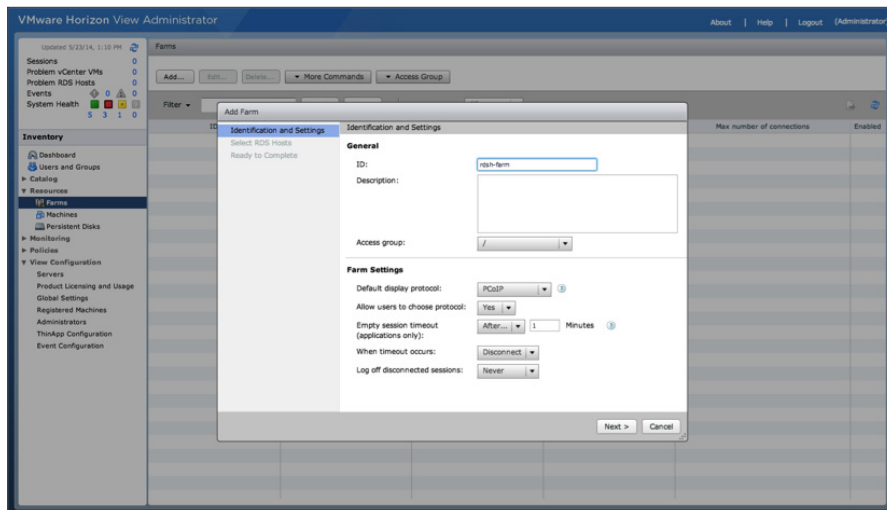
Create a Farm for Remote Desktop Session Hosts

Follow these steps:

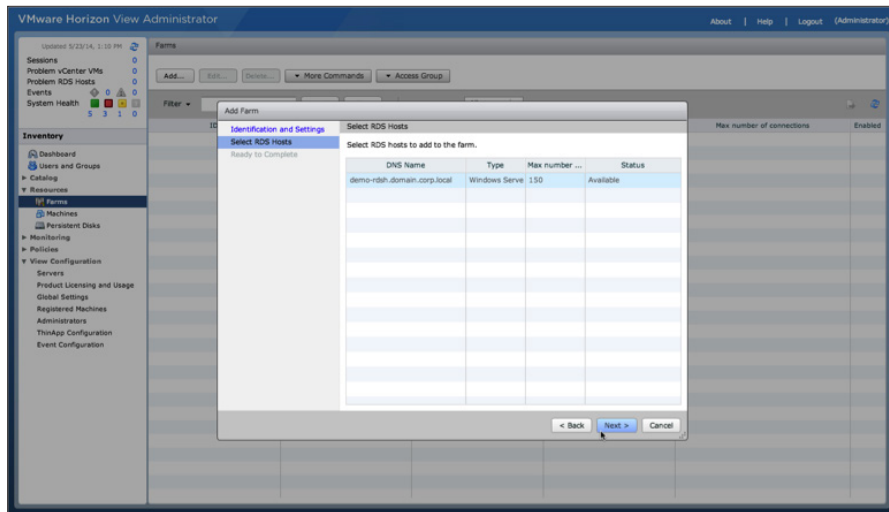
1. In the View Administrator console:
 - a. In the left pane, select **Resources > Farms**.
 - b. Click **Add** to start the Add Farm wizard.



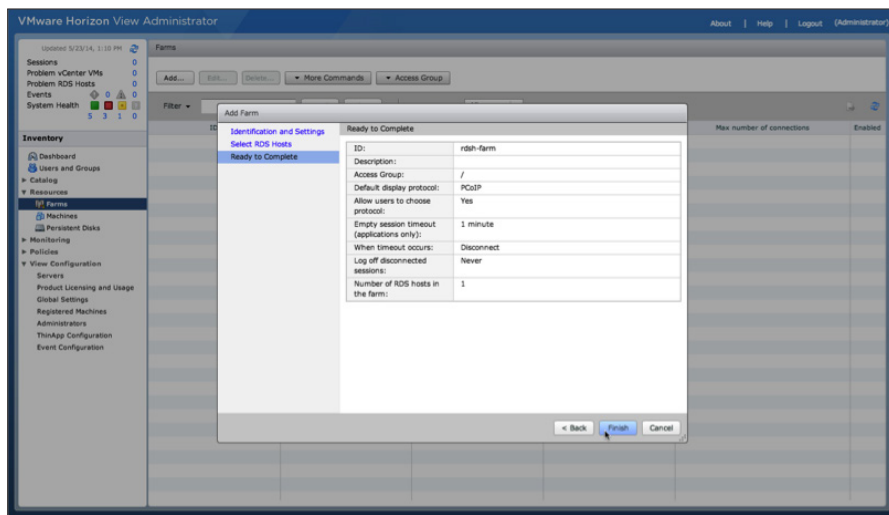
2. In the Add Farm wizard, enter a name for your farm in the **ID** text box.
3. For the other options, use the default settings or make changes, and click **Next**.



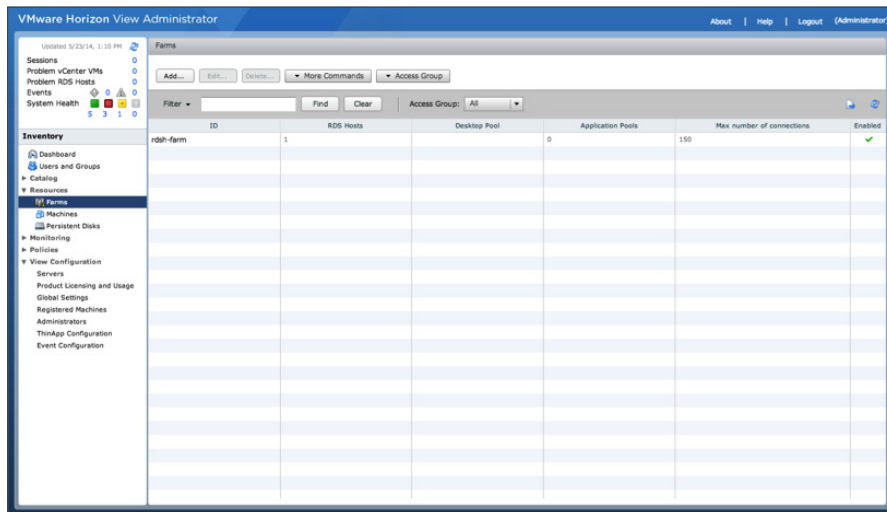
4. Select which RDS Hosts (RD Session Hosts) to add to your farm, and click **Next**.



5. Review the settings, and click **Finish** to set up your RDSH farm. If you want to make changes, click **Back**.



6. The Farms window appears, which now lists the new RDSH farm.



You are now ready to prepare and create a virtual machine for a linked-clone desktop pool.

Preparing Virtual Machines for Linked-Clone Desktop Pool Deployment

You can use virtual machines managed by vCenter Server

- To provision and deploy desktops as master images for automated full-clone pools
- As master images for linked-clone pools
- As desktop sources for manual pools

You must prepare virtual machines to deliver View desktop access.

See the [View Administration guide](#) for more information about preparing virtual machines for additional types of pool deployments.

In this series of exercises, you prepare a Windows 7 32-bit virtual machine to use to deploy remote desktops for stateless linked-clone deployment.

You install the required agents and optimize the virtual machine for linked-clone deployment in the following exercises:

- [Create the Master Image for Desktop Deployment](#)
- [Install View Agent](#)
- [Install the View Agent Direct-Connection Plug-In \(Optional\)](#)
- [Optimize the Virtual Machine for Desktop Deployment](#)
- [Install Custom Applications and Configure the Operating System \(Options\)](#)
- [Prepare the Virtual Machine for Linked-Clone Deployment](#)

Create the Master Image for Desktop Deployment

A master image is a virtual machine that has been created and configured for desktop deployment. Until you configure the virtual machine properly, it is not considered to be a master image. All of the procedures in the sections that follow will refer to a virtual machine until your master image has been created and is ready to be deployed.

Follow these steps:

1. Log in to your host from the vSphere Client, and create a new virtual machine using the following specifications for a nonproduction deployment as a guide.

TYPE	vCPU	RAM	VIRTUAL DISK SIZE
Knowledge worker	1 vCPU	2 GB RAM	24 GB
Power worker (with vSGA 3D graphics)	2 vCPUs	4 GB RAM	24 GB

Note: These desktop specifications are recommended for evaluating a nonproduction deployment. For a production environment, where desktop sizing varies based on the types of user workloads, see the [View Architecture Planning guide](#) for best practices on resource planning.

2. Install the Windows 7 32-bit guest operating system.
3. Activate your Windows operating system according to your organization's procedures.
4. After the installation is complete, log in to the virtual machine as a local administrator.

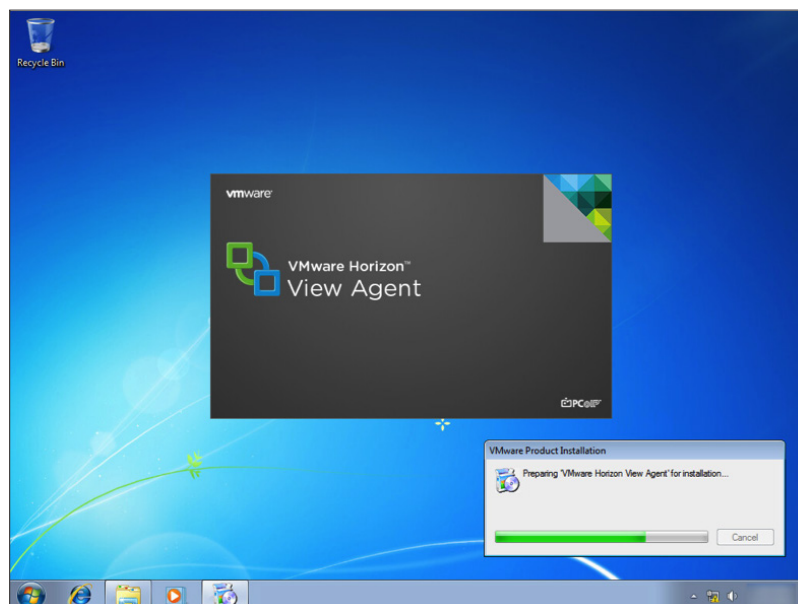
Proceed to the next exercise to install View Agent.

Install View Agent

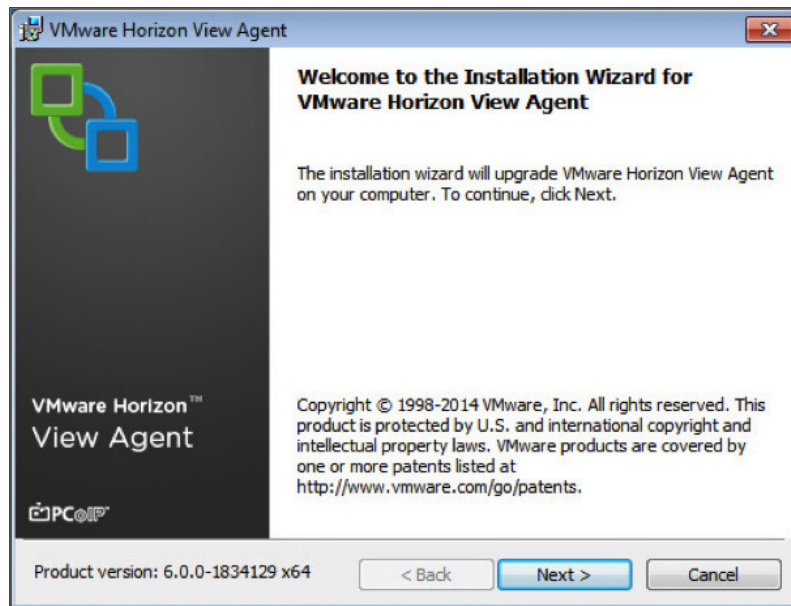
Installing View Agent also enables Persona Management on the virtual machine.

1. Launch the View Agent installer using the Run As Administrator option.
2. Ensure that the installer is accessible from this virtual machine.

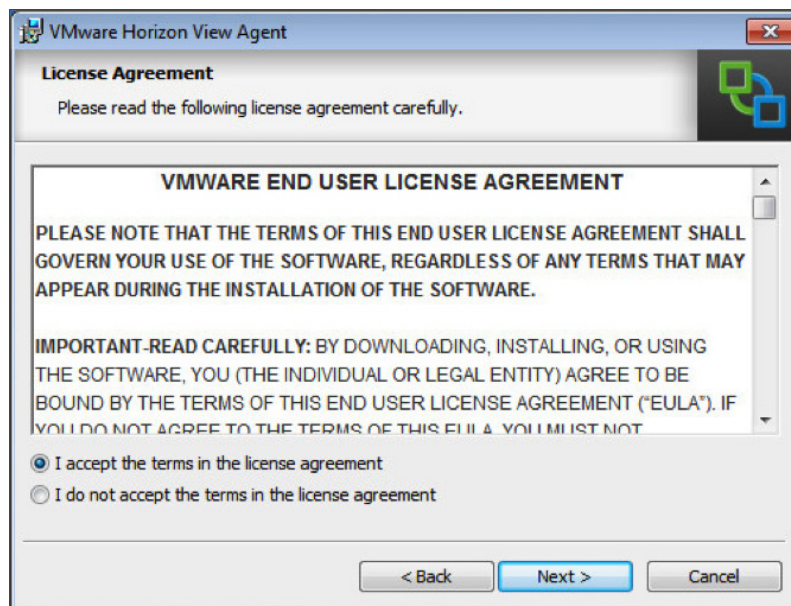
You are installing the View Agent on the virtual machine currently being configured, which will result in its becoming the master image. However, you are not finished configuring it yet.



3. Wait for the installer to load, and click **Next**.

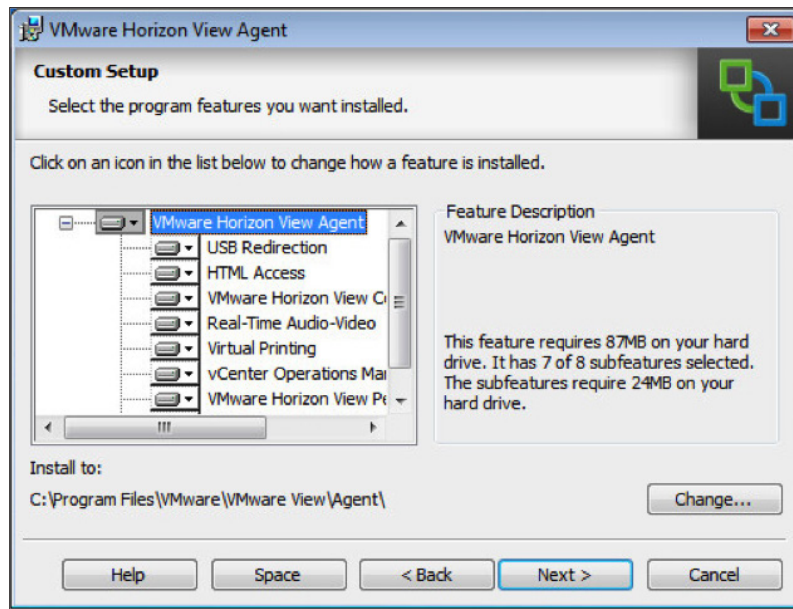


4. Review and accept the terms and conditions, and click **Next**.



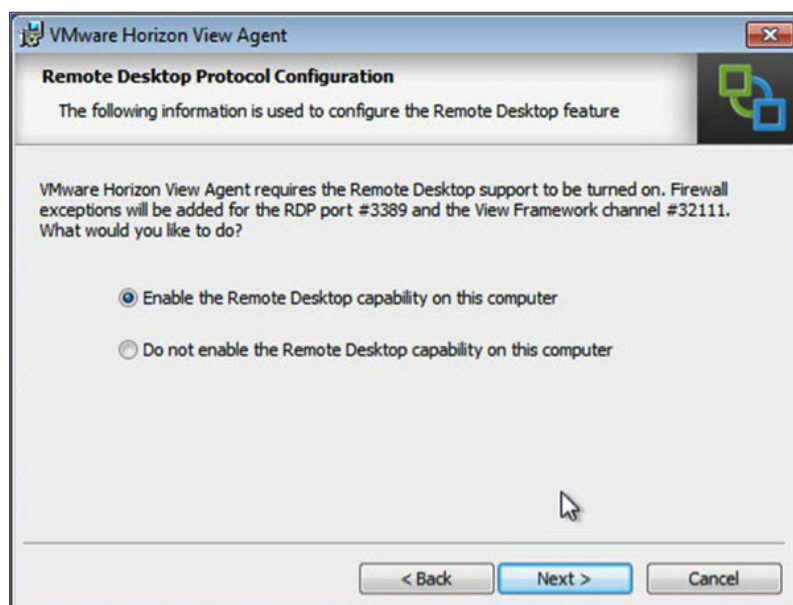
- In the Custom Setup window, enable all the features by default (recommended) to take full advantage of View Agent and properly complete these exercises.

Optionally, you can disable the features that you do not want and change the default installation directory by clicking **Change**.



- Click **Next**.
- From the Remote Desktop Protocol Configuration window, select **Enable the Remote Desktop capability on this computer**.

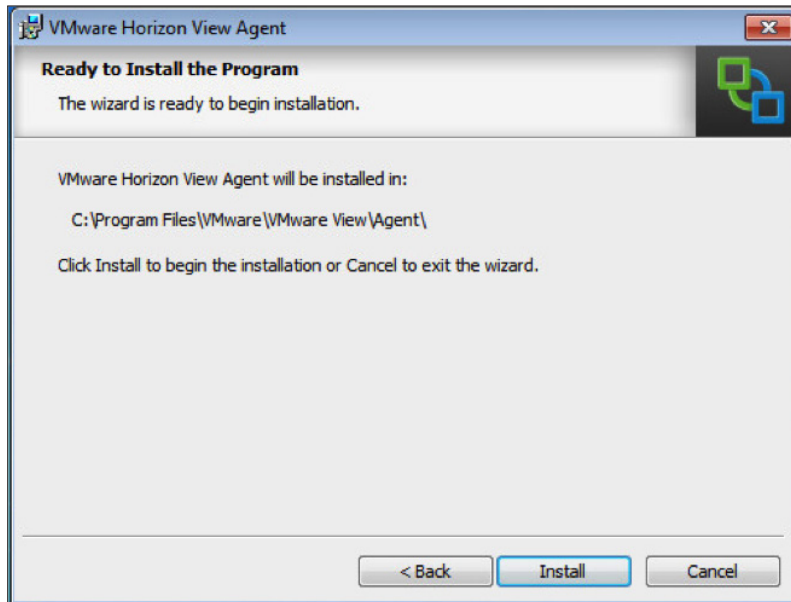
If you select the **Do not enable the Remote Desktop capability on this computer** option, you can manually enable this feature later and configure the firewall exceptions.



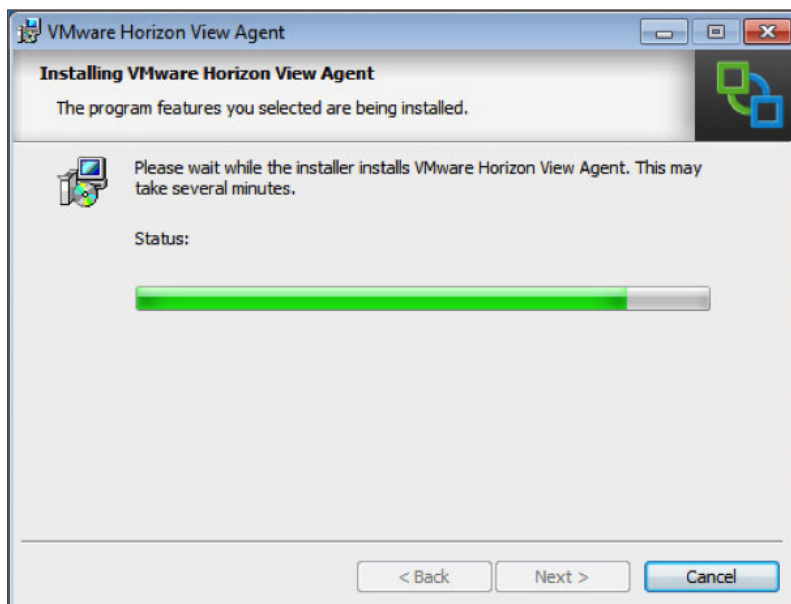
- Click **Next**.

9. To install View Agent, click **Install**.

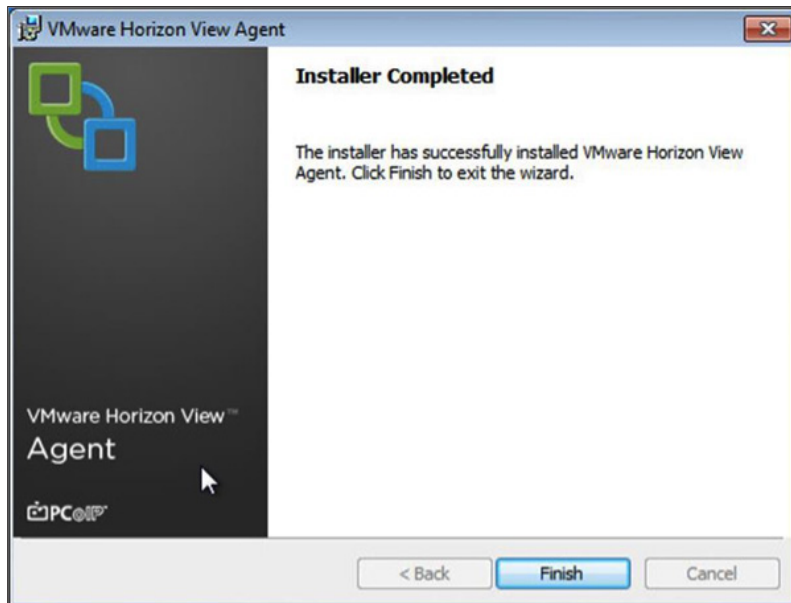
To make changes, click **Back**.



10. Monitor the installation status as it progresses.

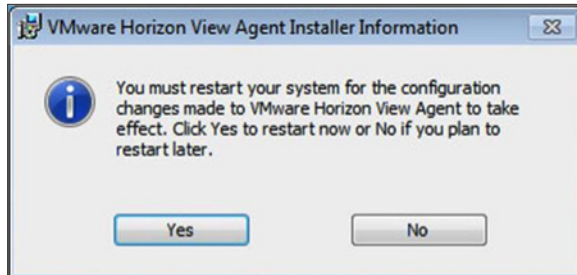


11. When the Installer Completed window appears, click **Finish** to close the View Agent installer.



12. You must restart the operating system to complete the installation.

In the VMware View Agent Installer Information dialog box, click **Yes**.



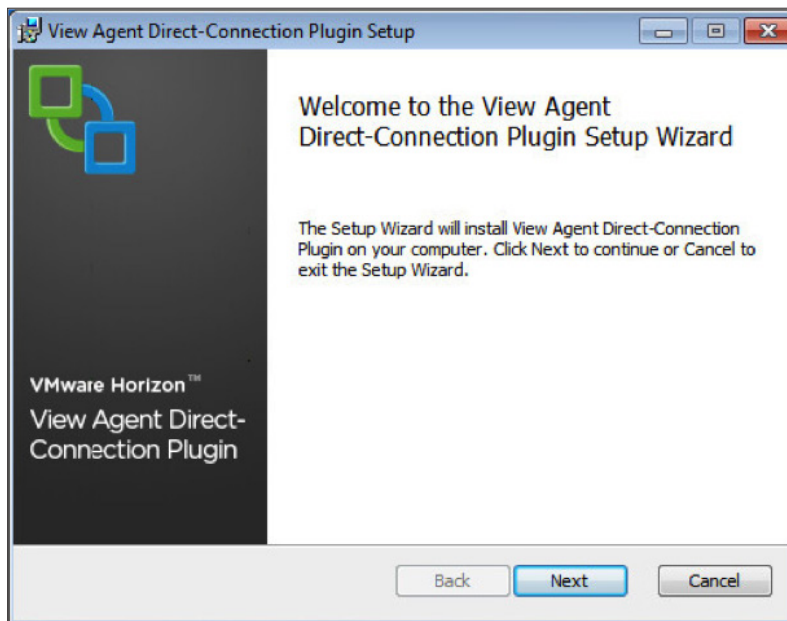
You have now installed View Agent and enabled Persona Management on the virtual machine. Proceed to the next exercise to install the View Agent Direct-Connection Plug-In.

Install the View Agent Direct-Connection Plug-In (Optional)

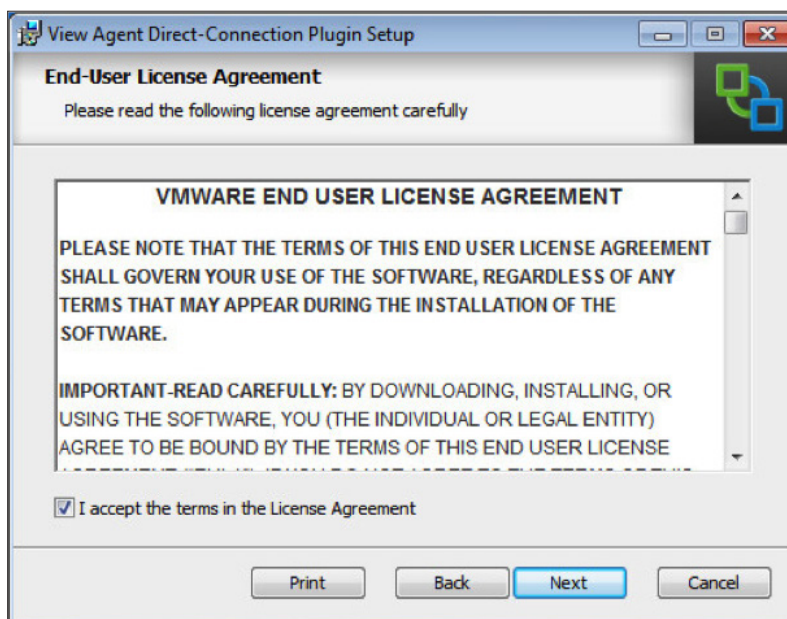
The View Agent Direct-Connection Plug-In enables any Horizon Client to connect directly to a View desktop without using View Connection Server.

This exercise is optional. If you do not want to use this feature, skipping this exercise does not prevent you from completing the subsequent exercises.

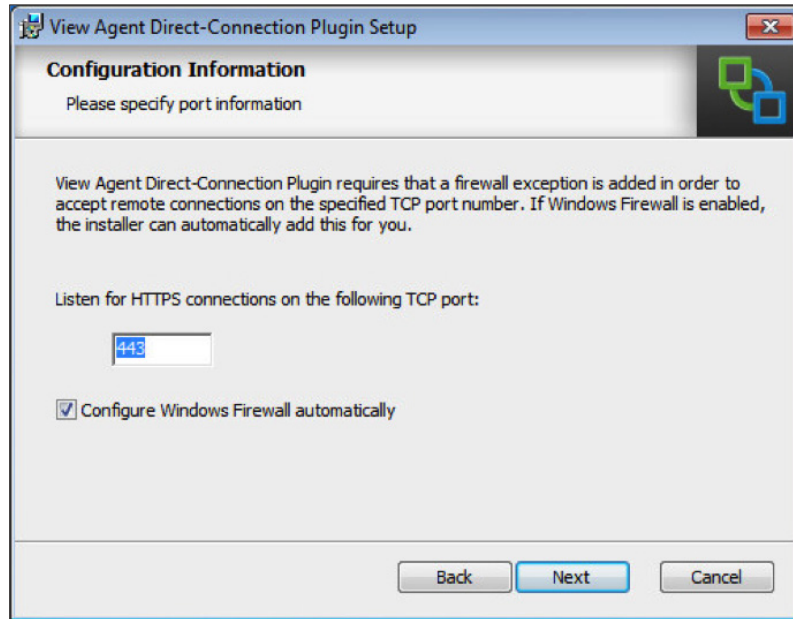
1. Launch the View Agent Direct-Connection Plug-In installer using the Run As Administrator option.
2. Ensure that the installer is accessible from your virtual machine.
3. When the installer loads, click **Next**.



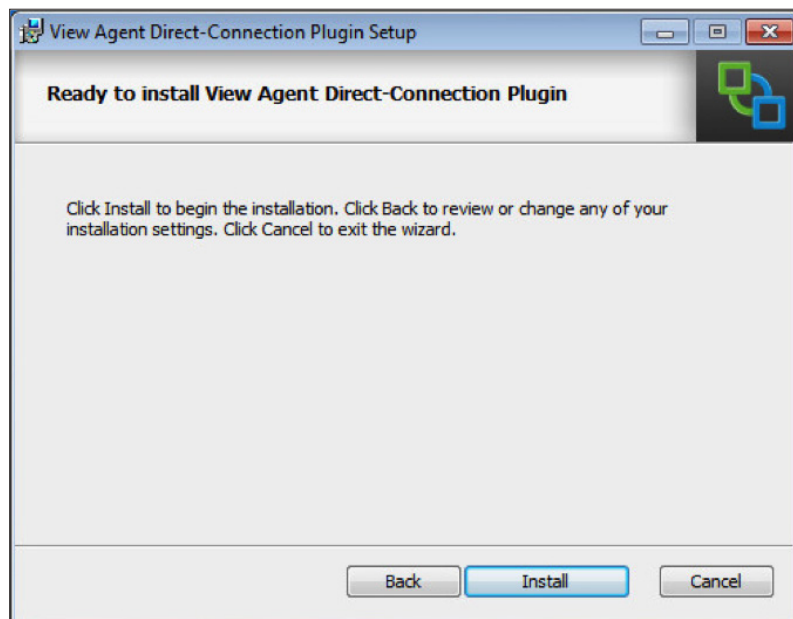
4. Review and accept the terms and conditions, and click **Next**.



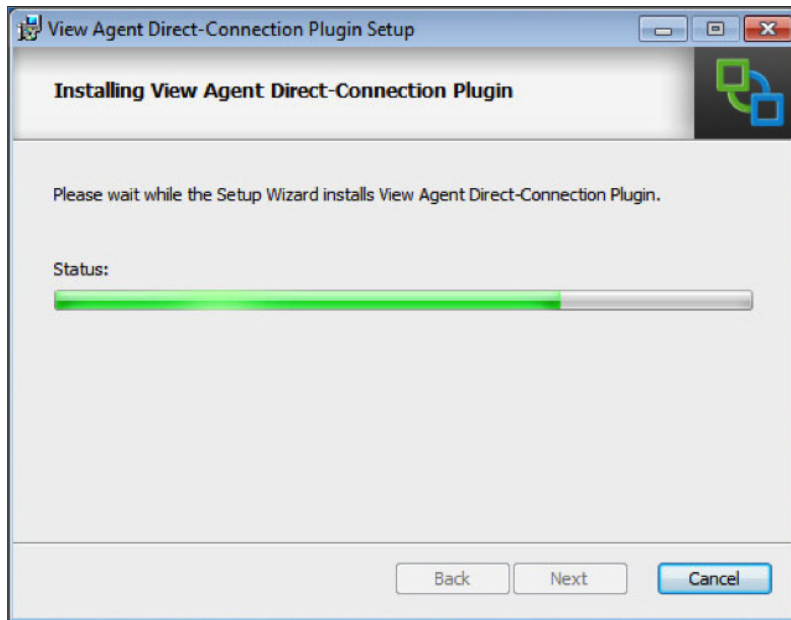
5. Confirm the default port required for HTTPS connections, select the **Configure Windows Firewall automatically** option, and click **Next**.



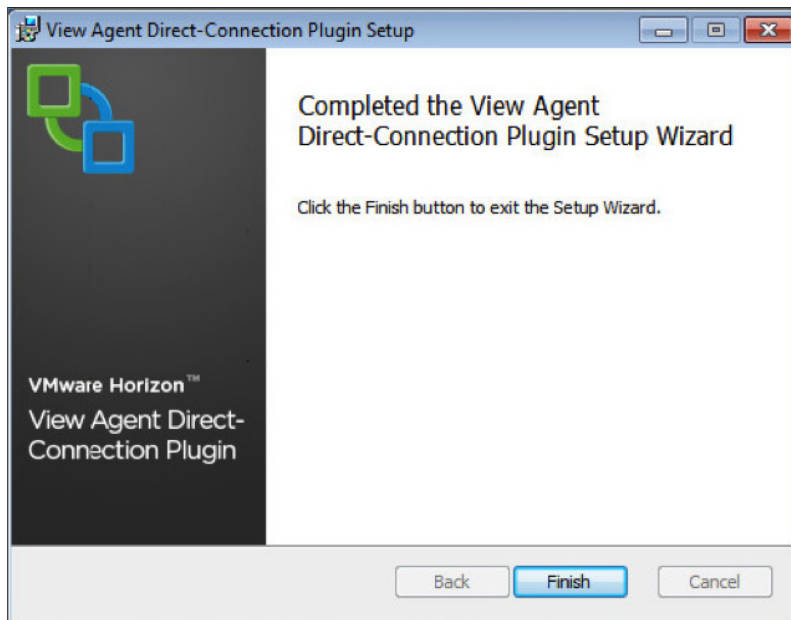
6. In the Ready to Install View Agent Direct-Connection Plugin dialog box, click **Install** to proceed.
If you want to make changes, click **Back**.



7. Monitor your installation status as it progresses.



8. When the installer has completed, click **Finish** to close the View Agent Direct-Connection Plug-In installer.



You can now proceed to the next exercise to optimize the virtual machine for desktop deployment.

Optimize the Virtual Machine for Desktop Deployment

We recommend that you optimize Windows for View desktop deployment as described in the [Optimization Guide for Desktops and Servers in View in VMware Horizon 6 and VMware Horizon Air Desktops and Apps](#).

The guide describes an option in the [VMware Operating System Optimization Tool \(OSOT\)](#) to optimize the master image to work with Persona Management.

After you have optimized the virtual machine, proceed to the next exercise to install custom applications and configure the virtual machine OS.

Install Custom Applications and Configure the Operating System (Options)

This exercise is optional but recommended. You can always return to your the linked-clone master image to

- Install additional applications or modifications
 - Update the existing desktop pools or deploy new ones
1. Install the custom application that you want preinstalled for View desktop deployment.
 2. Make any modifications to the Windows operating system.
 3. Verify that Windows Activation has been completed to ensure that your operating system is activated.

When you have finished installing custom applications and modifying the OS, you are ready to prepare the virtual machine for linked-clone deployment.

Prepare the Virtual Machine for Linked-Clone Deployment

To prepare the virtual machine for linked-clone deployment:

1. Join the virtual machine to the domain.
2. Ensure that the virtual machine is set to receive a DHCP IP address.
3. From the Windows command prompt, run the following command to release the DHCP lease.

```
ipconfig /release
```

4. Shut down the guest operating system, and power off the virtual machine.
5. Take a snapshot of the virtual machine from the vSphere Client.
6. Give the snapshot a meaningful name and description so that you have a reminder of what it contains.

This snapshot is used when you deploy the linked-clone desktop pool in a later exercise.

You have now prepared your virtual machine for linked-clone desktop deployment. Proceed to the next series of exercises to prepare a master image for *full-clone* desktop pool deployment.

Preparing a Virtual Machine for Full-Clone Desktop Pool Deployment

This section describes how to prepare a Windows Server 2008 R2 SP1 View virtual machine to use to deploy a full-clone desktop pool in a later exercise:

- [Create a Virtual Machine to Be Used for Desktop Deployment](#)
- [Install View Agent on the Desktop Image Virtual Machine](#)
- [Install the View Agent Direct-Connection Plug-In \(Optional\)](#)
- [Install Custom Applications and Configure the Virtual Machine Operating System \(Optional\)](#)
- [Prepare the Virtual Machine for Full-Clone Deployment](#)

Create a Virtual Machine to Be Used for Desktop Deployment

You can use virtual machines managed by vCenter Server

- To provision and deploy desktops as master images for automated full-clone pools
- As master images for linked-clone pools
- As a desktop source in a manual pool

You must prepare virtual machines to deliver View desktop access.

Full-clone desktop pools are deployed from copies of the virtual machine that you are preparing. (The virtual machine that the copies are made from is also called the master image.)

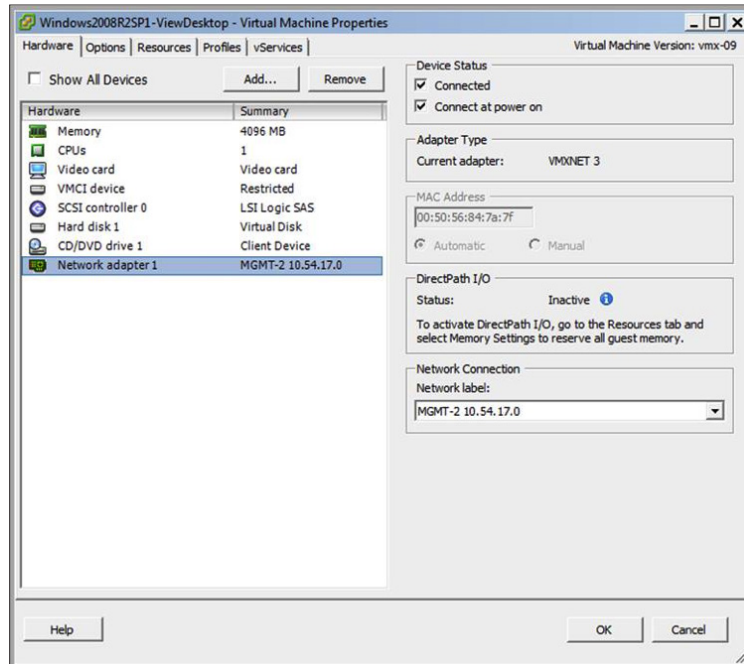
1. Log in to your host from the vSphere Client.
2. Create a new virtual machine using the following specifications as a guide.

Note: These desktop specifications are recommended for evaluating a nonproduction deployment. For a production environment, where desktop sizing varies based on the types of user workloads, see the [View Architecture Planning guide](#) for best practices on resource planning.

TYPE	vCPUS	RAM	VIRTUAL DISK SIZE
Knowledge worker	1 vCPU	2GB RAM	24GB
Power worker	2 vCPUs	4GB RAM	24GB

3. Ensure that the virtual machine network adapter type is VMXNET 3.

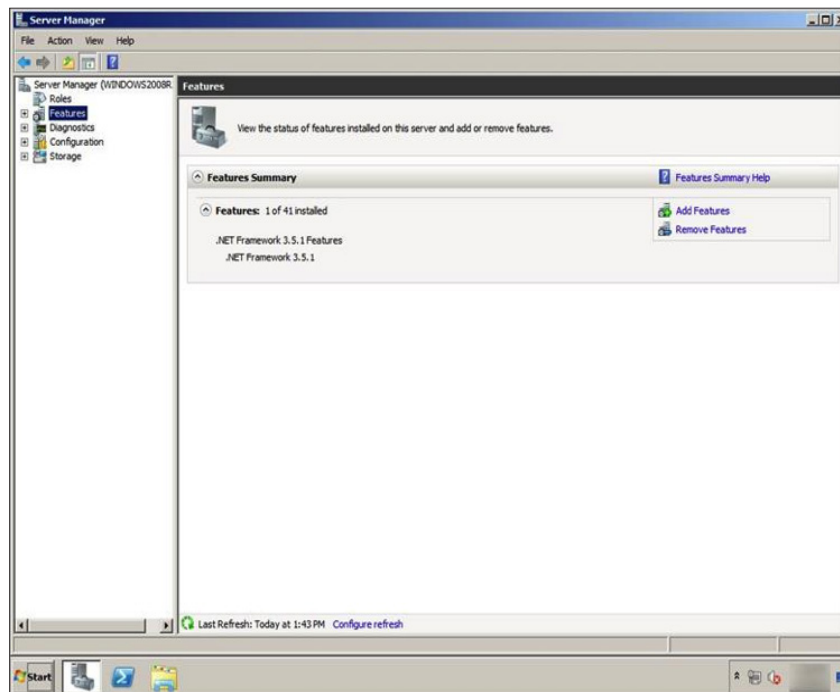
You do not want to use the E1000 adapter type because issues might arise during deployment and customization.



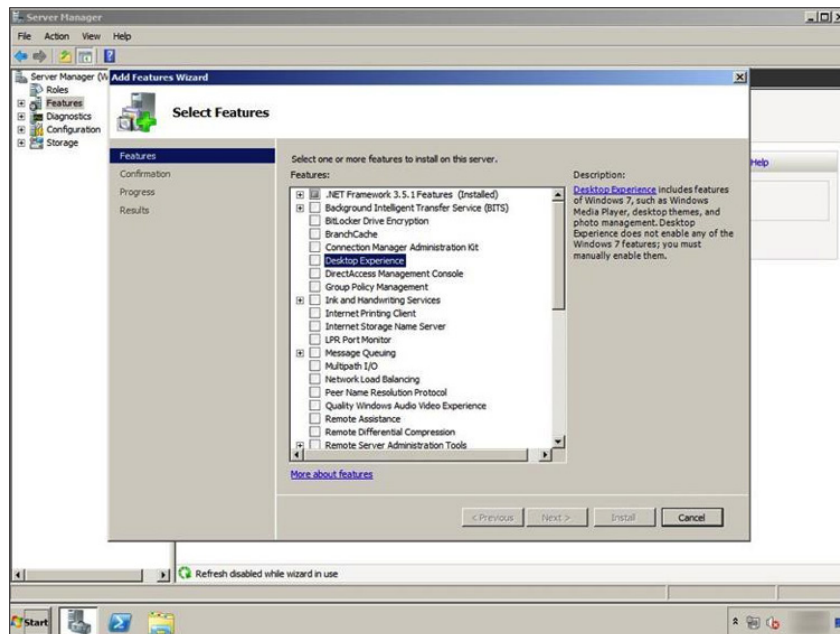
4. Install the Windows Server 2008 R2 with SP1 64-bit guest operating system, and ensure that Service Pack 1 has been applied to the OS if you used the base Windows Server 2008 R2 64-bit media.
5. Activate your Windows operating system according to your organization's procedures.
6. Log in to the virtual machine as a local administrator and open the Server Manager utility to install the Desktop Experience feature (required).

The Desktop Experience feature is required for correct operation with View.

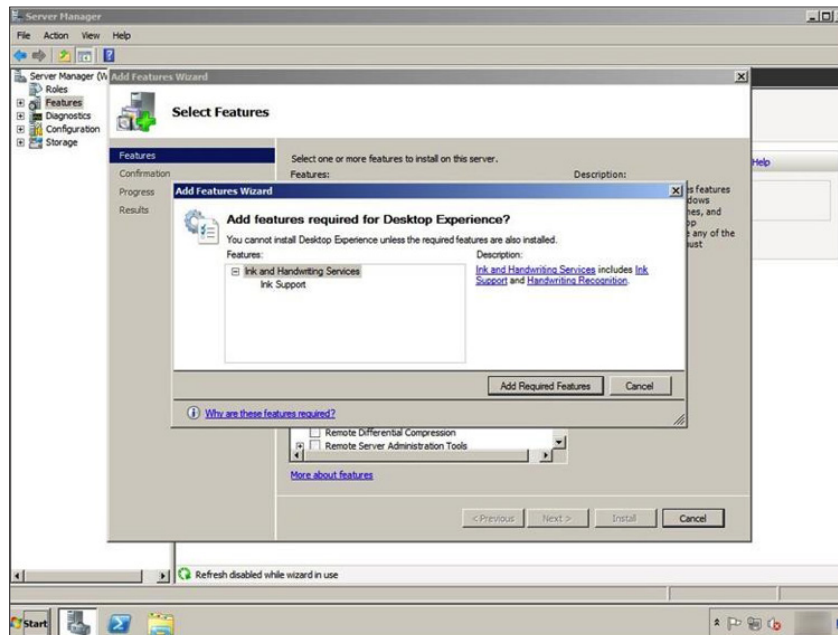
7. Click the **Features** menu, and click **Add Features**.



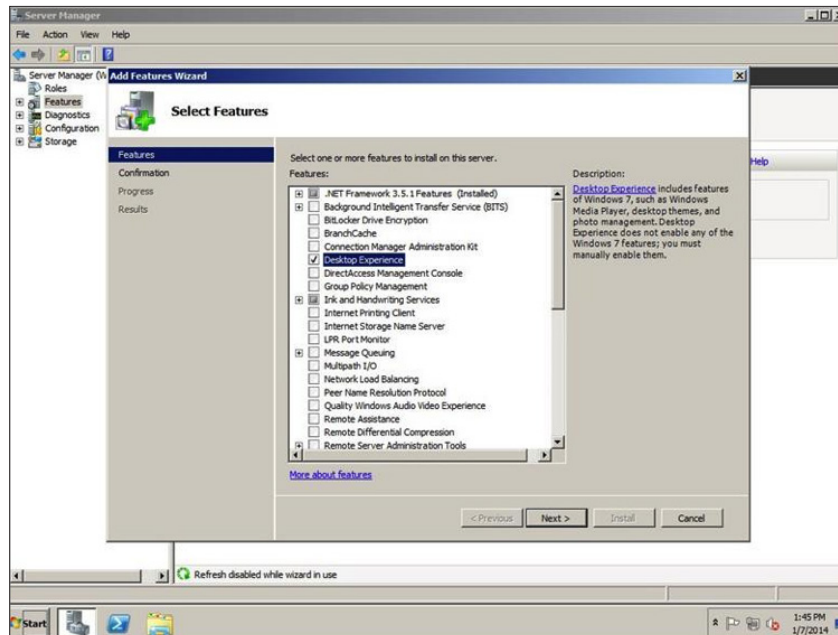
8. In the Add Features Wizard window, select the **Desktop Experience** feature, and click **Next**.



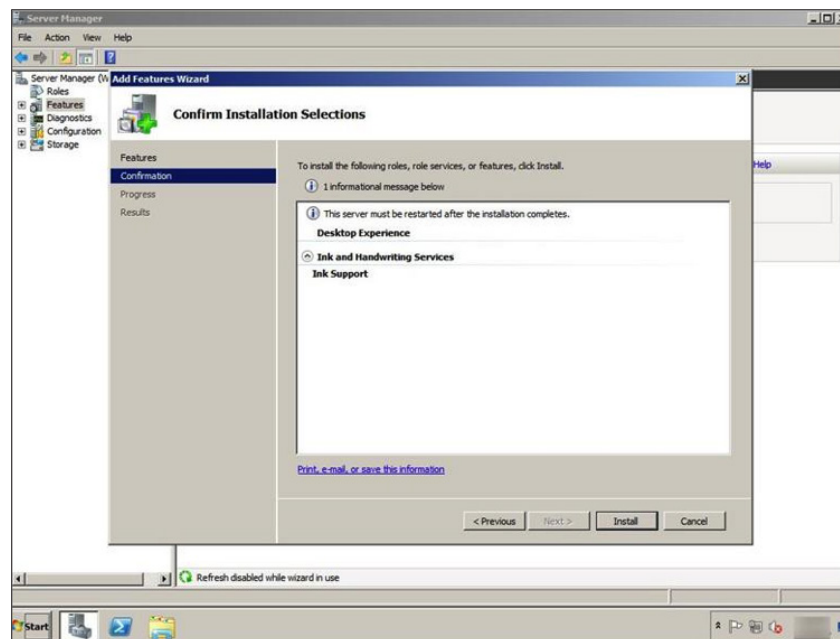
9. If you need to add feature prerequisites, click **Add Required Features**.



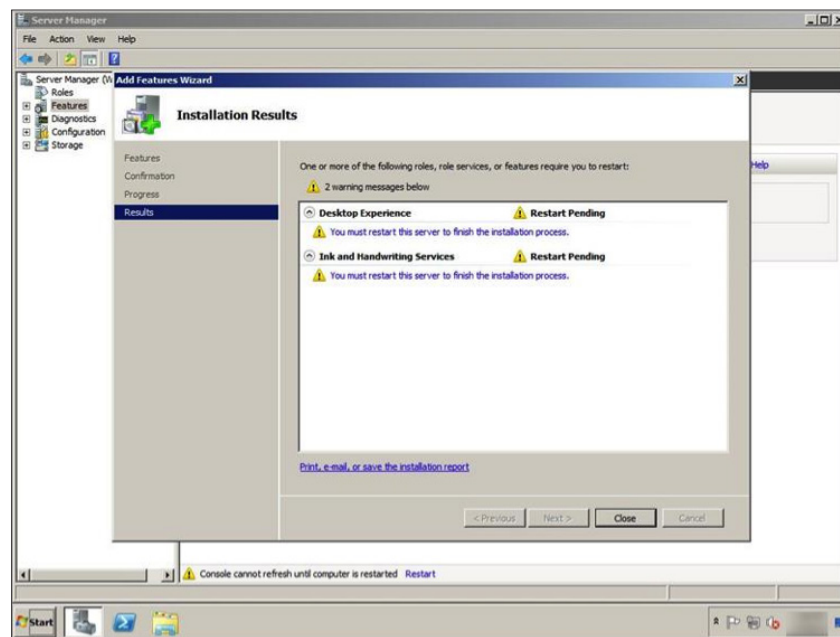
10. Confirm that Desktop Experience and the required prerequisites are selected, and click **Next**.



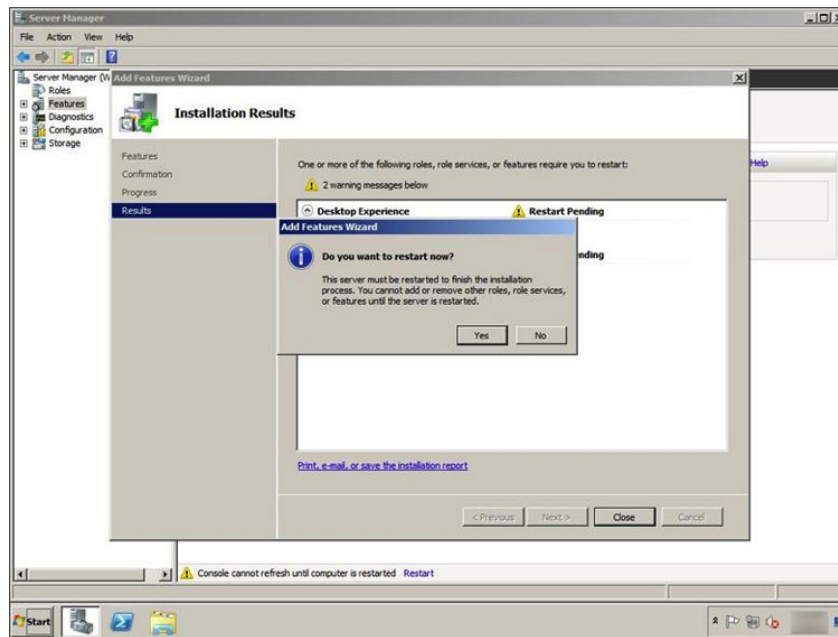
11. To install the features, click **Install**.



12. After reviewing the summary of the features and required actions, click **Close** to continue.



13. Click **Yes** to restart the computer and complete the installation.

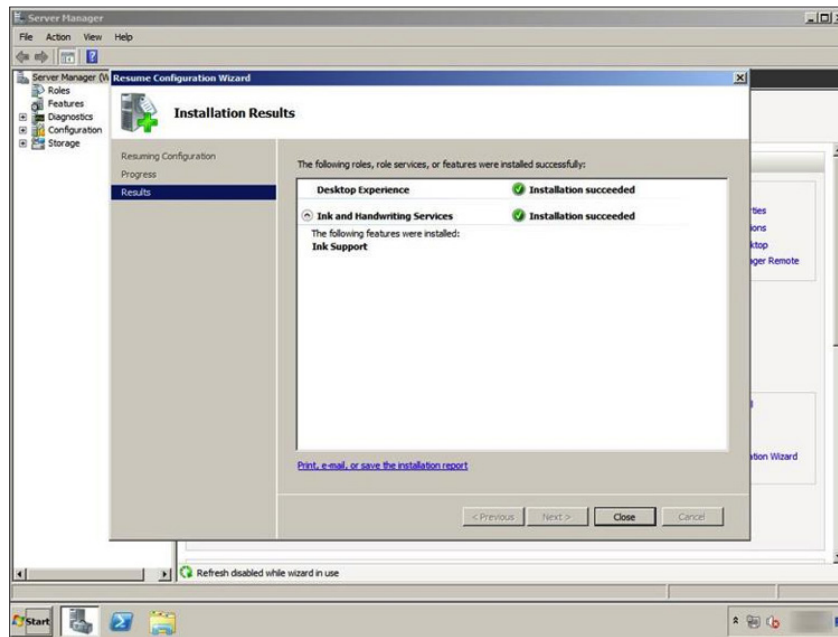


14. Monitor the feature installation as it progresses.



15. When the installation is finished, log back in.

- 16 In the Installation Results window, which verifies the installation of the Desktop Experience feature, click **Close**.

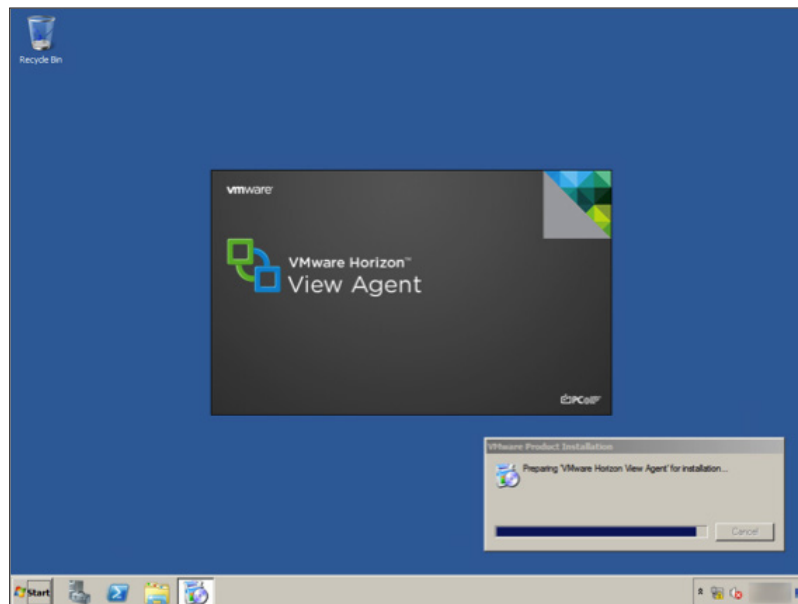


You have now finished all the operating system prerequisites for the Windows 2008 R2 SP1 View virtual machine. Proceed to install View Agent.

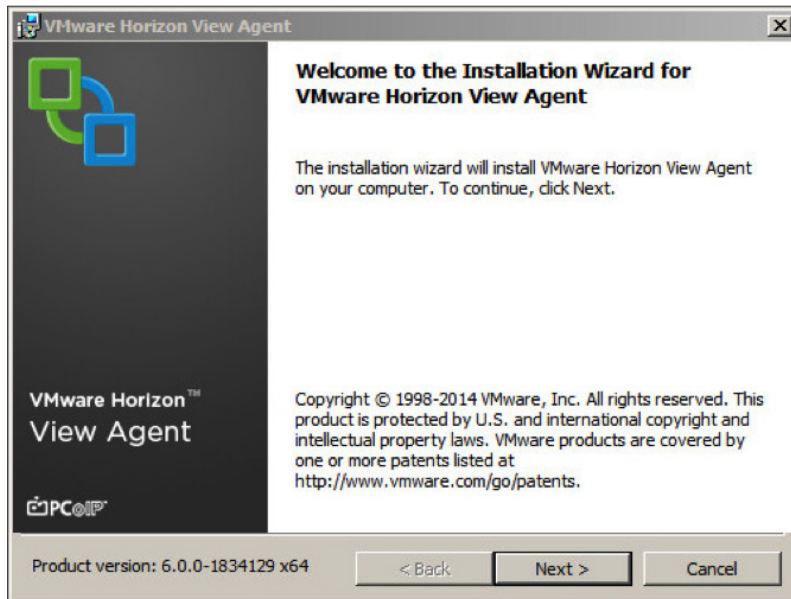
Install View Agent on the Virtual Machine

The View Agent installer must be accessible from your virtual machine.

1. Launch the View Agent installer using the Run As Administrator option.
2. Ensure that the installer is accessible from your virtual machine.



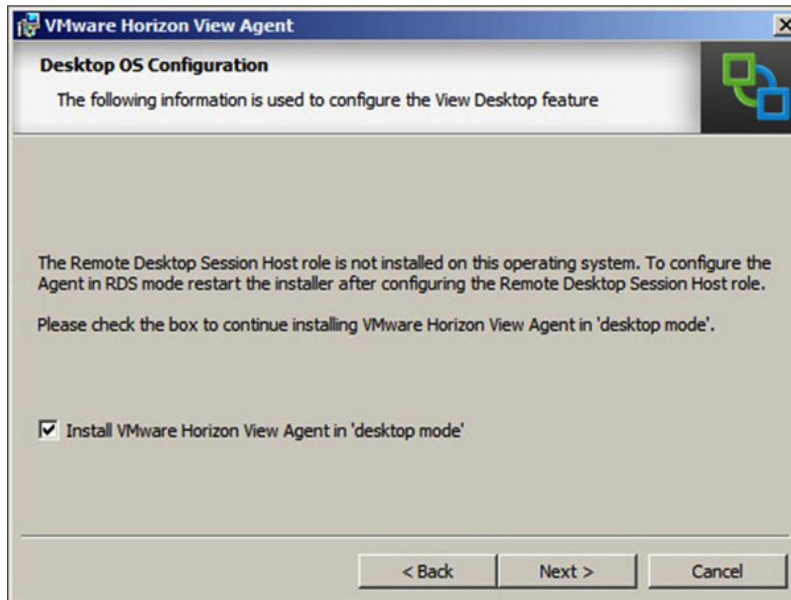
- When the installer has loaded, click **Next**.



- Read the license agreement, accept the terms and conditions, and click **Next**.

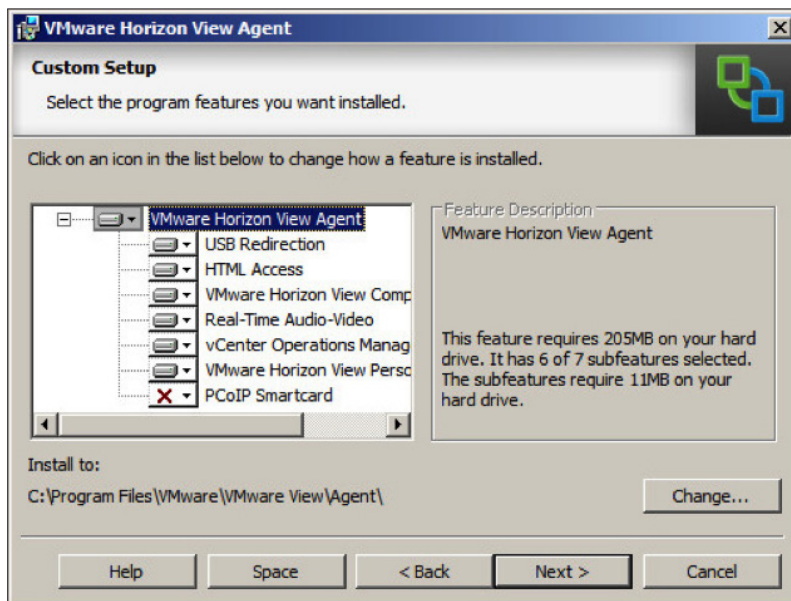


- In the Desktop OS Configuration warning, select **Install VMware Horizon View Agent in 'desktop mode'**, and click **Next**.



Note: The available features that can be installed with View Agent are listed. It is recommended that you use the features selected to ensure that all View Agent features are available when you deploy your desktop pool.

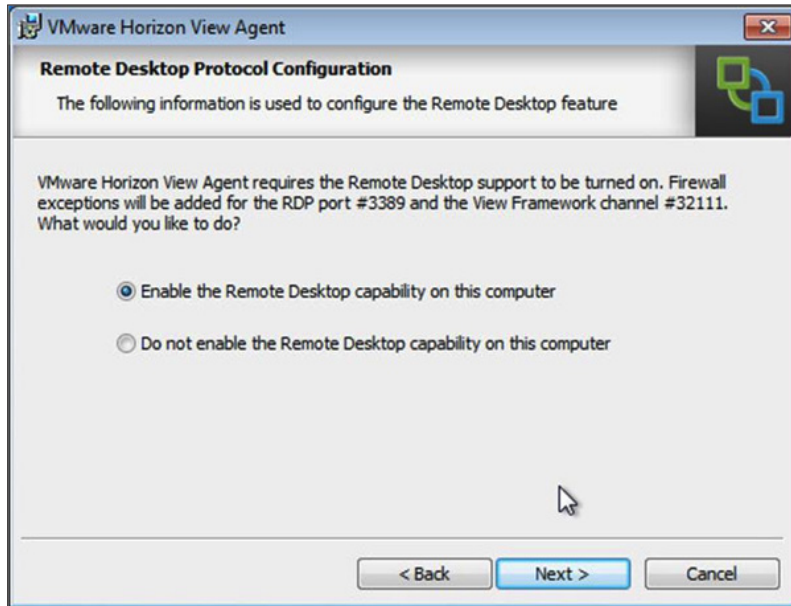
- To change the default installation directory, click **Change**.



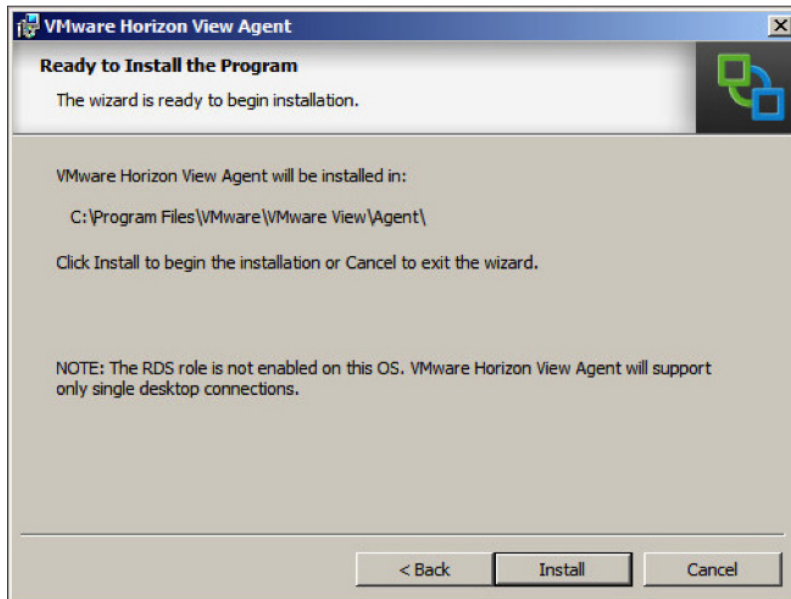
- When you are ready to proceed, click **Next**.

8. Select **Enable the Remote Desktop capability on this computer**.

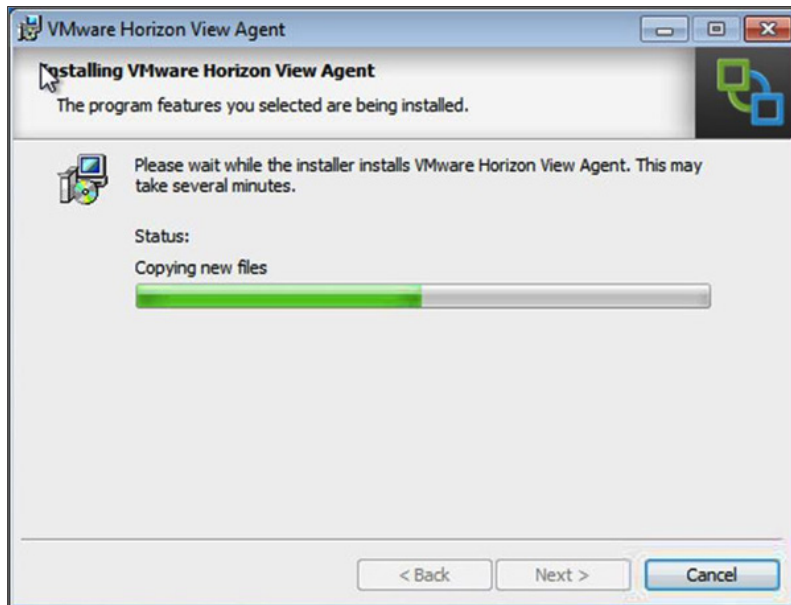
If you select the **Do not enable** option, you can manually enable this feature later and configure the firewall exceptions.



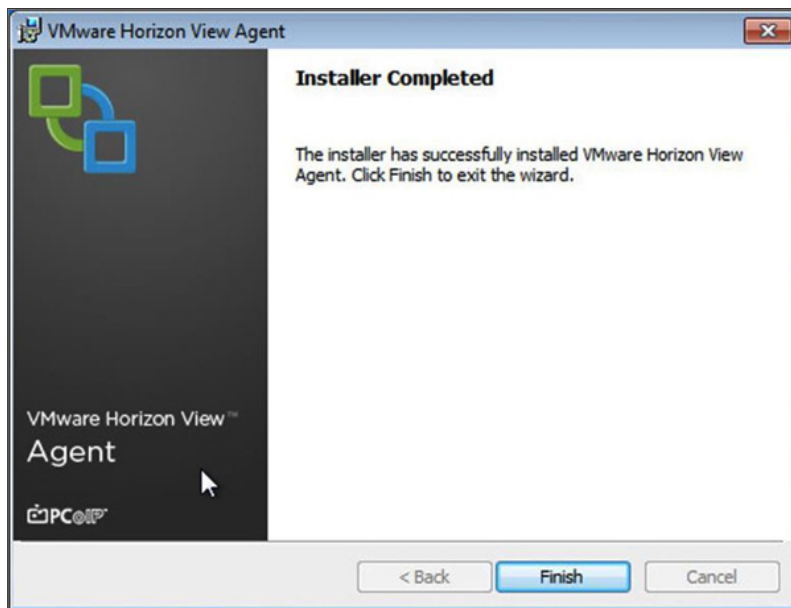
9. Click **Next**.
10. To install View Agent, click **Install**.
To make changes, click **Back**.



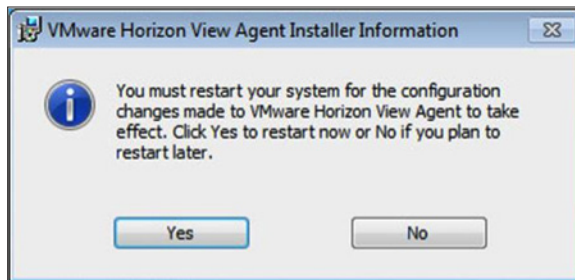
11. Monitor your installation status as it progresses.



12. When the Installer Completed window displays, click **Finish** to close the View Agent installer.



13. In the VMware View Agent Installer Information dialog box, click **Yes**.



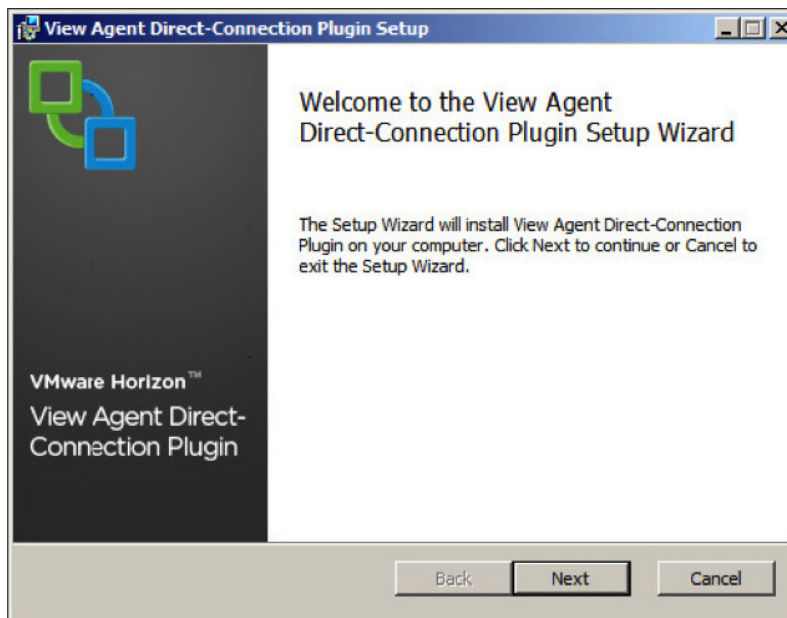
You have now installed View Agent. Proceed to the next exercise to install the VMware View Agent Direct-Connection Plug-in.

Install the View Agent Direct-Connection Plug-In (Optional)

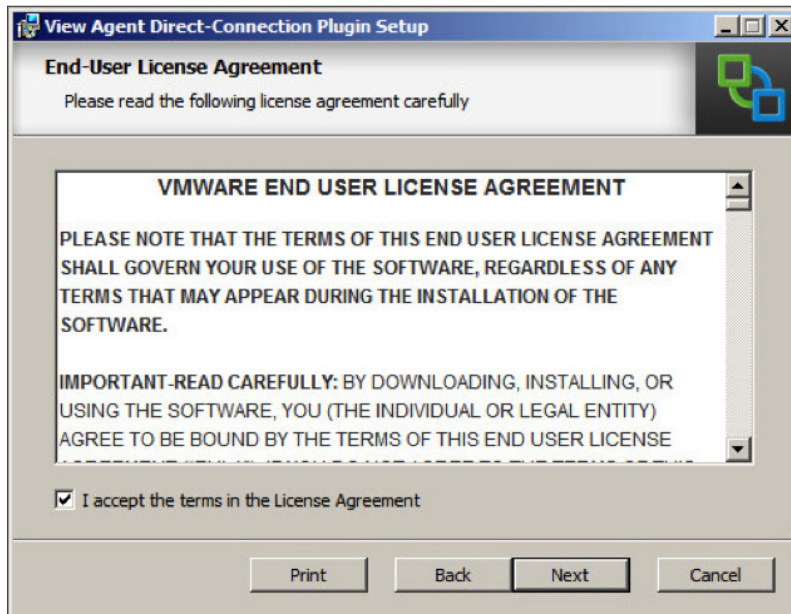
The View Agent Direct-Connection Plug-in enables any Horizon Client to connect directly to a View desktop without using View Connection Server.

This exercise is optional. If you do not want to use this feature, skipping this exercise does not prevent you from completing the subsequent exercises.

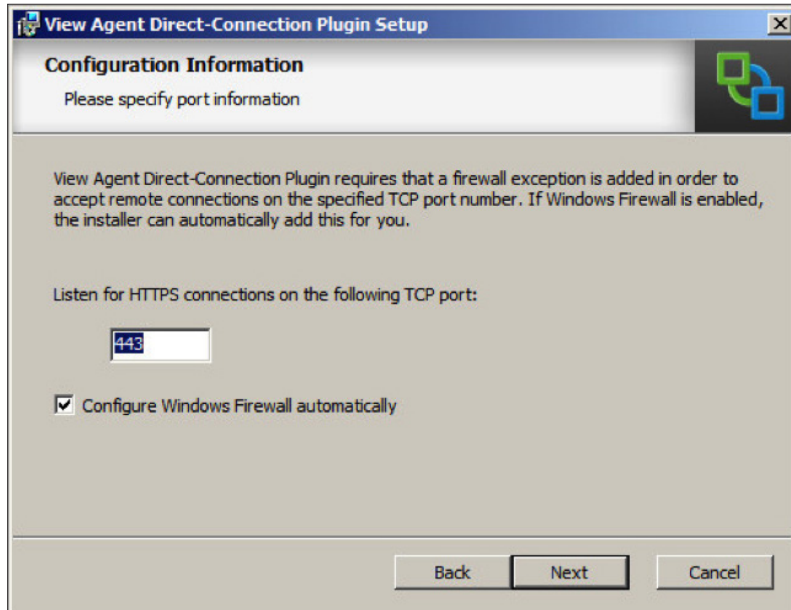
1. Launch the View Agent Direct-Connection Plug-in installer using the Run As Administrator option.
2. Ensure that the installer is accessible from your virtual machine.
3. When the launcher loads, click **Next**.



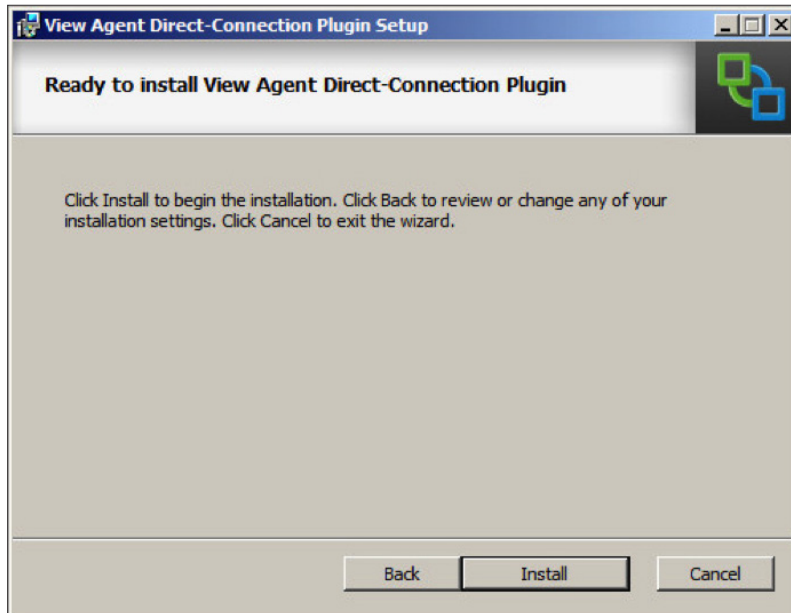
4. Read the license agreement, accept the terms and conditions, and click **Next**.



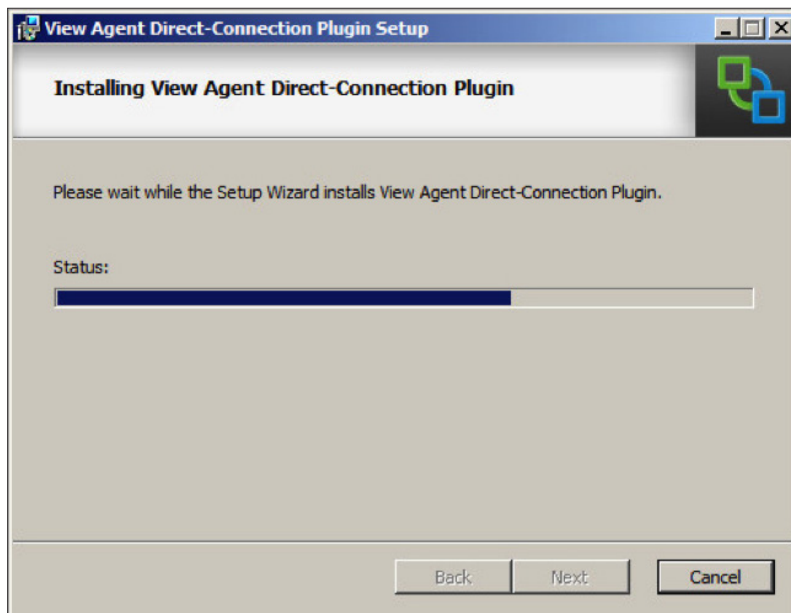
5. Confirm the default port required for HTTPS connections, select the **Configure the Windows Firewall automatically** option, and click **Next**.



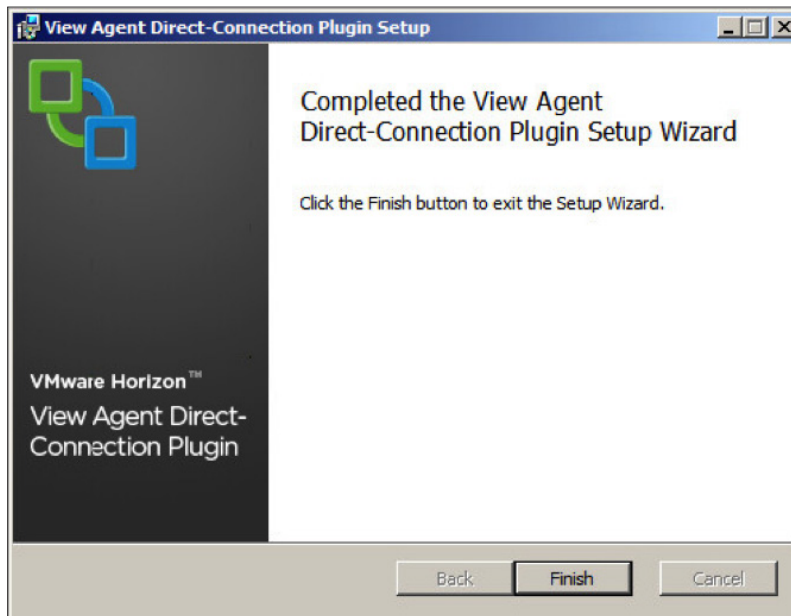
6. In the Ready to Install dialog box, click **Install** to proceed.
If you want to make changes, click **Back**.



7. Monitor your installation status as it progresses.



- When the installer has completed, click **Finish** to close the View Agent Direct-Connection Plug-in installer.



You can now install your custom applications and make modifications to your Windows operating system.

Install Custom Applications and Configure the Operating System (Options)

This exercise is optional but recommended. You can always return to your Windows 2008 R2 SP1 View master image to install additional applications or modifications. Use the View Administrator console to update existing desktop pools or deploy new ones.

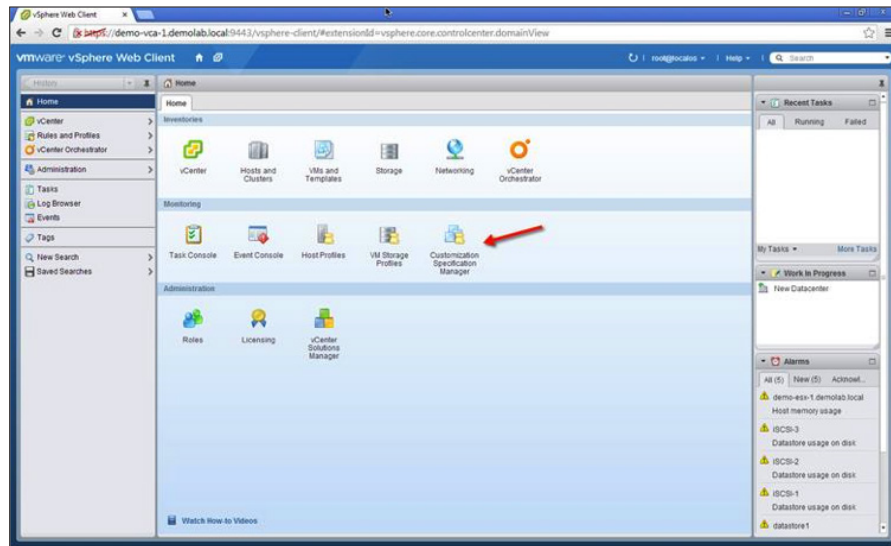
1. Install the custom applications that you want preinstalled for View desktop deployment.
2. Make any modifications to the Windows operating system.
3. Verify that Windows Activation has been completed to ensure that your operating system is activated.

When you have finished installing custom applications and modifying the OS, you are ready to prepare the virtual machine for full-clone deployment.

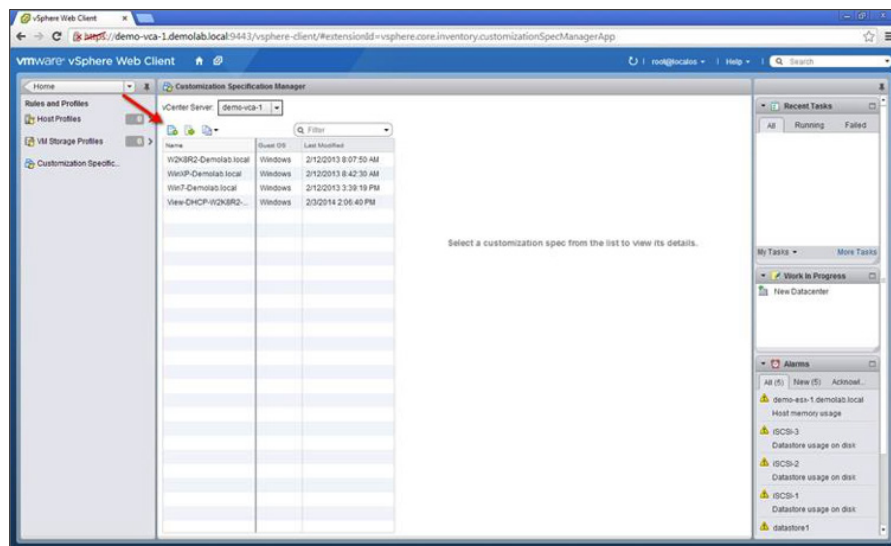
Prepare the Virtual Machine for Full-Clone Deployment

To deploy an automated pool with full clones, it is recommended that you create a customization specification to use during desktop pool deployment. You create the specification in vCenter through the vSphere Web Client. For more information, see the [vSphere 5.5 Documentation](#).

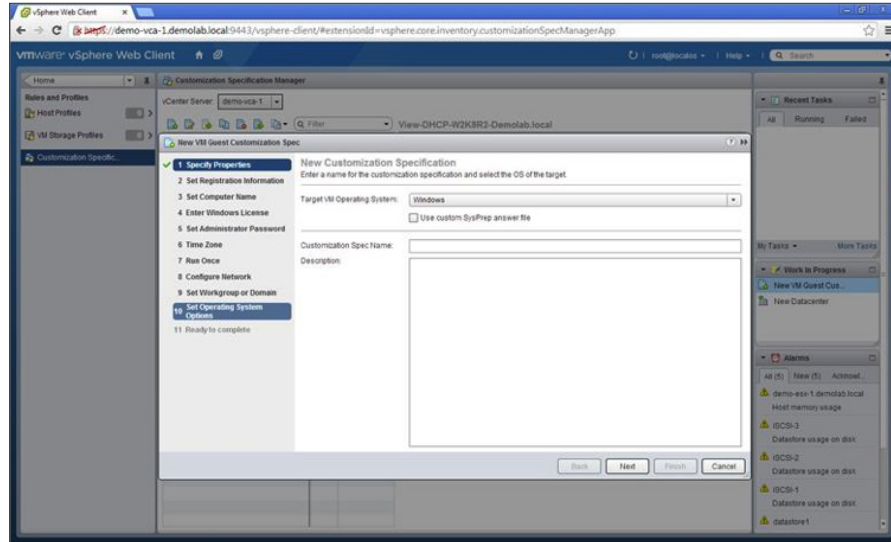
1. Navigate to the URL that connects you to your vSphere environment (vCenter Server) through the vSphere Web Client.
2. On the home page, click **Customization Specification Manager**.



3. Click the **Add** icon to create a customization specification to correspond to the Windows 2008 R2 SP1 View master image that you created.

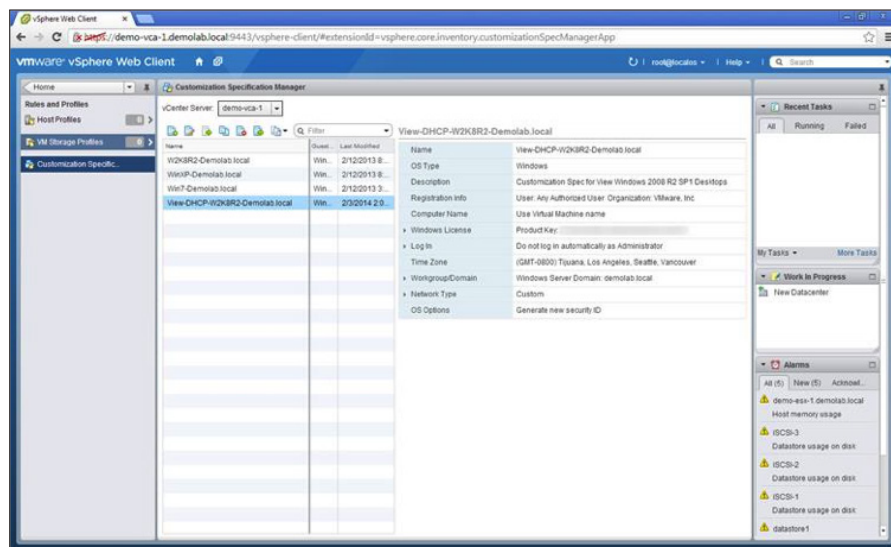


- Use the New VM Guest Customization Spec wizard to create the specification by providing information regarding your Windows licensing, Network (DHCP is recommended), and other Windows system-related options.



The new customization specification is added to the list.

- Note the name of the customization specification because you need it when deploying the automated full-clone pool.



Before continuing, you must convert your full-clone desktop image into a standalone virtual machine. You can make this change in the Options menu of your virtual machine from your vSphere Web Client. After you make this change, this virtual machine can now be considered the master image to be used by View. You are ready to deploy View desktops and applications.

Deploying View Desktop and Application Pools

After you have finished preparing virtual machines, you are ready to deploy View desktops and applications in pools. In this series of exercises, you create and deploy linked-clone and full-clone desktop pools, and RDSH desktop and application pools.

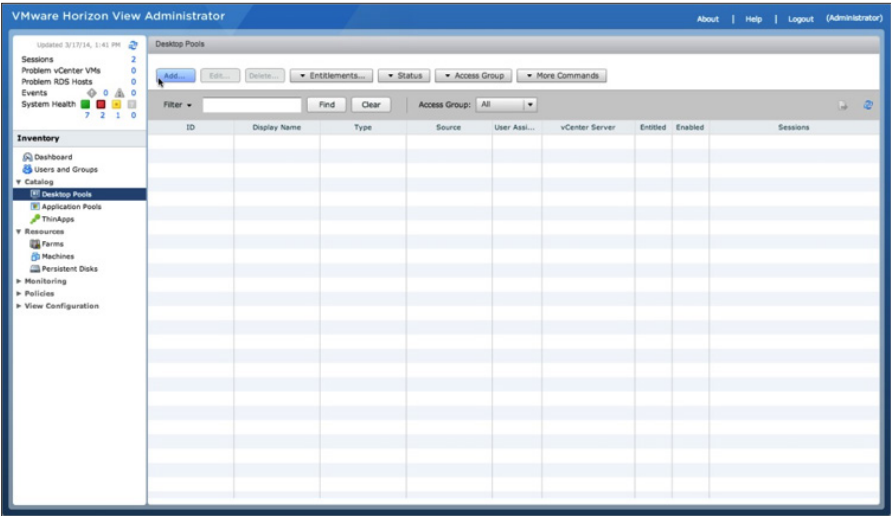
- [Deploy a Linked-Clone Desktop Pool](#)
- [Deploy a Full-Clone Desktop Pool](#)
- [Deploy an RDSH Desktop Pool](#)
- [Deploy an Application Pool](#)

Deploy a Linked-Clone Desktop Pool

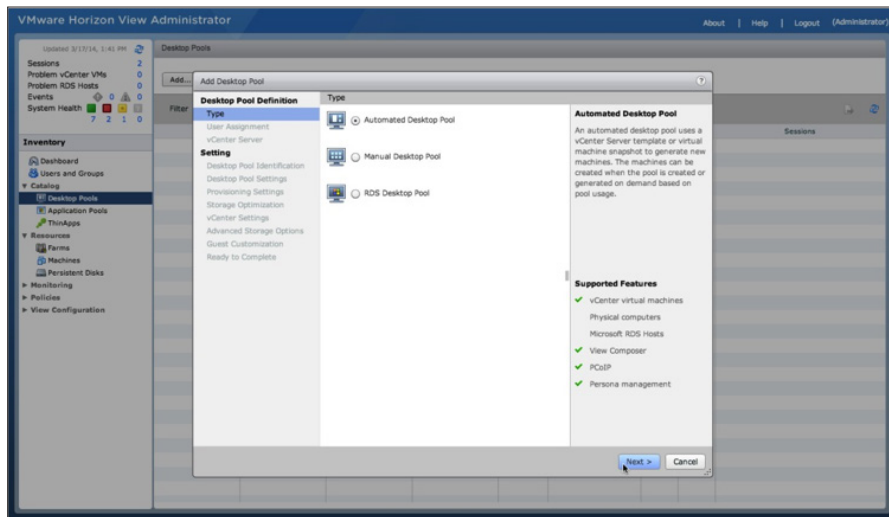
You deploy a linked-clone desktop pool based on the virtual machine that you prepared in earlier exercises.

You will now use the prepared virtual machine as the master image for linked-clone deployment to create and deploy a linked-clone desktop pool.

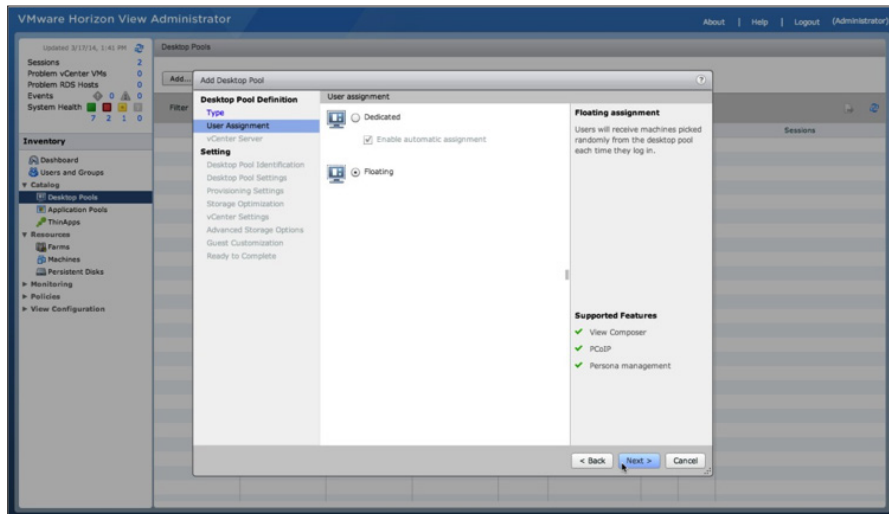
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To deploy a new pool, click **Add**.



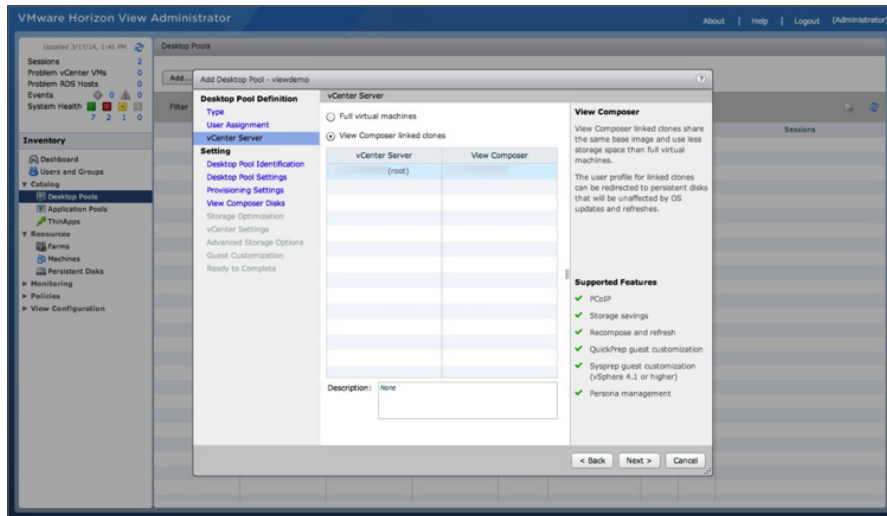
3. In the Add Desktop Pool window, select **Automated Desktop Pool**, and click **Next**.



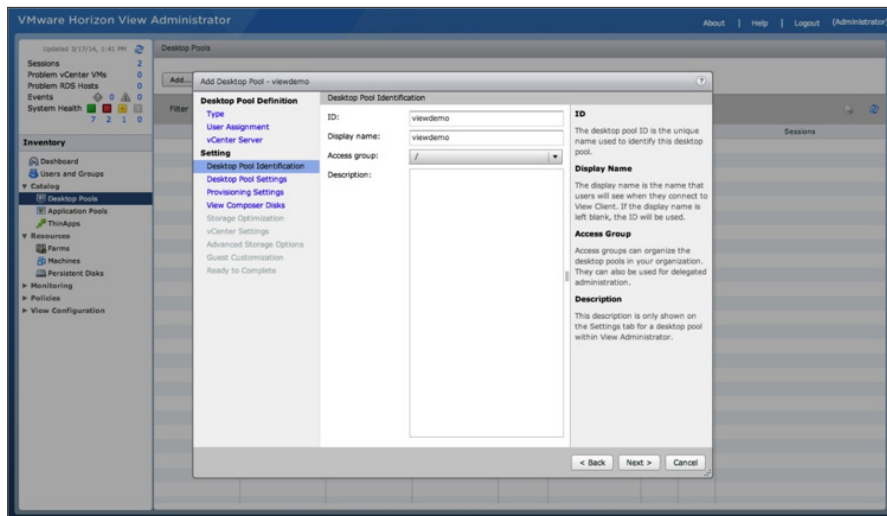
4. Specify the type of User Assignment for the pool.
5. Select **Floating**, and click **Next**.



6. Select the **View Composer linked clones** virtual desktop to deploy, and click **Next**.

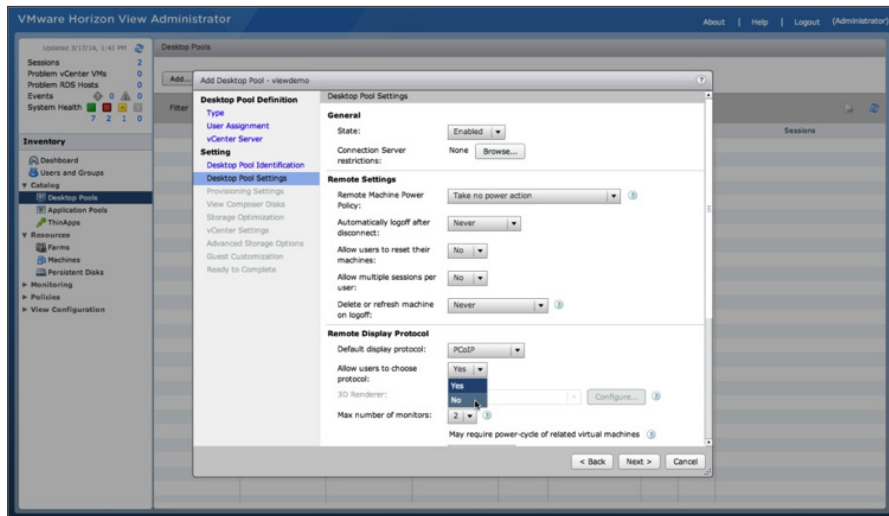


7. Add a pool ID and Display name.
Optionally, select a folder to organize your pools.
8. Click **Next**.

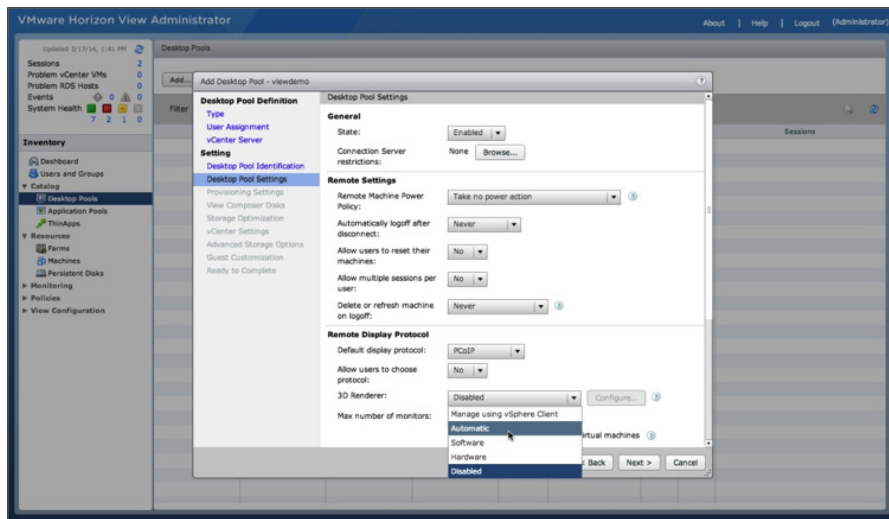


9. Adjust the Desktop Pool Settings to enable certain features.
For this example, enable vSGA - 3D Virtual Shared Graphics for the desktop pool.

10. Under Remote Display Protocol, set **Allow users to choose protocol** setting to **No**.



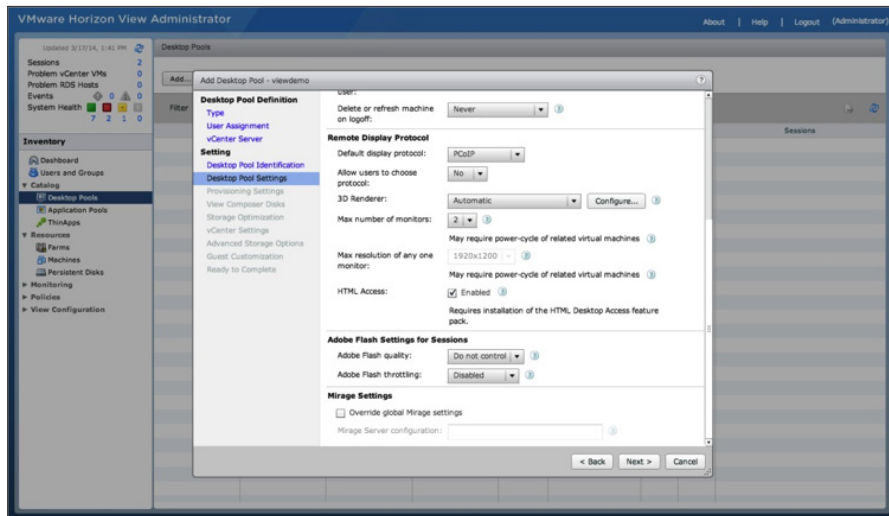
11. Under Remote Display Protocol, for 3D Renderer, select **Automatic** from the drop-down menu.



12. Scroll down the Desktop Pool Settings window to view the other available options.

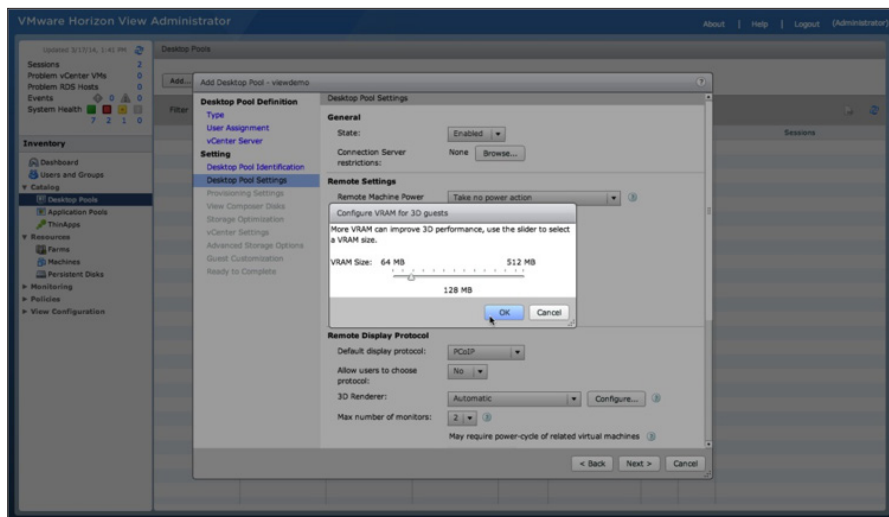
13. Enable **HTML Access**.

14. Next to 3D Renderer, click **Configure**.



15. Configure the amount of VRAM available to each virtual desktop guest using the VRAM Size slider, and click **OK**.

16. Click **Next** to configure the Provisioning Settings.



17. Adjust the Provisioning Settings:

- a. Select **Use a naming pattern** and in the Naming Pattern text box, enter a naming pattern.

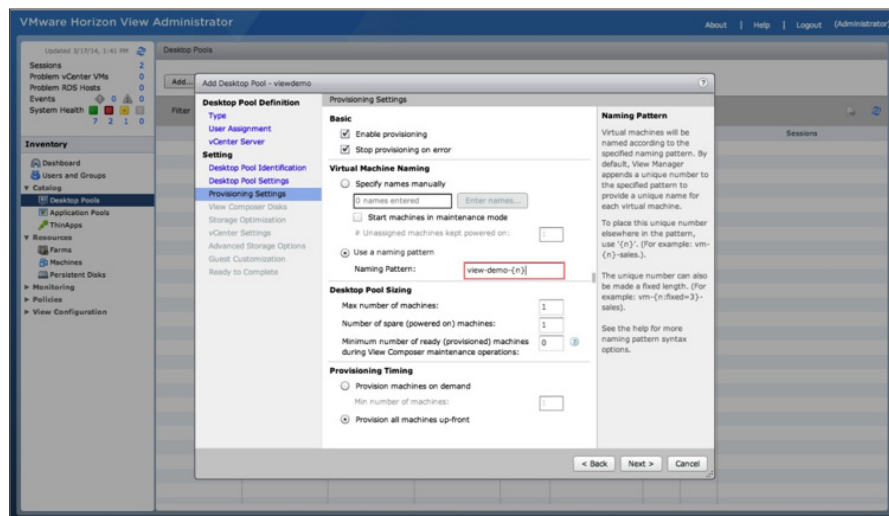
A common pattern is **<poolname>-{n}**, which displays the pool name with an incremented desktop number as desktops in the pool are provisioned.

- b. Specify the maximum pool size:

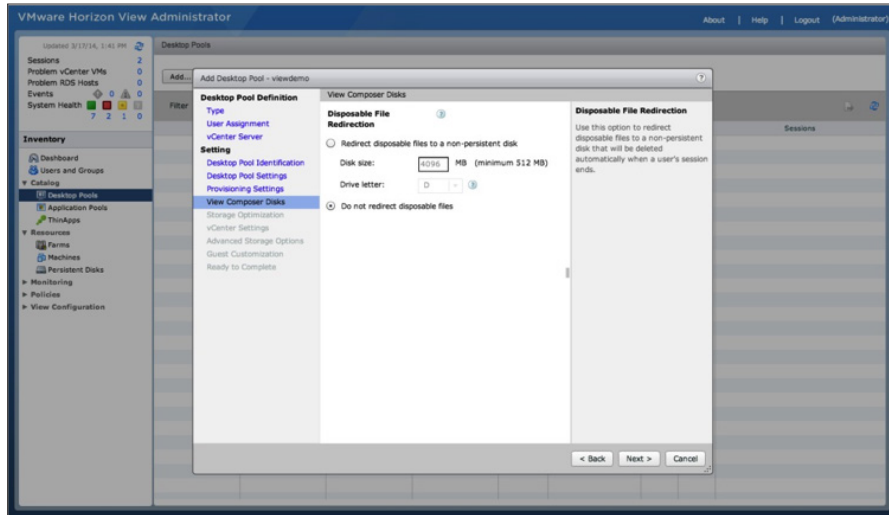
- i. Deploy a small number of desktops to test your pool.
- ii. Increase the number of desktops after you have confirmed that your deployment is successful.

- c. Under Provision Timing, select **Provision all machines up-front**.

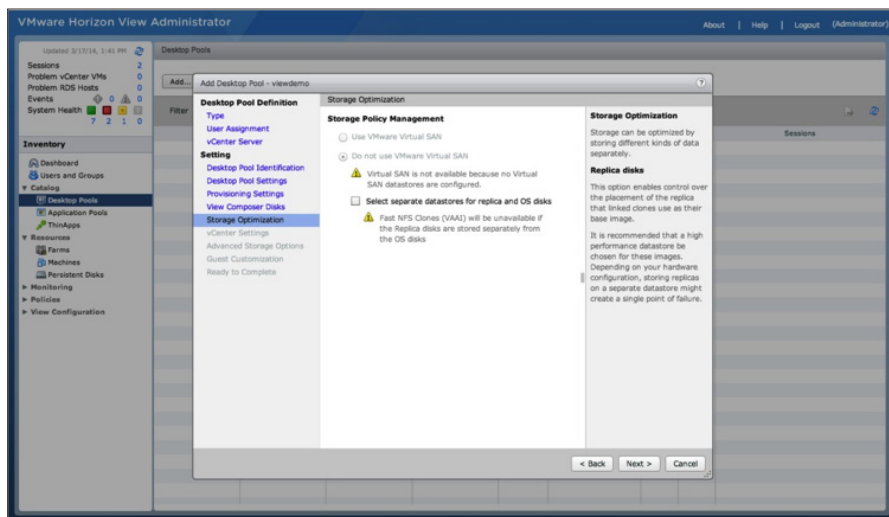
Alternatively, you could provision the desktops on demand and decide on the minimum number of desktops to have ready at initial pool deployment. Then you can provision any additional desktops as required, up to the maximum number of desktops. You can try these different pool features during subsequent pool deployments.

18. Click **Next**.

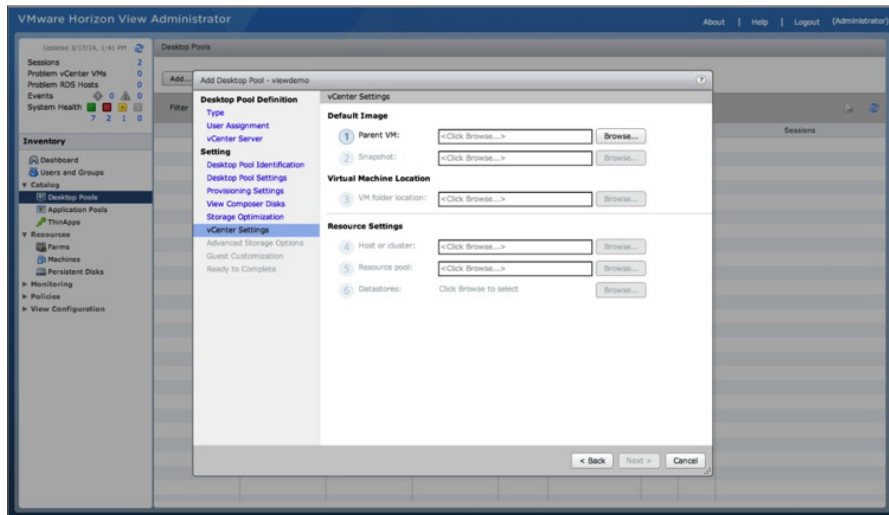
19. Specify the type of View Composer disposable disks to deploy with the pool:
 - a. For this exercise, select **Do not redirect disposable files**.
 - b. Click **Next**.



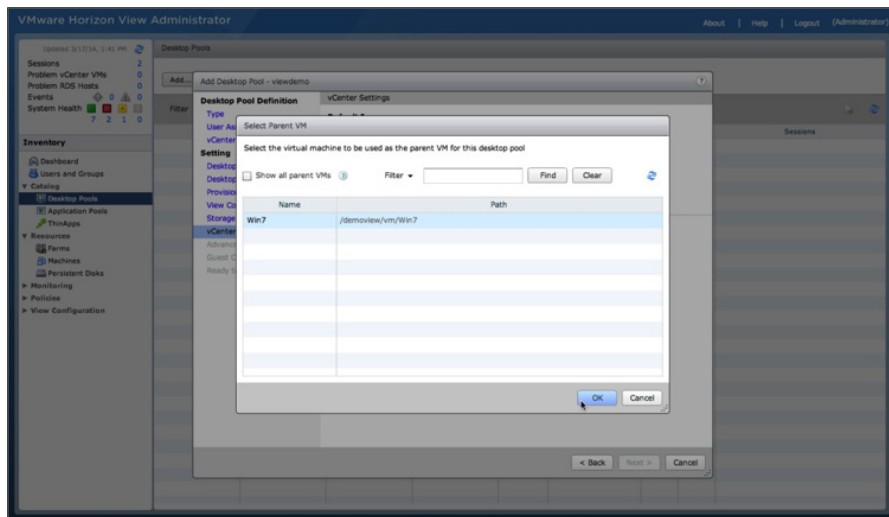
20. Do not make any modifications to the Storage Optimization options, and click **Next**.



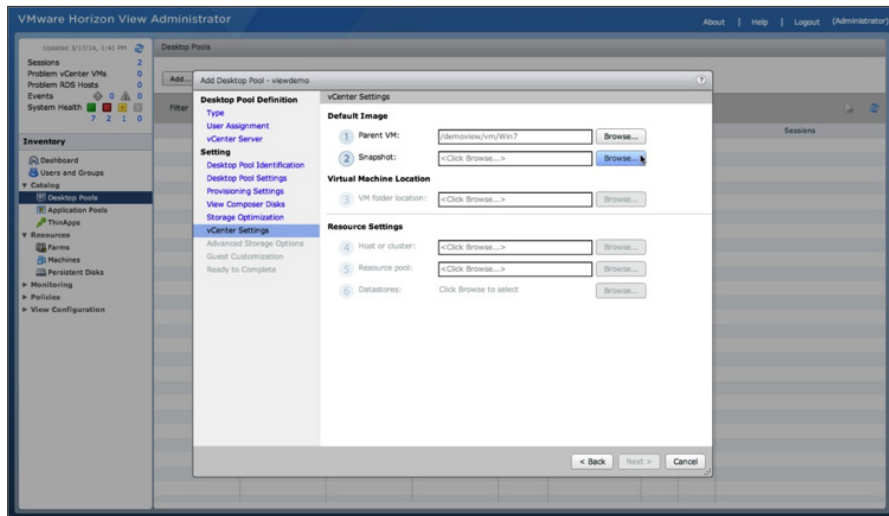
21. For the vCenter Settings:
 - a. Select your Windows 7 master image and associated options.
 - b. Next to the Parent VM text box, click **Browse**.



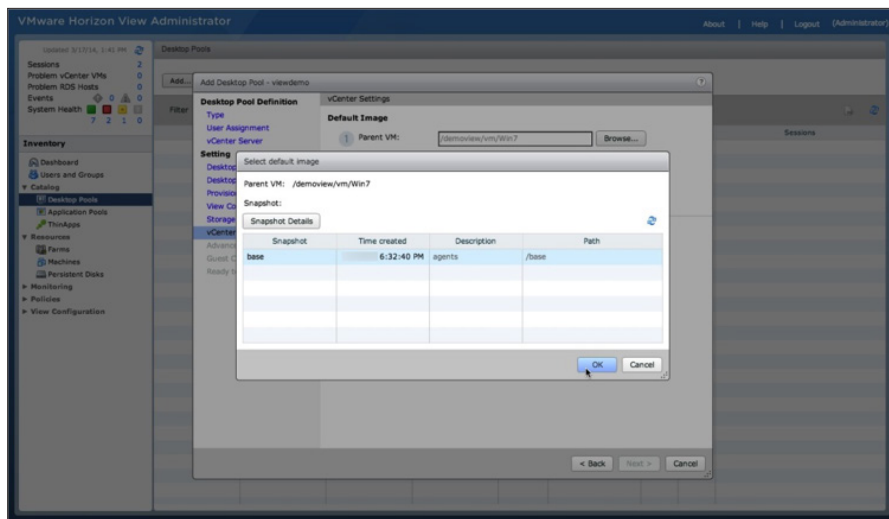
22. Select the Windows 7 virtual machine to use for the pool deployment, and click **OK**.



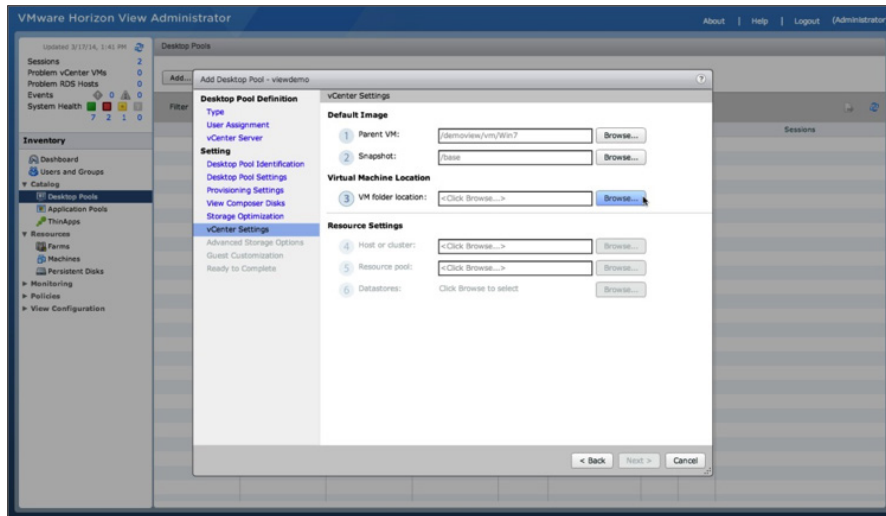
23. Next to the Snapshot text box, click **Browse**.



24. Select the snapshot to use for the pool deployment, and click **OK**.

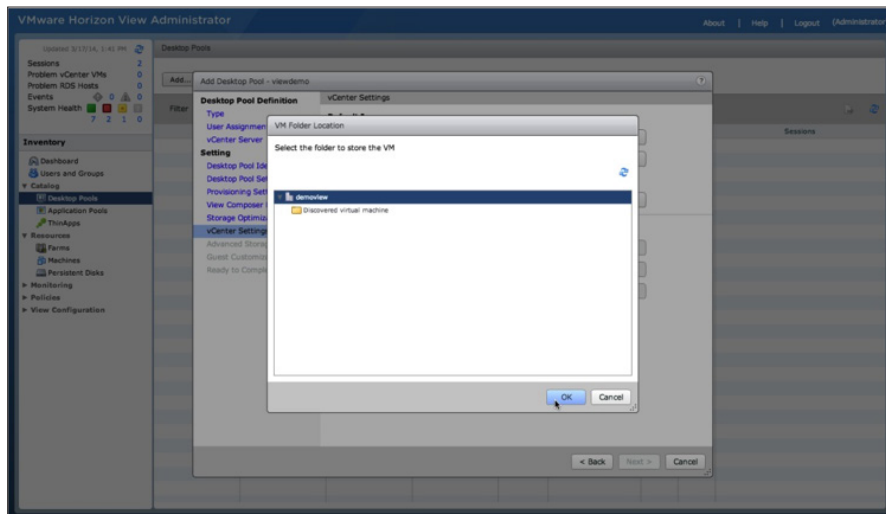


25. Next to the VM folder location text box, click **Browse**.

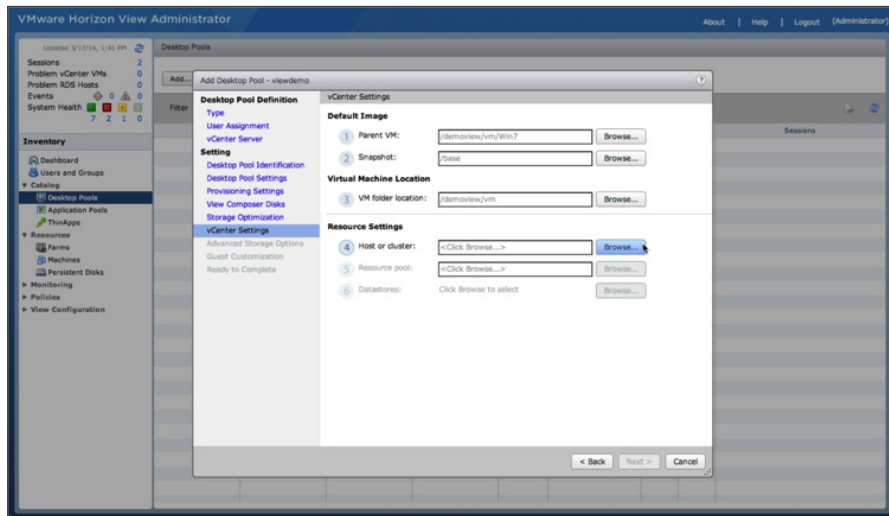


26. Select the folder location.

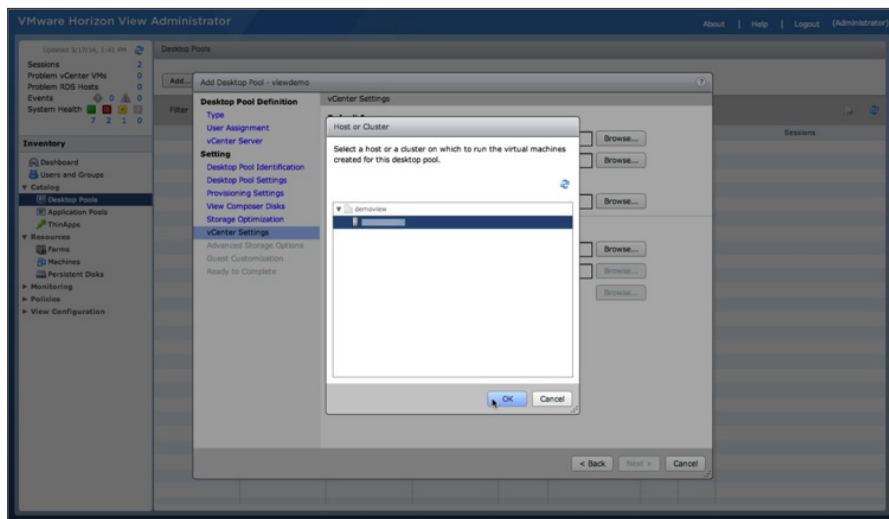
27. If you do not have a folder created, select the data center, and click **OK**.



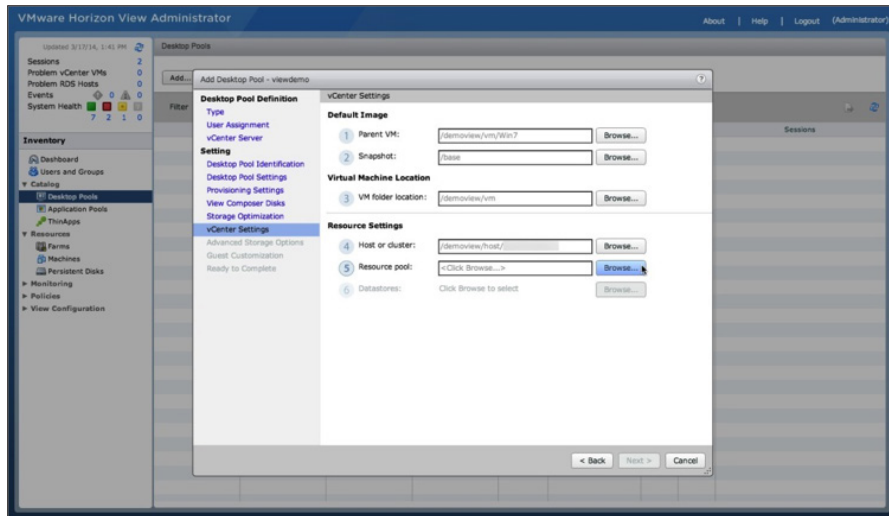
28. Next to the Host or cluster text box, click **Browse**.



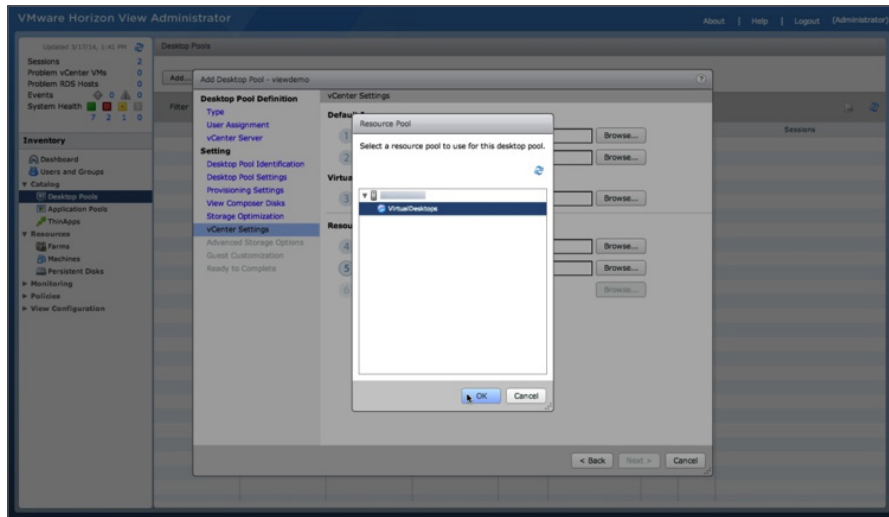
29. Select the target host or cluster for your pool desktop deployment, and click **OK**.



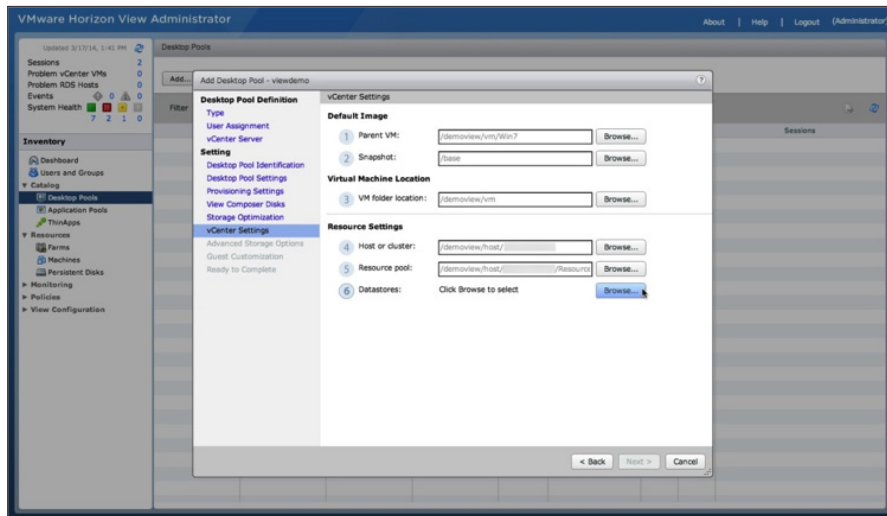
30. Next to the Resource pool text box, click **Browse**.



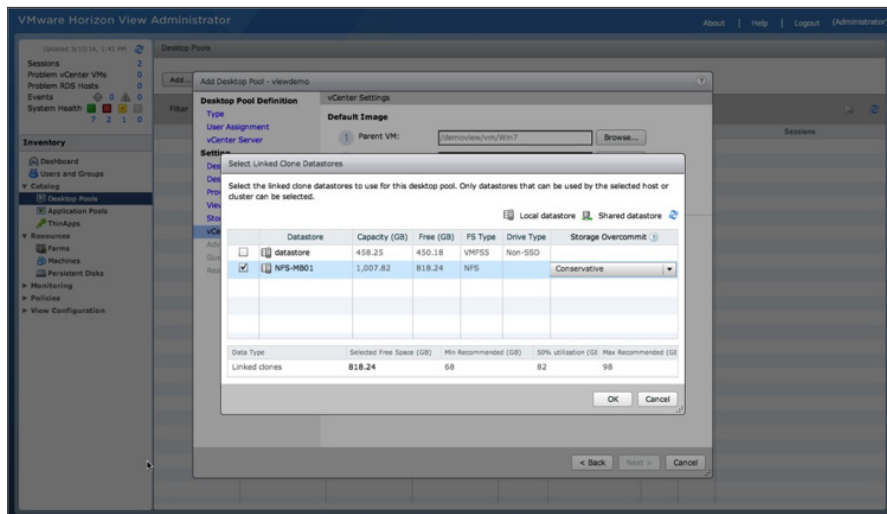
31. Select the resource pool to use, or select the host if you have not set up a resource pool, and click **OK**.



32. Next to the Datastores text box, click **Browse**.



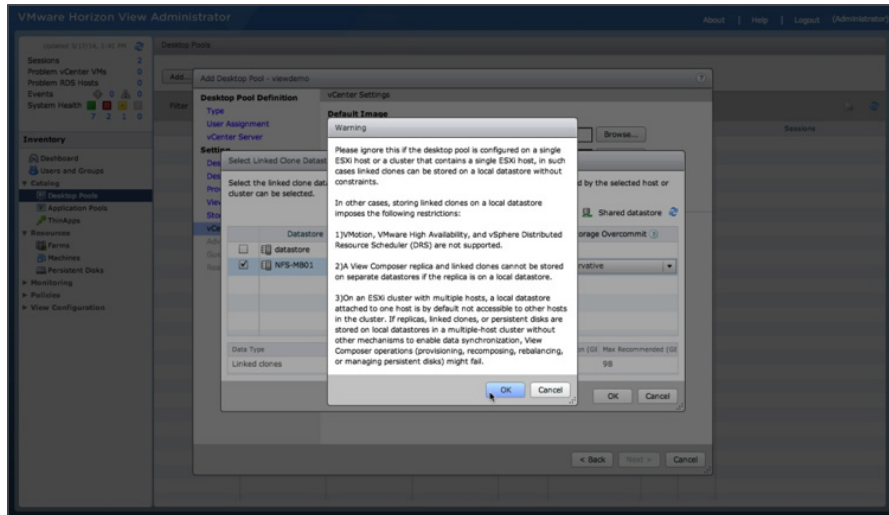
33. Select the target datastore to store your virtual desktops:
- Leave the Storage Overcommit setting as the default **Conservative**.
 - Click **OK**.



You receive a warning if you are storing your virtual desktops on a local datastore or are using only a single host.

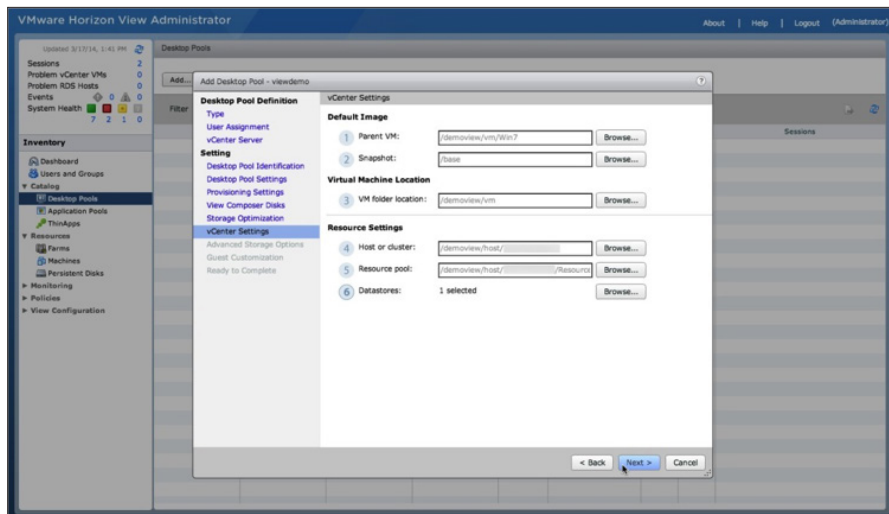
34. Ignore this warning because you are using a single host.

35. Click **OK** to continue.



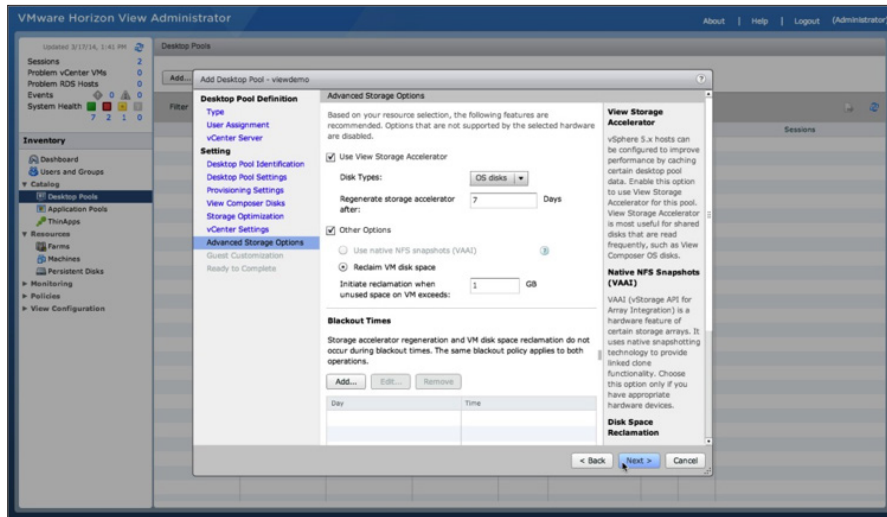
36. Review your vCenter Settings, and click **Next**.

To make changes, click **Back**.

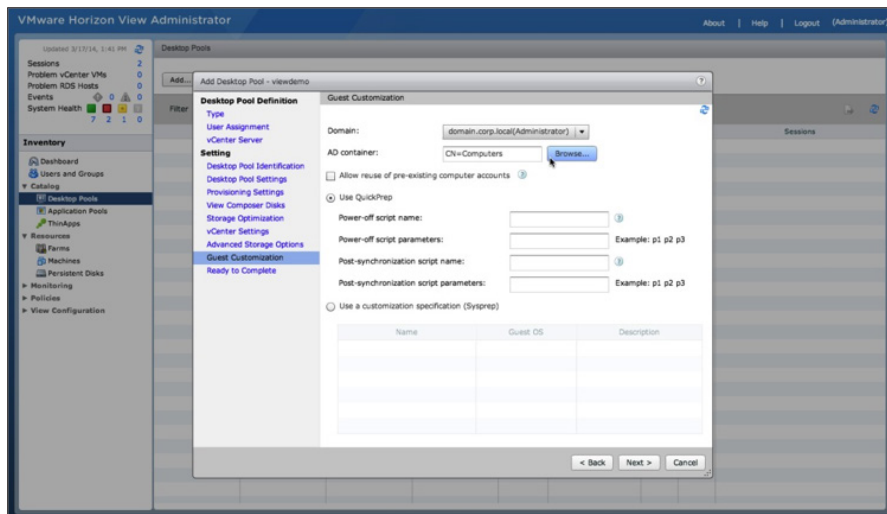


37. Adjust the Advanced Storage Options:

- Optionally select **Use View Storage Accelerator**.
- Select **Other Options** and then select **Reclaim VM disk space**.
- Specify the value for **Initiate reclamation when unused space on VM exceeds**.
The recommended value is 1 GB.
- Click **Next**.

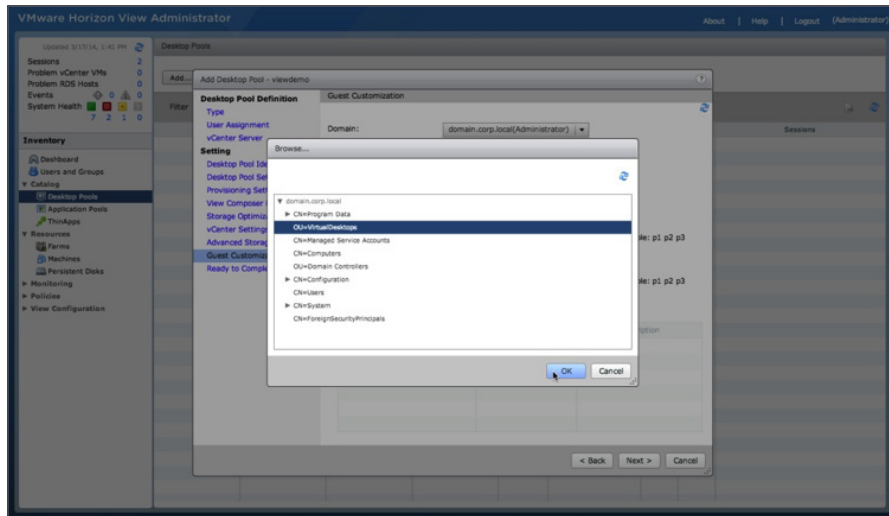


38. Adjust the **AD container** by clicking **Browse** next to the text box to view the available AD containers for the domain.



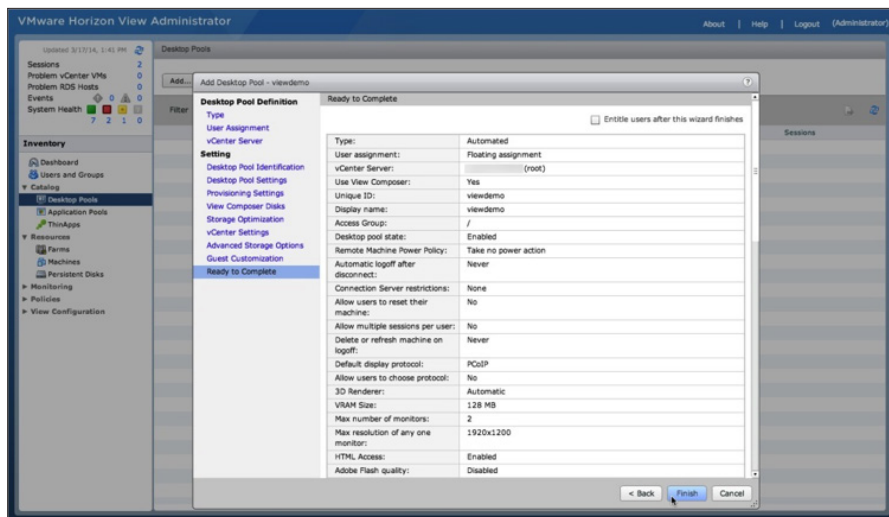
39. Select a valid OU or the default CN to store your View desktop computer account names, and click **OK**.

40. In the Guest Customization window, click **Next**.



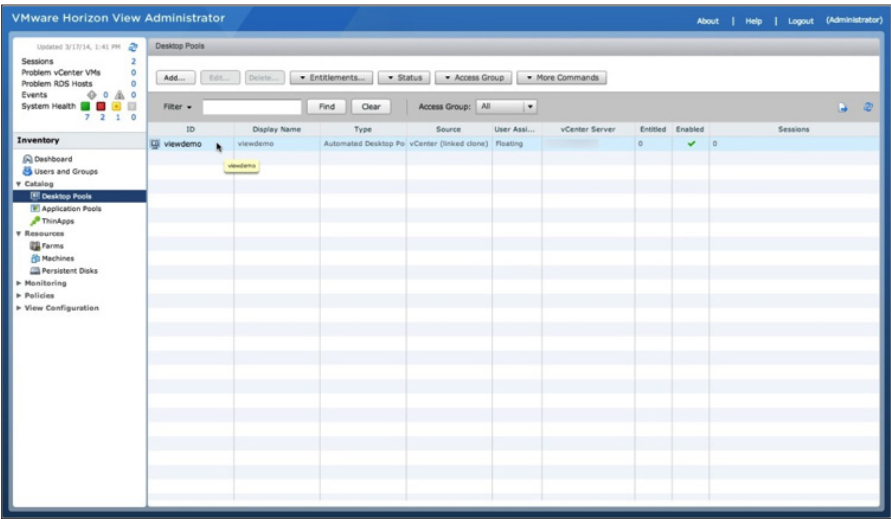
41. Review the summary of all your Desktop Pool Definition settings, and click **Finish** to deploy the pool.

To make changes, click **Back**.



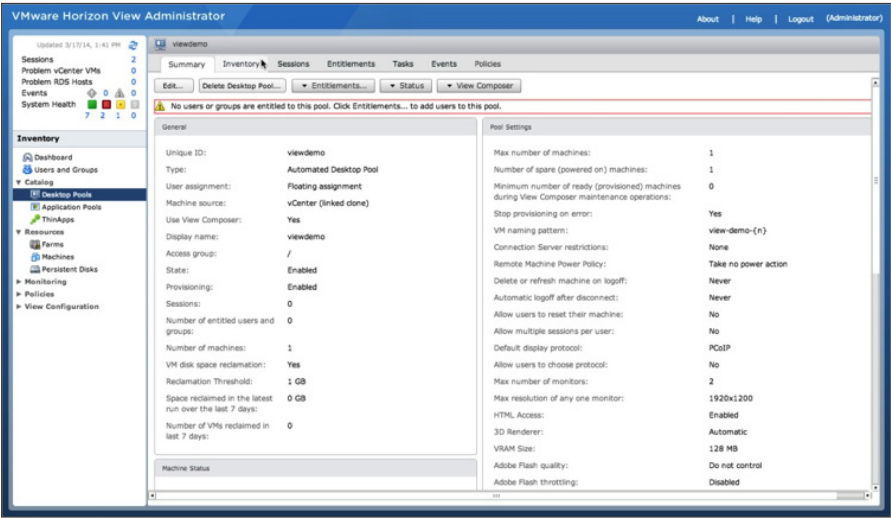
You return to the Desktop Pools inventory list.

42. Double-click your desktop pool to check the deployment status.



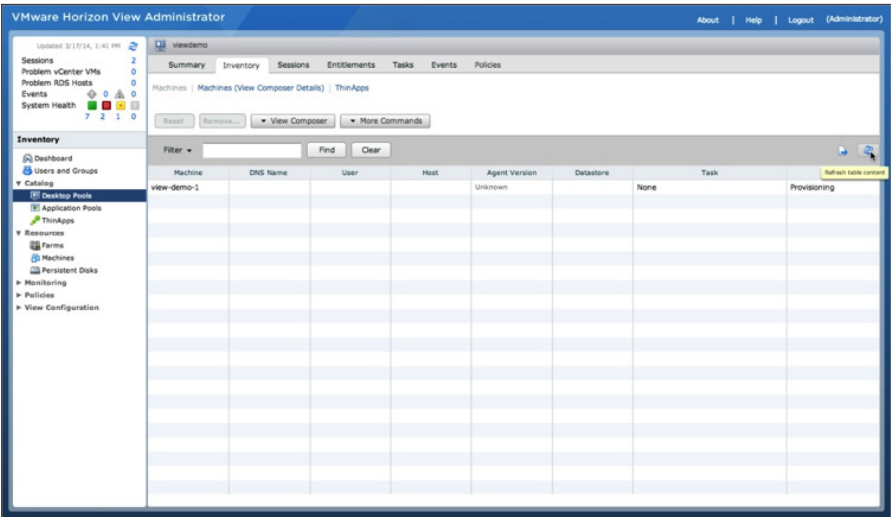
You return to the pool settings overview.

43. Click the **Inventory** tab to check the individual desktop deployment status.

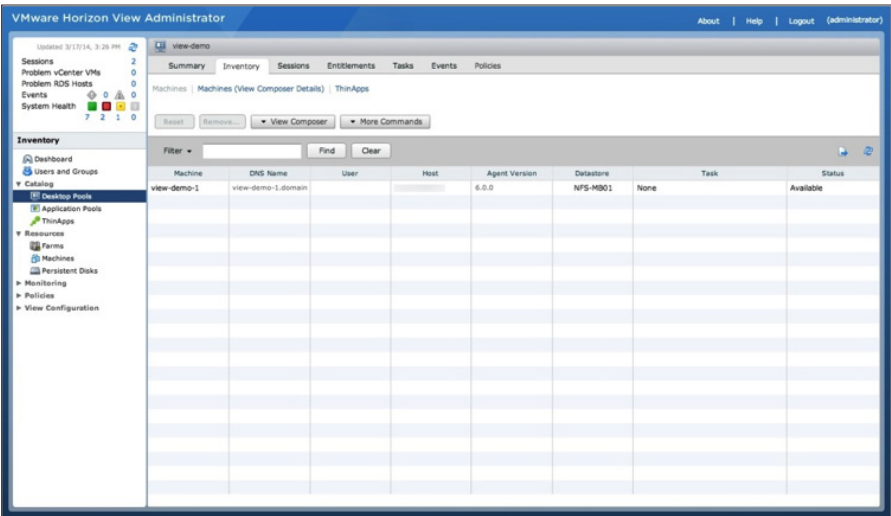


You can now monitor the deployment status for each desktop.

44. Click the **Refresh** icon to update the status.



When a desktop status changes to Available, it is ready to entitle and use. When all your desktops change to Available, your desktop pool has been successfully deployed.

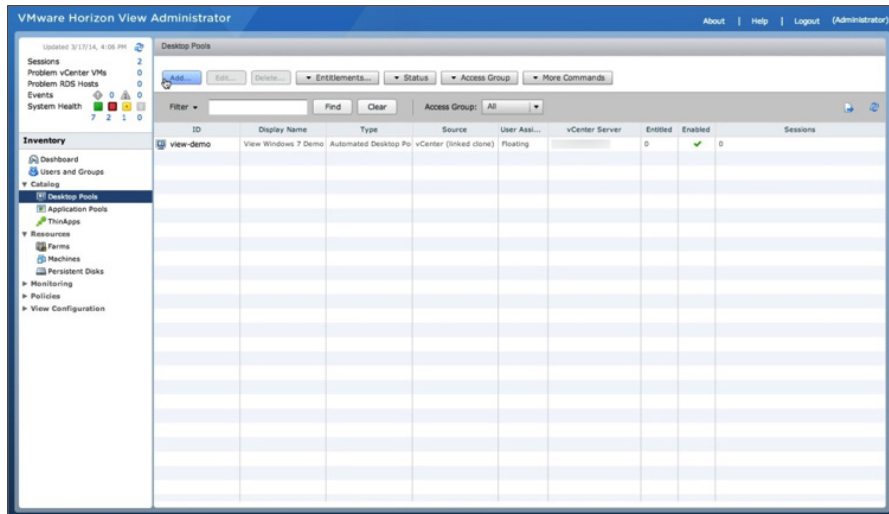


You have now created a linked-clone desktop pool. You can now proceed to deploy a full-clone desktop pool.

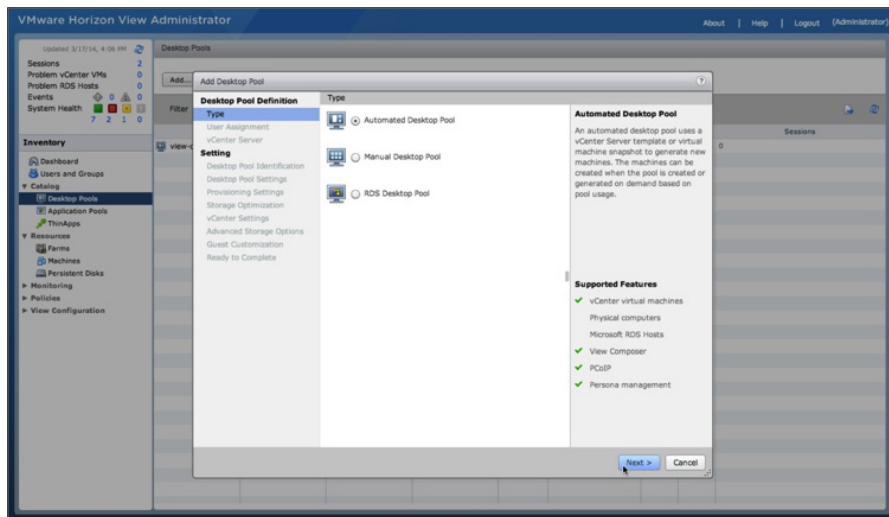
Deploy a Full-Clone Desktop Pool

You deploy a full-clone desktop pool based on the Windows Server 2008 R2 SP1 View master image that you created in earlier exercises.

1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To deploy a new pool, click **Add**.



3. In the Add Desktop Pool window, select **Automated Desktop Pool**, and click **Next**.



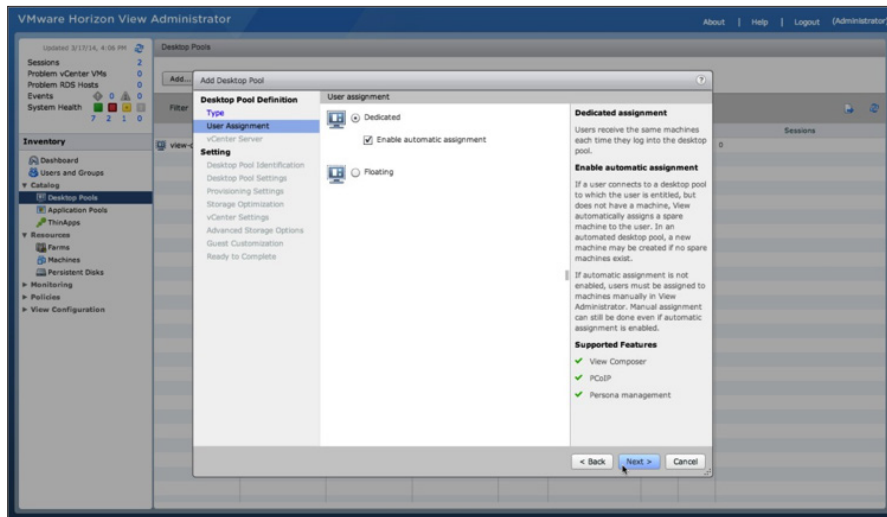
4. Specify the type of User assignment for the pool:

- a. Select
- Dedicated**
- .

You can also select **Floating**, but for this exercise, select **Dedicated**.

- b. (Optional) Select
- Enable automatic assignment**
- .

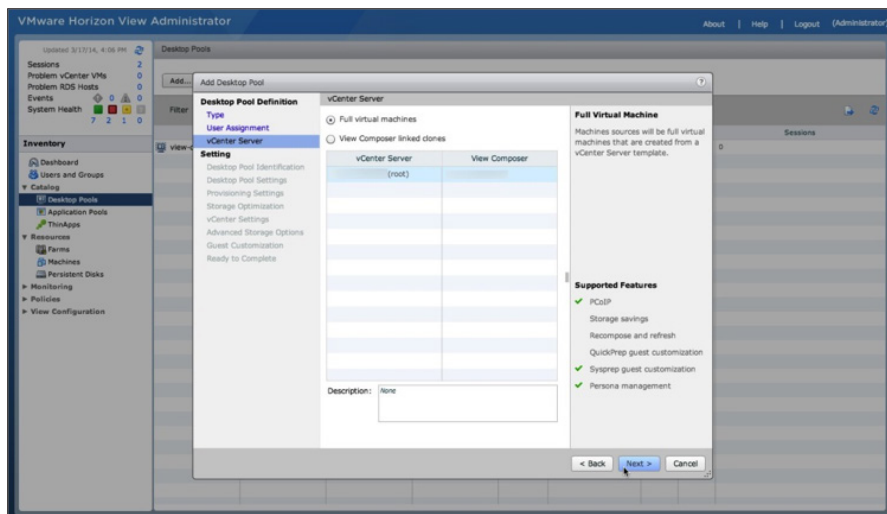
- c. Click
- Next**
- .



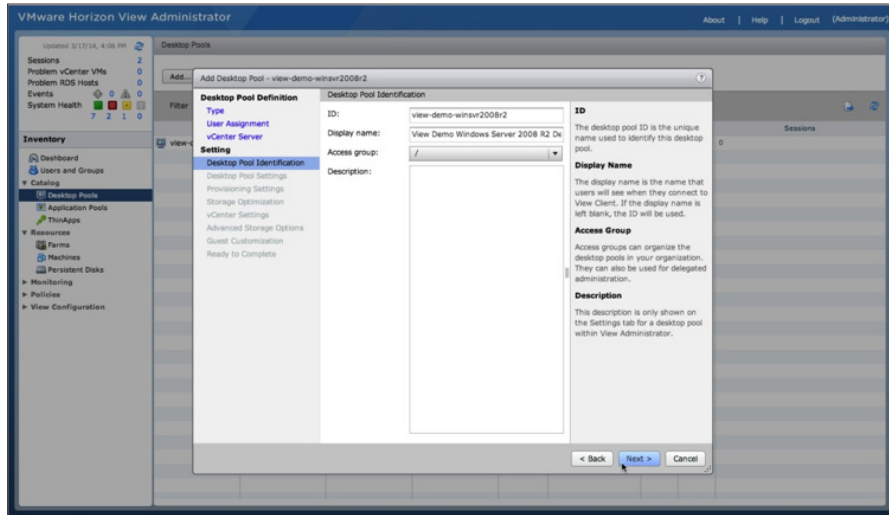
5. Select the type of virtual desktop to deploy:

- a. Select
- Full virtual machines**
- .

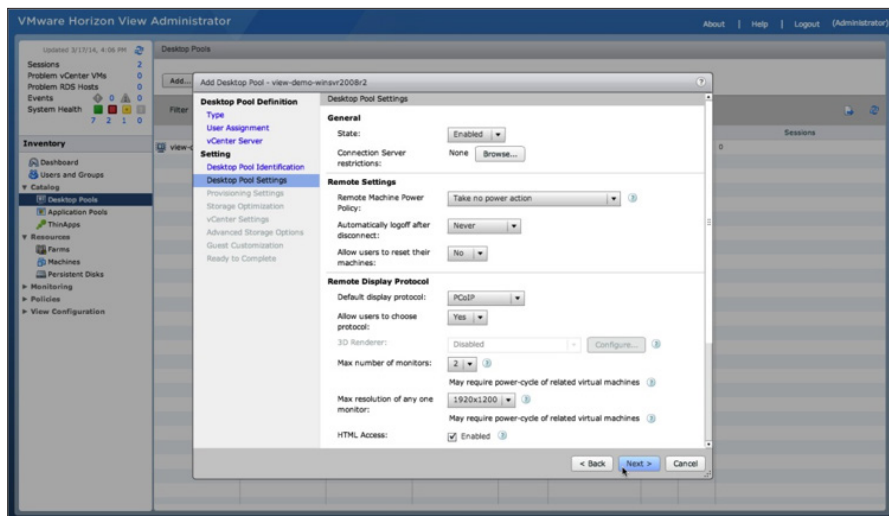
- b. Click
- Next**
- .



6. Add a pool **ID** and **Display name**.
7. Optionally, select a folder to organize your pools.
8. Click **Next**.



9. Scroll down the Desktop Pool Settings window to see the available options.
10. Make sure that **HTML Access** is enabled.
11. Click **Next**.



12. Adjust the Provisioning Settings:

- a. Select **Use a naming pattern** and in the **Naming Pattern** text box, enter a naming pattern.

A common pattern is **<poolname>-{n}**, which displays the poolname with an incremented desktop number as desktops in the pool are provisioned.

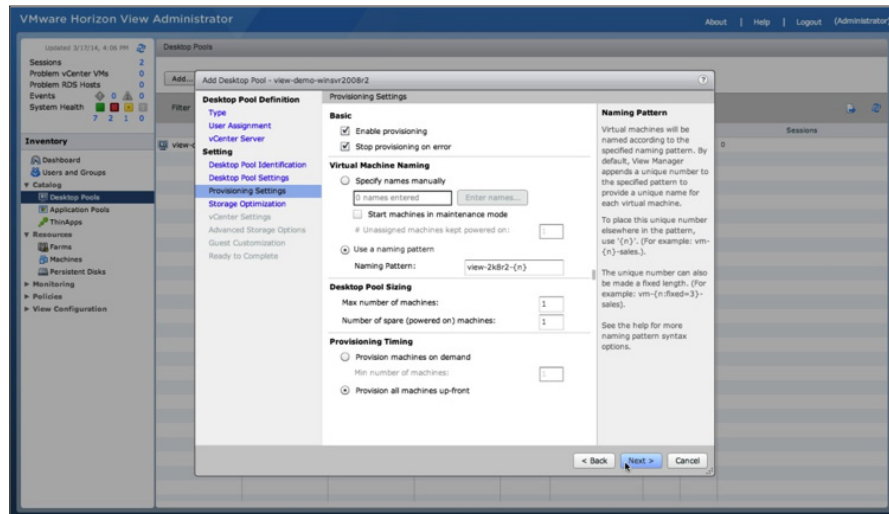
- b. Specify the maximum pool size:

- i. Deploy a small number of desktops to test your pool.
- ii. Increase the number of desktops after you have confirmed that your deployment is successful.

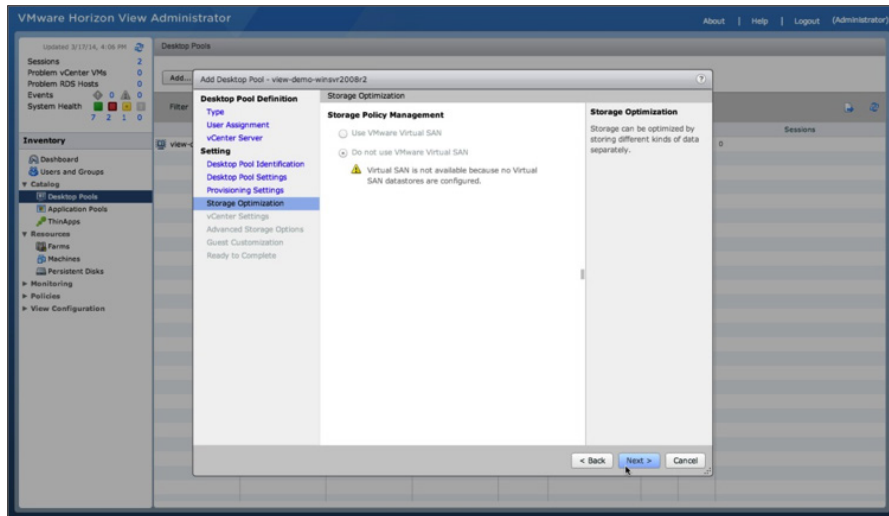
- c. Under Provisioning Timing, select **Provision all machines up-front**.

Alternatively, you could provision the desktops on demand and decide on the minimum number of desktops to have ready at initial pool deployment. Then you can provision any additional desktops as required, up to the maximum number of desktops. You can try these different pool features during subsequent pool deployments.

- d. Click **Next**.

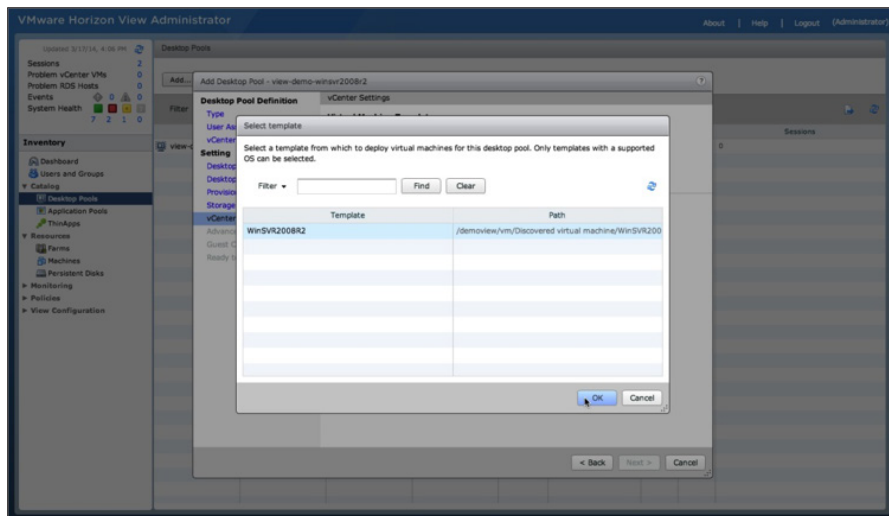


13. For the Storage Optimization settings, accept the defaults and click **Next**.

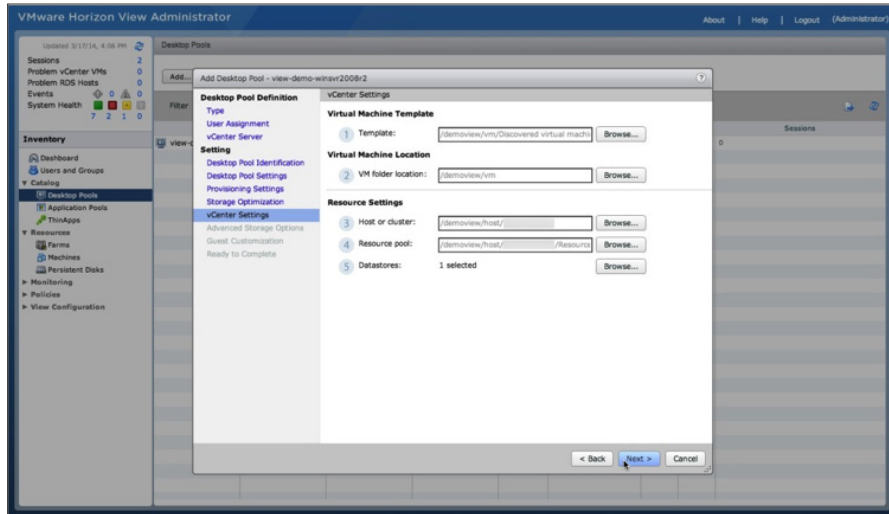


14. For the vCenter Settings, select the virtual machine master image to use by clicking **Browse** next to the **Template** text box.

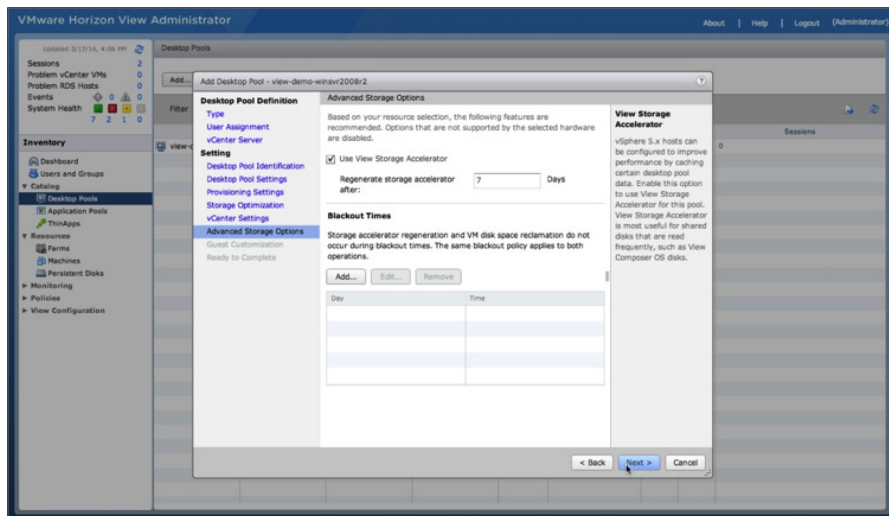
15. Select the Windows Server 2008 R2 SP1 View master image that you set up earlier and click **OK**.



16. Continue through the other vCenter Settings, selecting values for
 - a. VM folder location
 - b. Host or cluster
 - c. Resource pool
 - d. Datastores
17. Click **Next**.



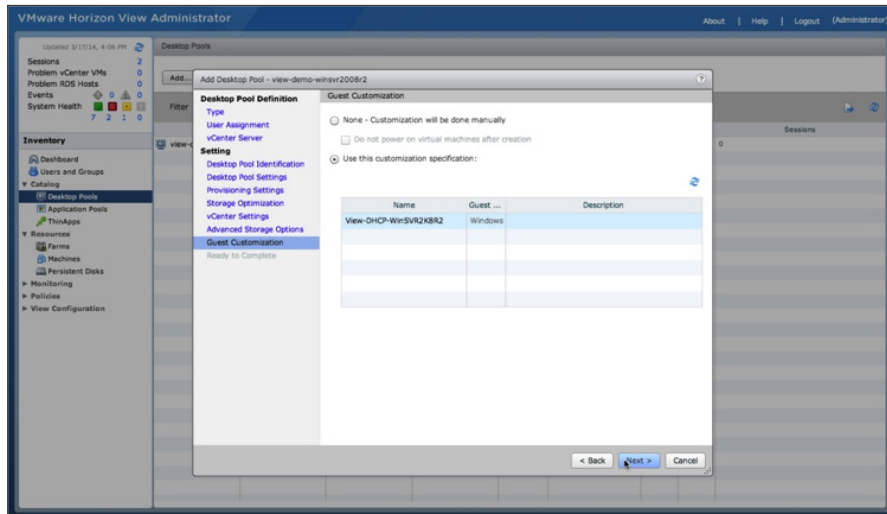
18. Adjust the Advanced Storage Options:
 - a. Optionally select **Use View Storage Accelerator**.
 - b. Click **Next** to continue.



19. For the Guest Customization options:

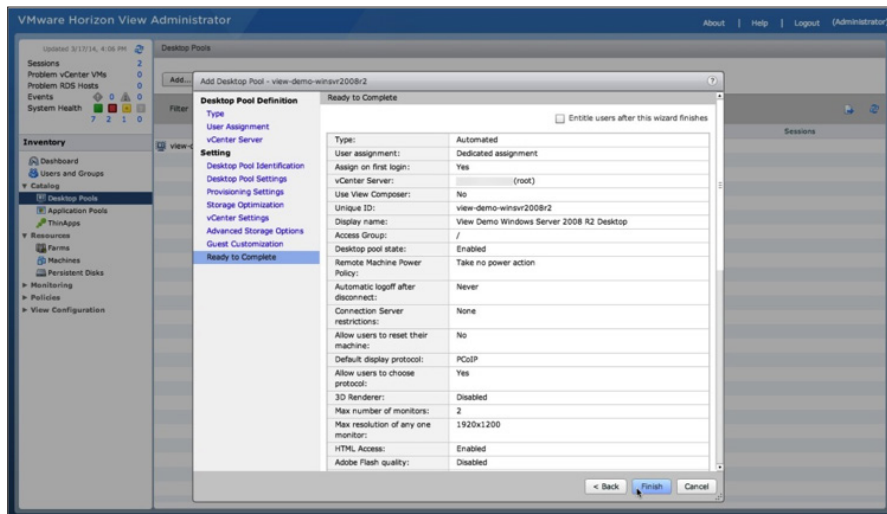
- Select **Use this customization specification**.
- Select the customization specification that you created to customize your Windows Server 2008 R2 SP1 View master image.

20. Click **Next**.



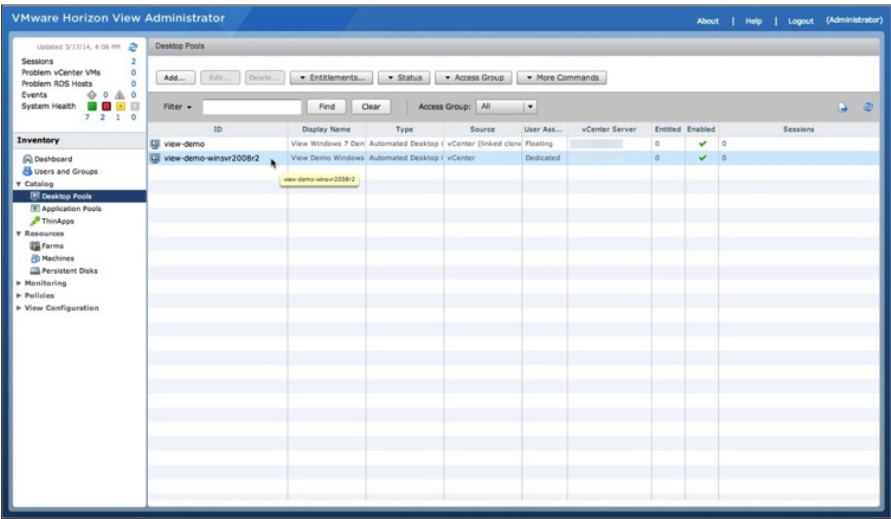
21. Review the summary of all your pool settings and click **Finish**.

To make changes, click **Back**.



You return to the pool inventory list.

22. Double-click your desktop pool to check the deployment status.

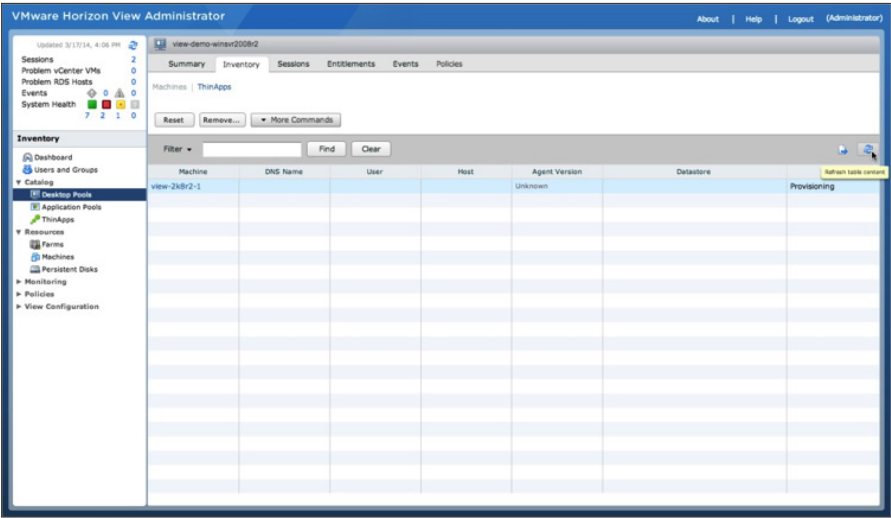


You return to the pool settings overview.

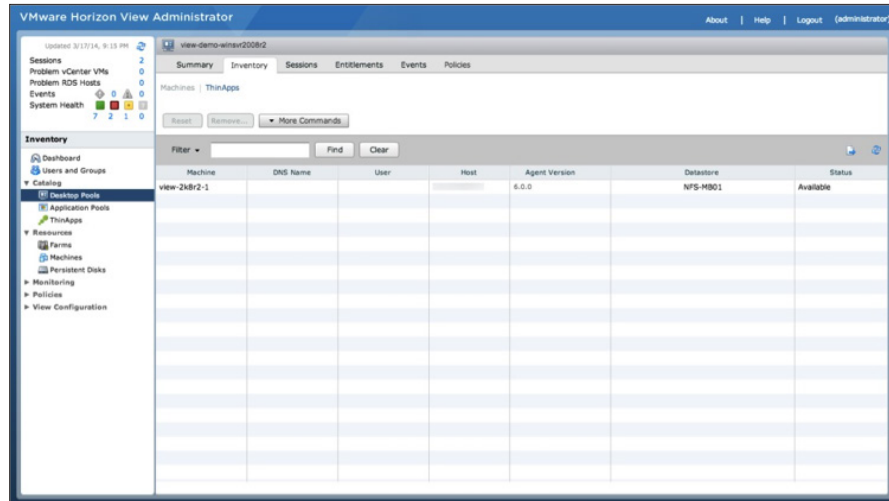
23. Click the **Inventory** tab to check the individual desktop deployment status.

You can monitor the deployment status for each desktop.

24. Click the **Refresh** icon to update the status.



When a desktop status changes to Available, it is ready to entitle and use. When all your desktops change to Available, your desktop pool has been successfully deployed.



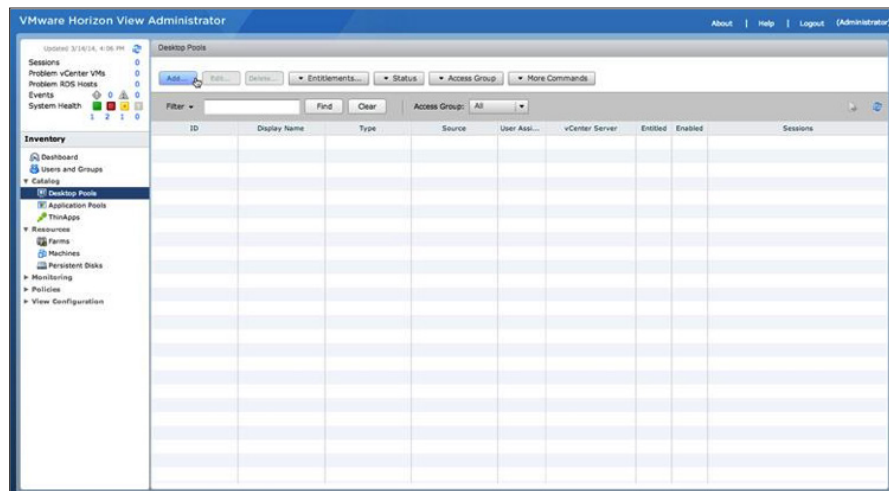
You have now deployed a full-clone desktop pool.

Deploy an RDSH Desktop Pool

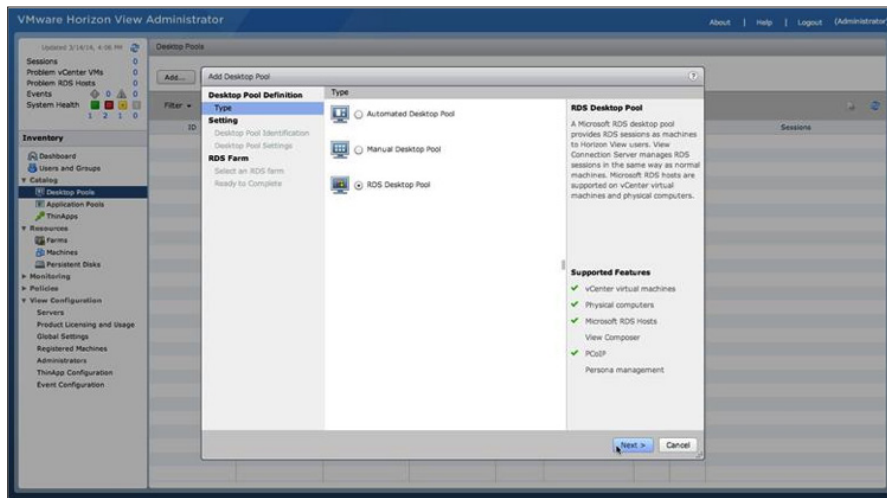
You will now deploy an RDSH desktop pool. In previous View releases, this was known as a Microsoft Terminal Services pool. An RDSH desktop pool has different characteristics compared to full-clone-based or linked-clone-based automated desktop pools. An RDSH desktop pool is based on a session to an RDSH server. An RDSH desktop supports both RDP and PCoIP display protocols.

To deploy an RDSH desktop pool, you will use the RDSH server that you set up and configured in previous exercises.

1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To create a new pool, click **Add**.



3. In the Add Desktop Pool window, select **RDS Desktop Pool**, and click **Next**.

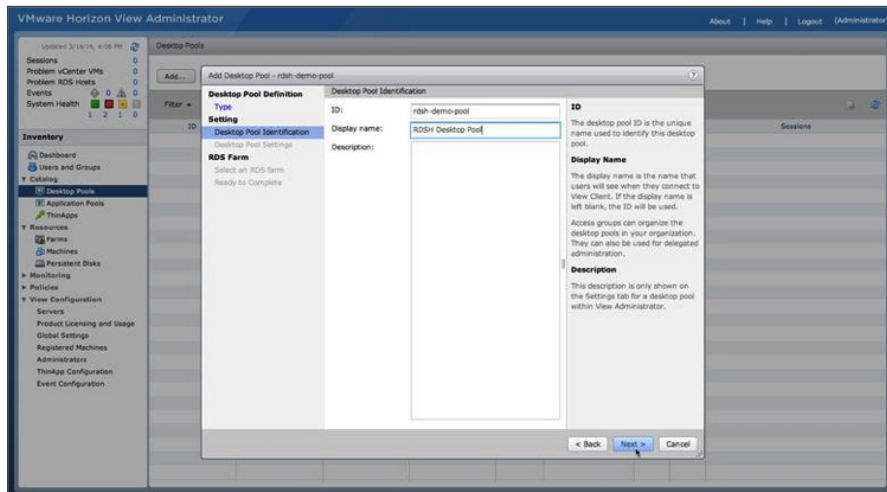


4. Give your desktop pool an **ID** and **Display name**.

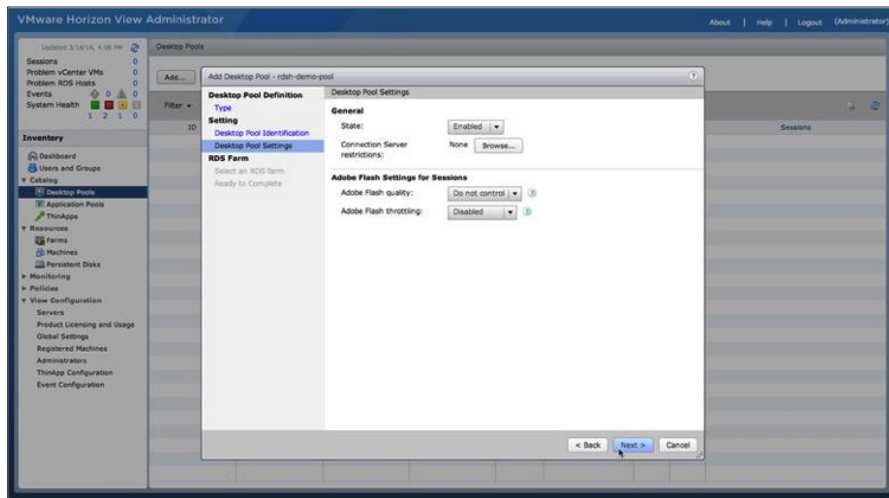
The **ID** is a unique name used to identify the desktop pool.

The **Display name** is the name that end users see when connecting to the desktop pool.

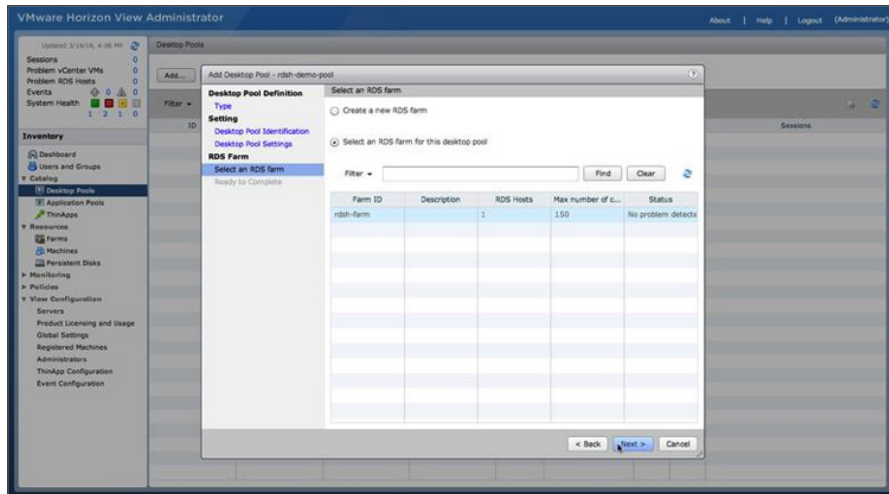
5. Click **Next**.



6. Adjust the Desktop Pool Settings or keep the default settings, and click **Next**.

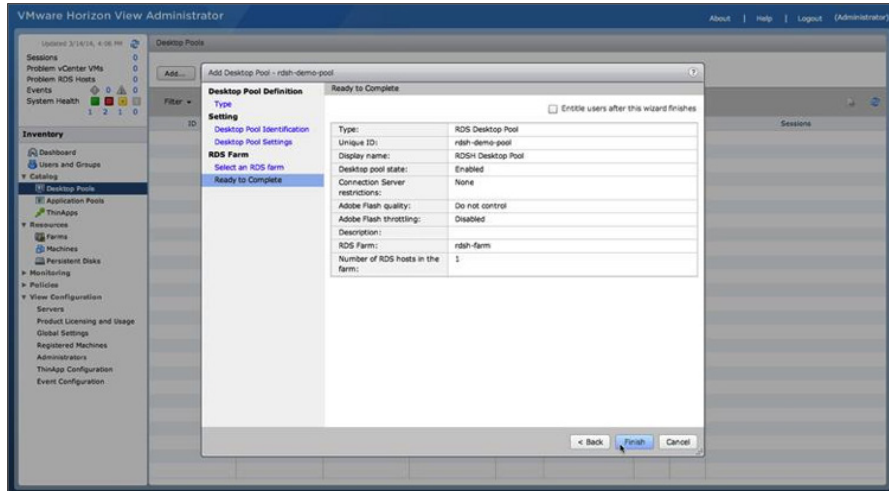


7. Select the **Select an RDS farm for the desktop pool** option and click **Next**.

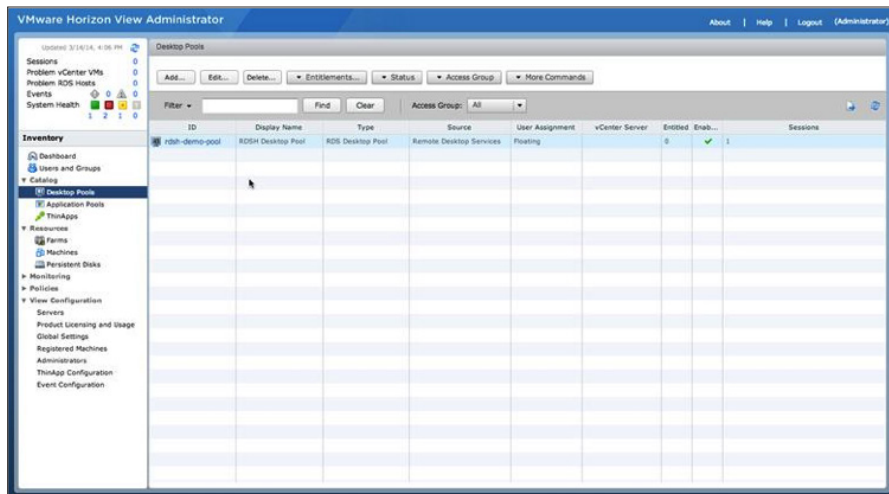


8. Review the RDSH Desktop Pool settings and click **Finish**.

To make changes, click **Back**.



You return to the Desktop Pools window, where the RDSH Desktop Pool that you just created is listed.

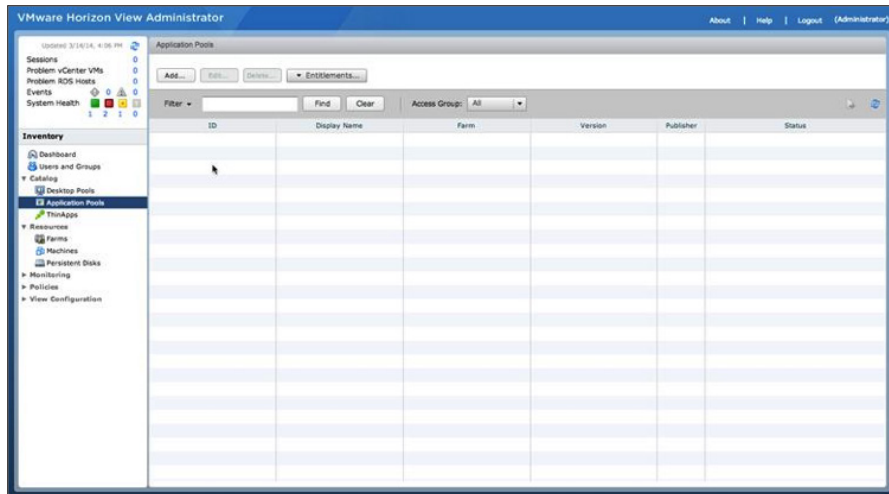


You have now deployed an RDSH desktop pool. In the next exercise, you deploy an RDSH-based application pool.

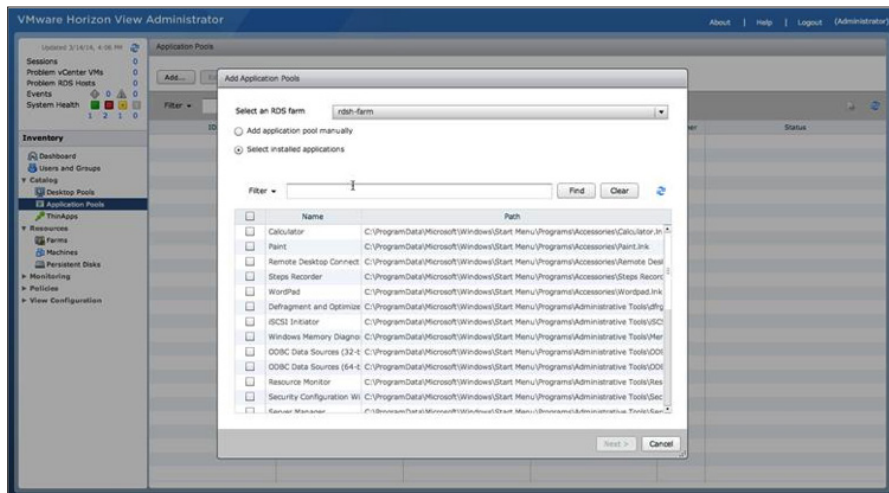
Deploy an Application Pool

An application pool lets you deliver a single application to many users. The application runs on a farm of RD Session Hosts.

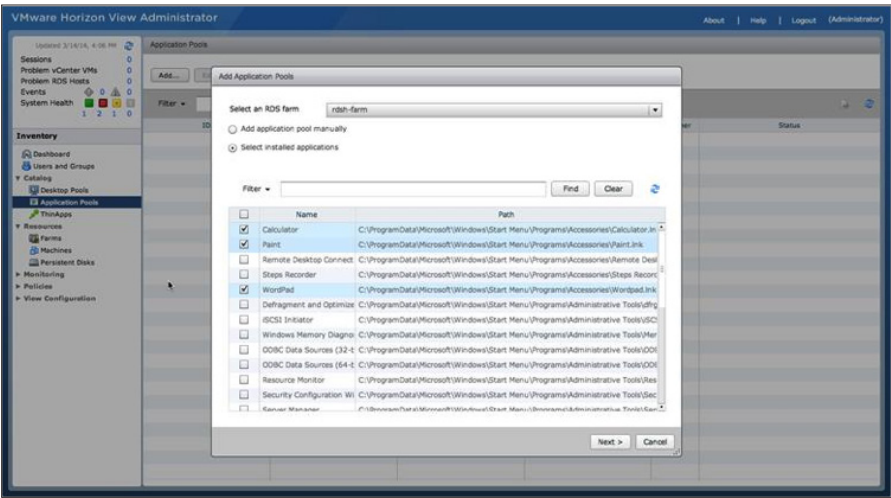
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To create a new application pool, select Application Pools, and click **Add**.



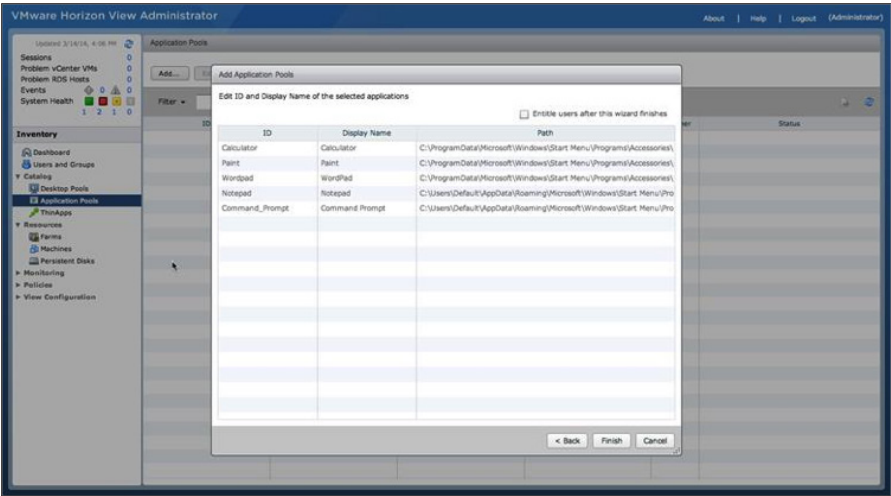
3. In the Add Application Pools wizard, you see a list of all the available applications that can be used to create an application pool.



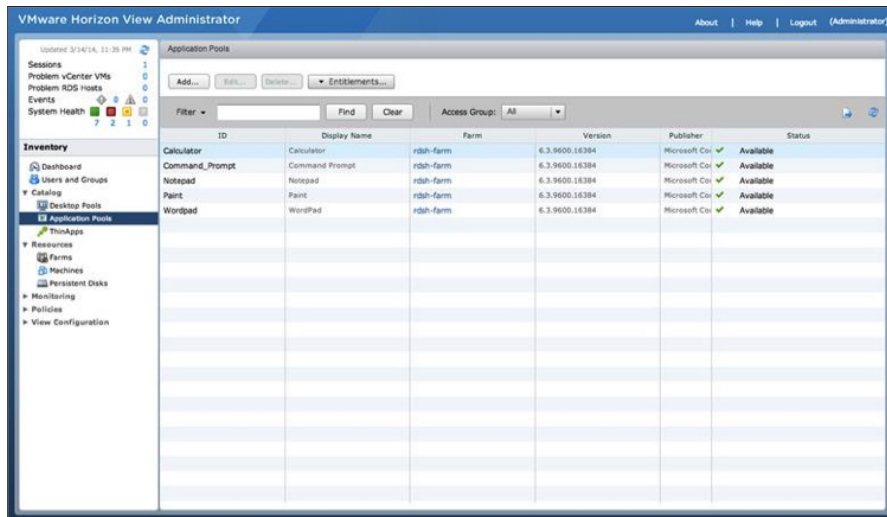
4. Select the applications that you want created as application pools, and click **Next**.



5. Edit the **ID** or **Display Name** of the selected applications and click **Finish**.



6. You return to the Application Pools window where you see all the applications that you selected.



You have now created an application pool.

Entitling Users to View Desktops and Applications

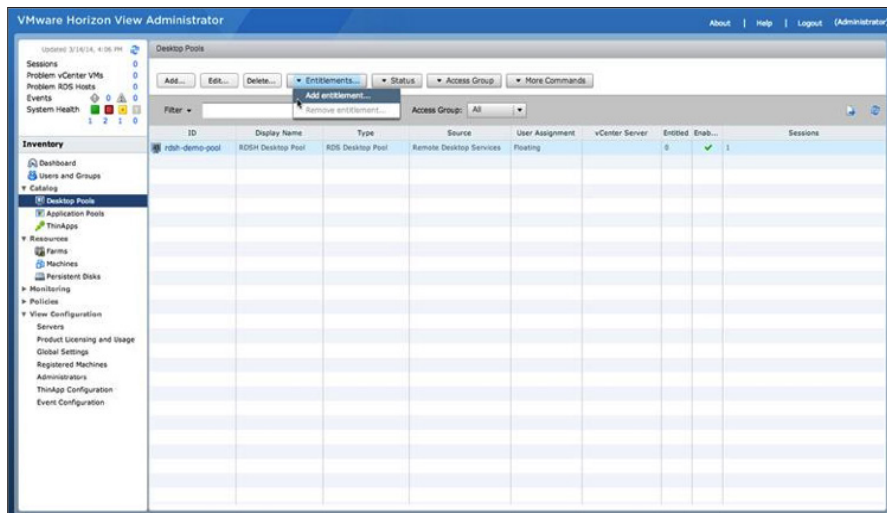
Now that you have deployed three different desktop pools, you are ready to entitle users to them.

- [Entitle Users to a Desktop Pool](#)
- [Entitle Users to an Application Pool](#)

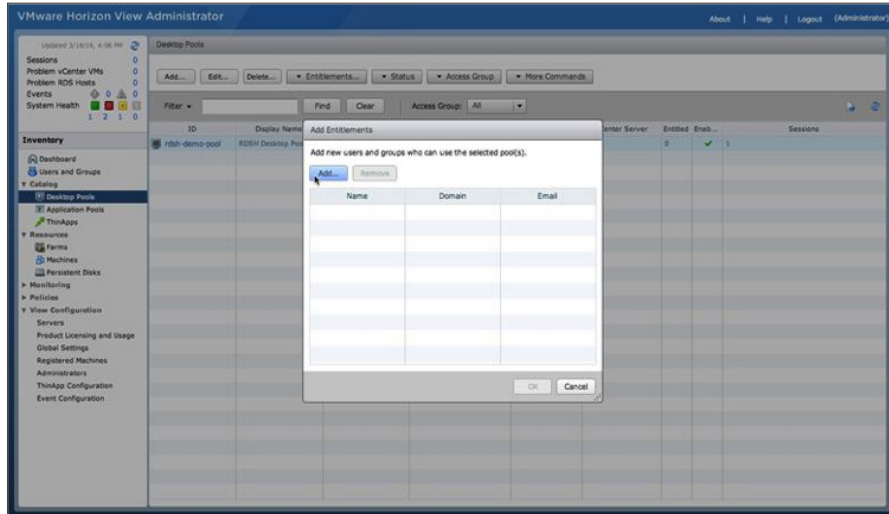
Entitle Users to a Desktop Pool

This exercise shows you how to entitle users to one desktop pool. You can repeat the exercise to entitle users to additional desktop pools.

1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. Click the desktop pool that you want to entitle.
3. Click the **Entitlements** tab and then click **Add entitlement**.



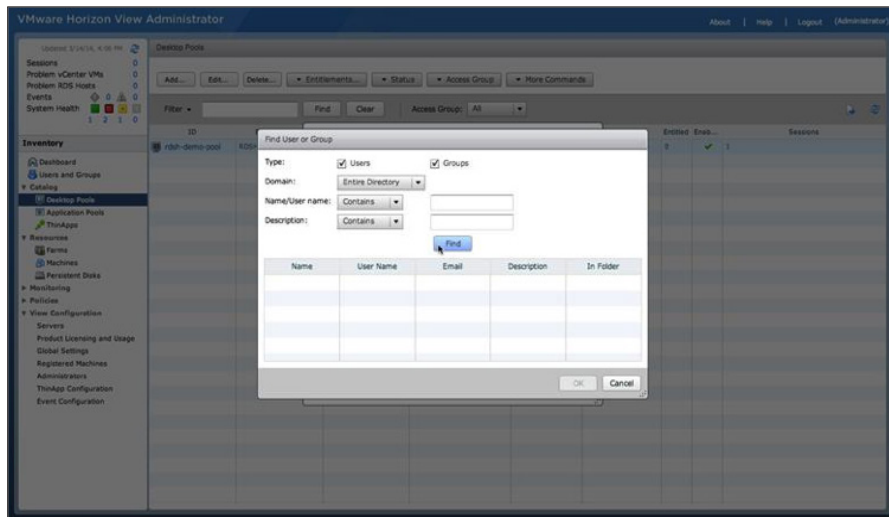
4. The Add Entitlements dialog box lists the pool's entitled users and groups.
5. Click **Add** to entitle new users or groups to the desktop pool.



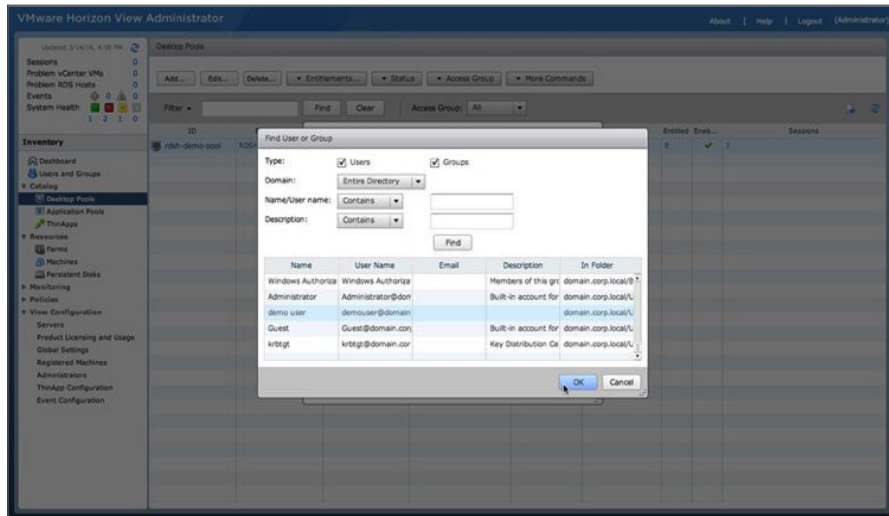
6. In the Find User or Group dialog box, search your domain controller for users or groups to entitle to this desktop pool.

You can narrow your query using the drop-down menus to add search terms and modifiers.

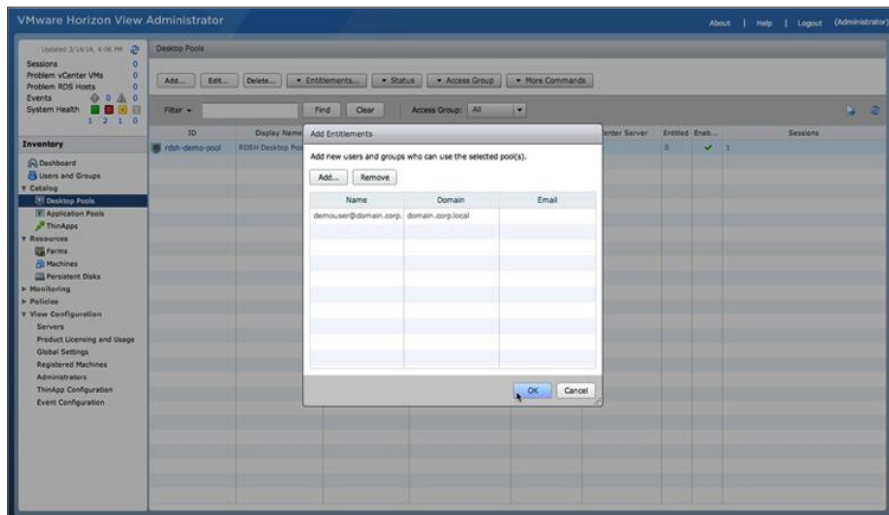
7. Click **Find**.



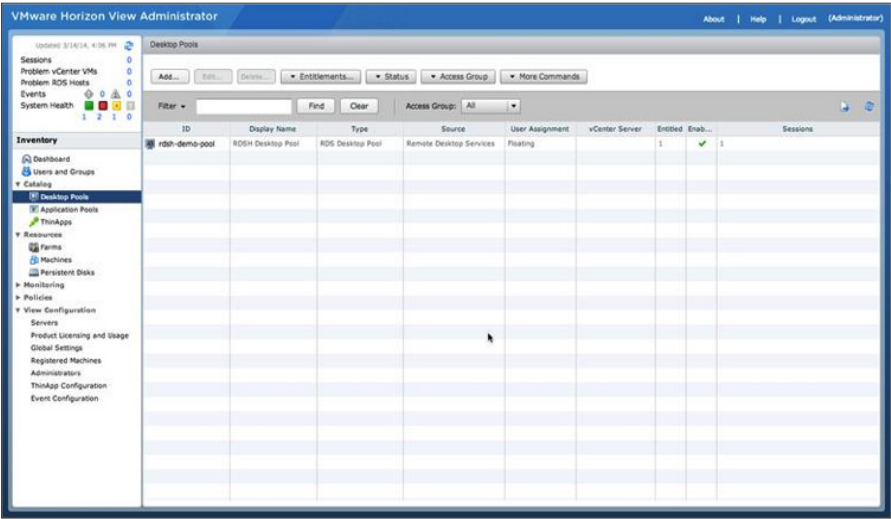
8. Scroll through the results to select all the users or groups to entitle, and click **OK**.



9. Review the summary of users that you have selected.
You can add more users or groups, or remove them from the entitlement list.
10. When you are done, click **OK**.
The users or groups are now entitled to this desktop pool.



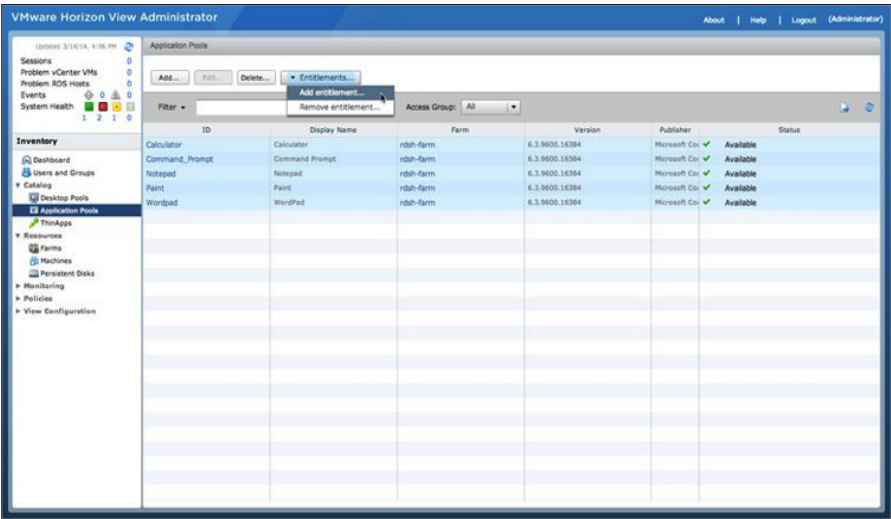
11. Verify the total number of entitlements for the pool in the **Entitled** column.



Repeat these steps to entitle other users or groups to the rest of your desktop pools or to reverse their entitlements. Proceed to the next exercise to entitle users to application pools.

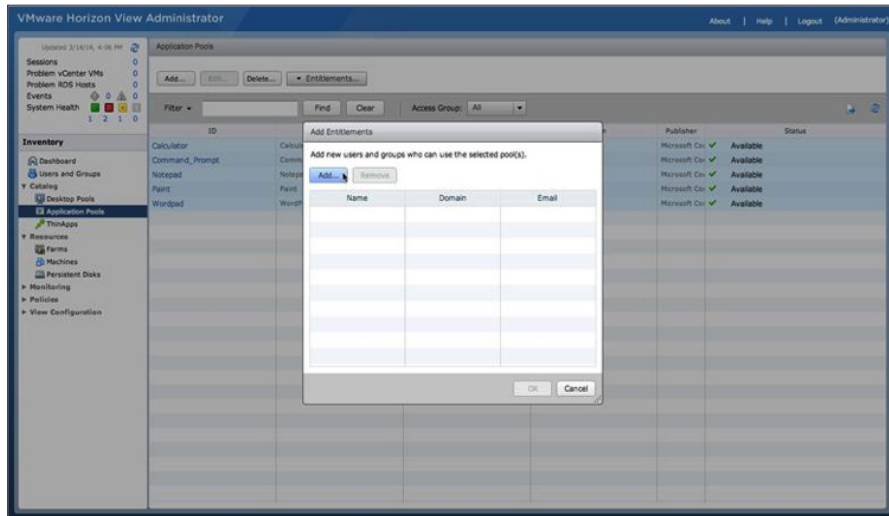
Entitle Users to an Application Pool

- 1. Log in to the View Administrator console, and navigate to **Catalog > Application Pools** to see a list of all your application pools.
- 2. Click the application pool or select multiple application pools to entitle.
- 3. Click the **Entitlements** tab, and click **Add entitlement**.



- 2. The Add Entitlements dialog box lists the pool's entitled users and groups.

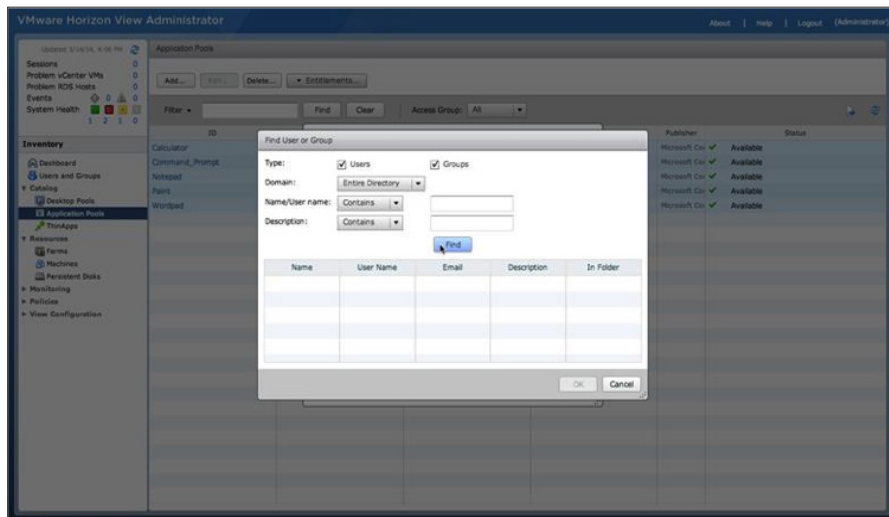
- Click **Add** to entitle new users or groups to the application pool.



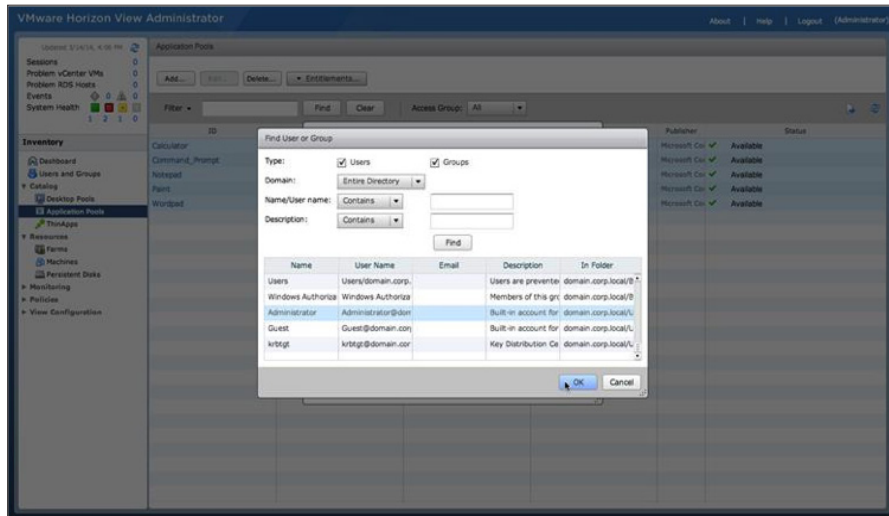
- In the Find User or Group dialog box, search your domain controller for users or groups to entitle to this application pool.

You can narrow your query using the drop-down menus to add search terms and modifiers.

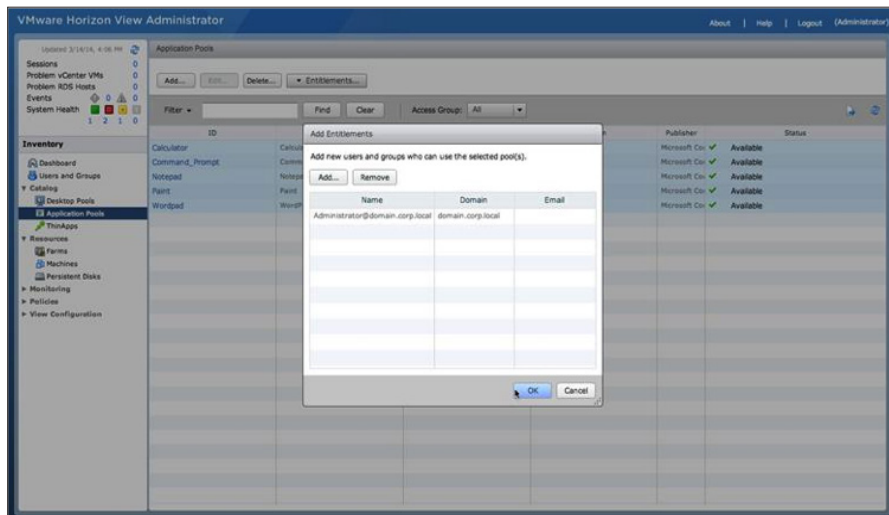
- Click **Find**.



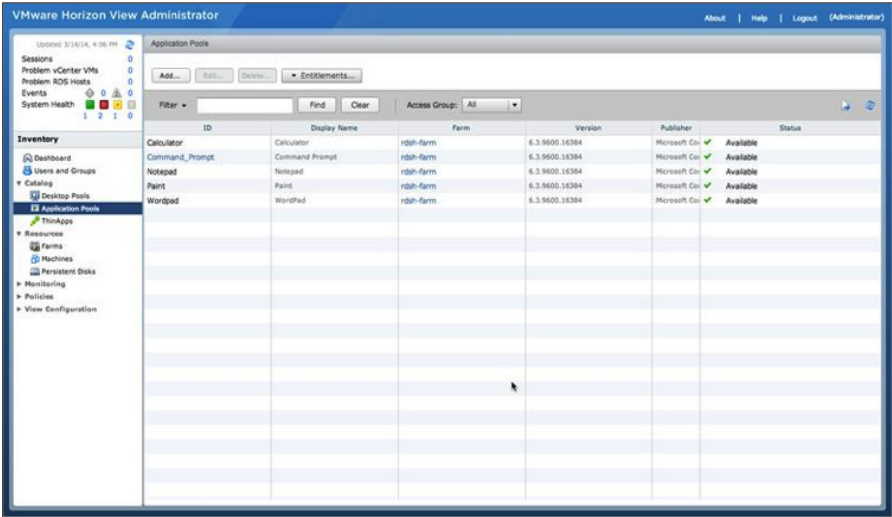
6. Scroll through the results to select all the users or groups to entitle, and then click **OK**.



7. Review the summary of users that you have selected.
You can add more users or groups or remove them from the entitlement list.
8. When you are done, click **OK**.
The users or groups are now entitled to this application pool.



You are returned to the Application Pools window. You can repeat these steps to entitle additional users or groups or reverse their entitlements.



This completes this series of exercises. You are ready to proceed to the exercises using Horizon Clients to connect to View desktops and applications.

Connecting to View Desktops and Applications

After you have finished deploying View desktops, you are ready to explore end-user connection options. This series of exercises starts by walking you through the process of connecting to View desktops using different Horizon Clients, including HTML access and mobile clients.

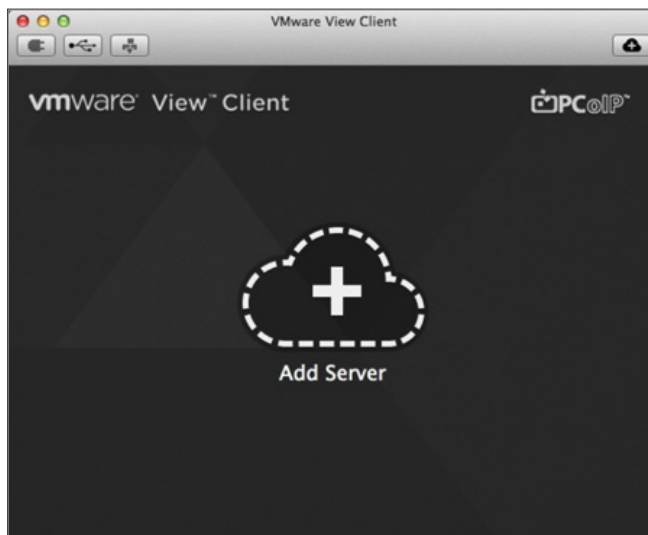
- [Connect to View Desktops Using Horizon Client](#)
- [Connect to View Desktops Using HTML Access](#)
- [Connect to View Desktops from a Mobile Horizon Client](#)
- [Connect to an Application Using the Horizon Client](#)

A prerequisite for these exercises is to install Horizon Clients on your end-user computers and devices.

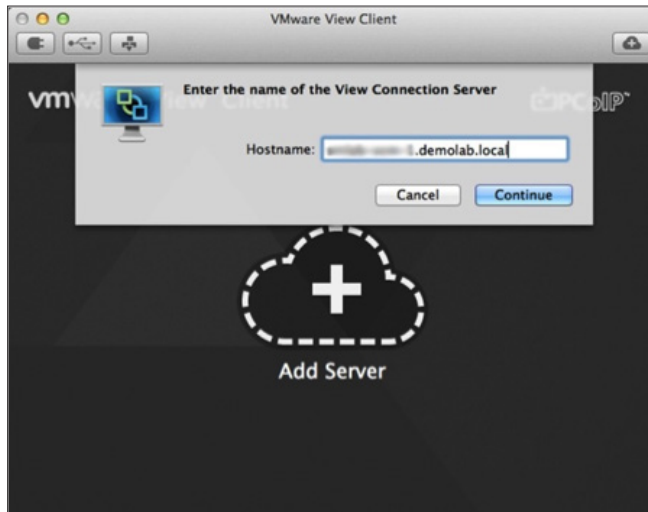
Connect to View Desktops Using Horizon Client

This exercise guides you through using Horizon Client on an endpoint, either Windows or Mac OS.

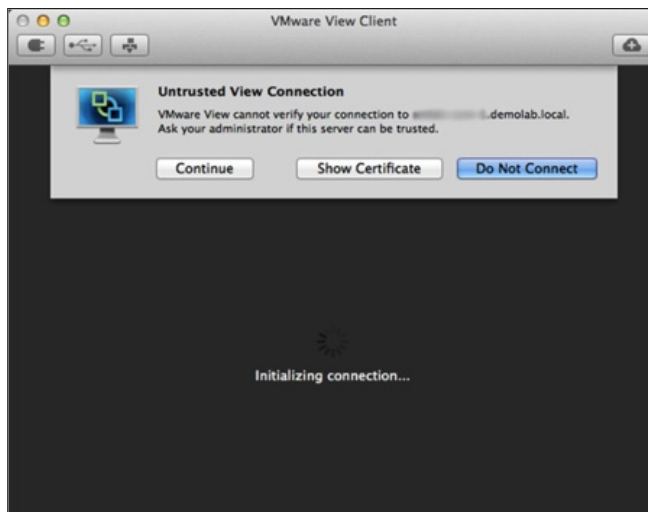
1. On your endpoint device, install Horizon Client.
2. On your target client, launch Horizon Client, and click **Add Server**.



3. In the **Hostname** text box, enter the fully qualified domain name of your View Connection Server, and click **Continue**.

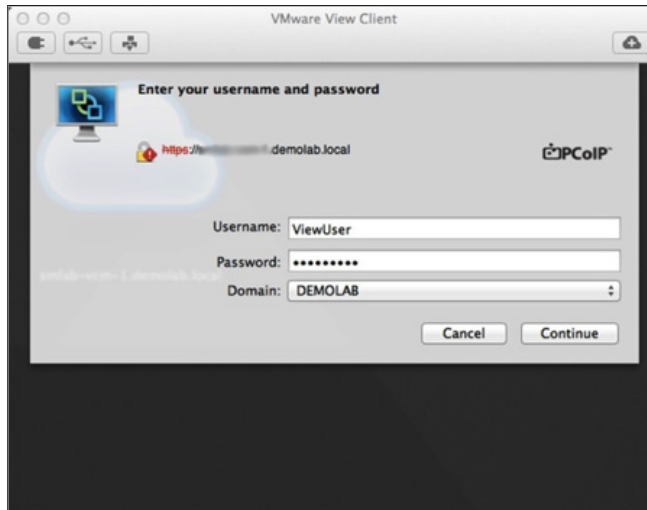


4. If you are using the default self-signed SSL certificate, do the following with the Untrusted View Connection warning:
 - a. To ensure the certificate is valid, click **Show Certificate**.
 - b. To proceed, click **Continue**.

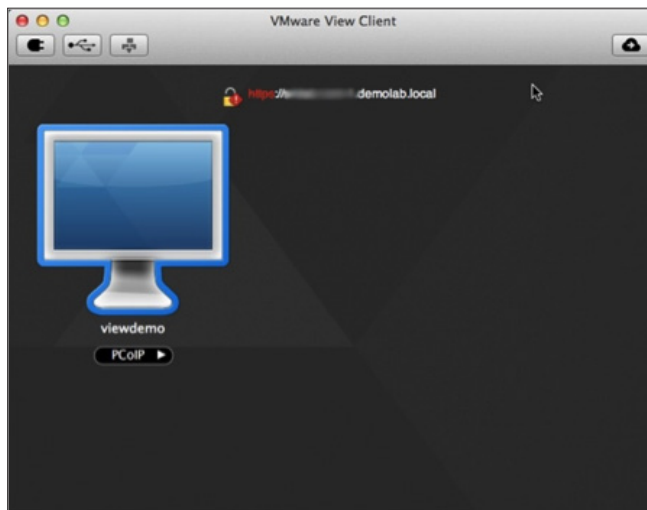


5. Enter your user credentials in the **Username** and **Password** text boxes, and click **Continue**.

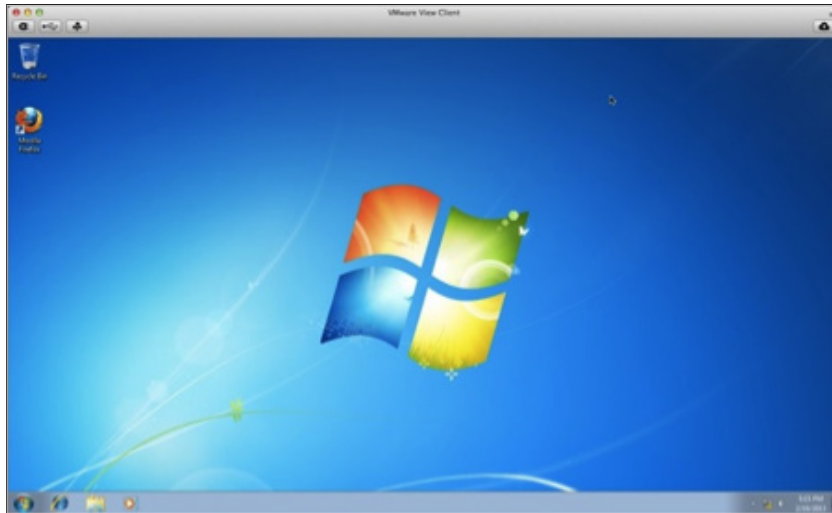
Note: You must be entitled to a desktop pool or specific desktop to access it.



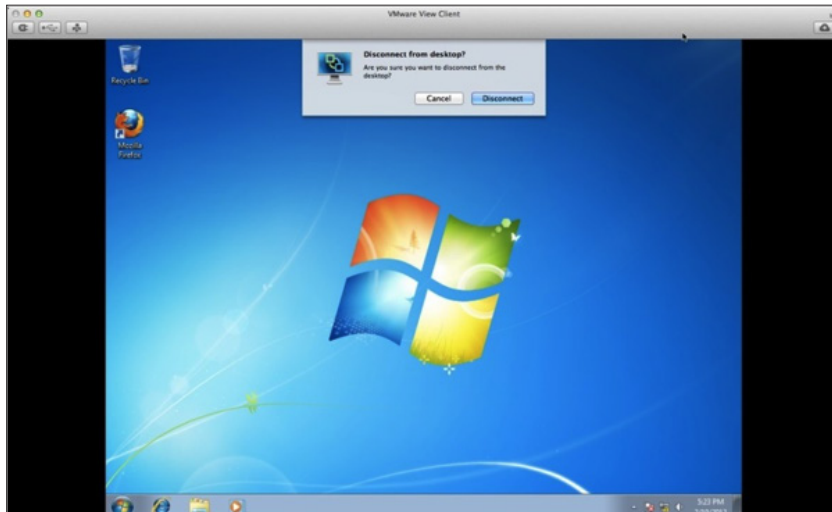
6. From the group of desktops available to your credentials, click the desktop to connect to.



7. Verify that you have successfully connected to your View desktop.



8. When you are ready to end your View desktop session, click the **Disconnect** icon at the top left of the View Client menu bar, and click **Disconnect**.



You have now used Horizon Client to launch and disconnect from View desktop sessions. Proceed to the next exercise to connect using HTML access.

Connect to View Desktops Using HTML Access

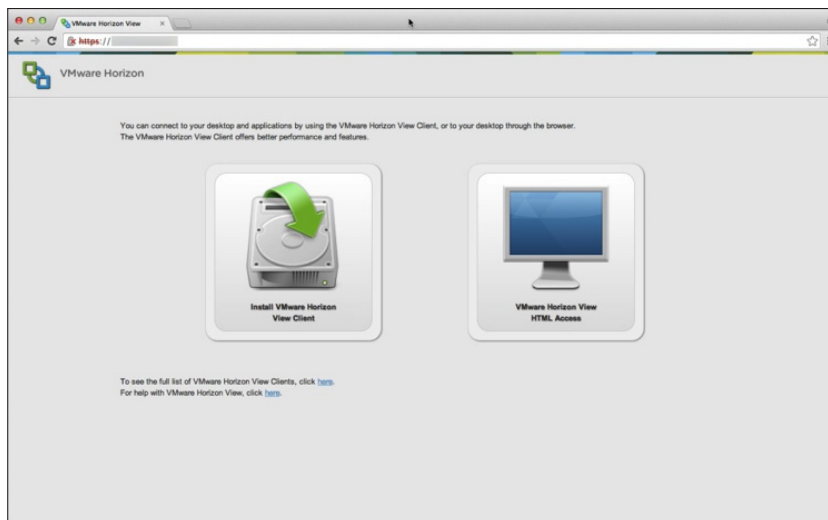
You can connect to a View desktop from an HTML5-enabled Web browser.

The supported Web browsers are:

- Chrome 28 or later
- IE 9 or later
- Safari 6 or later
- Firefox 21 or later
- Mobile Safari, iOS 6, or later

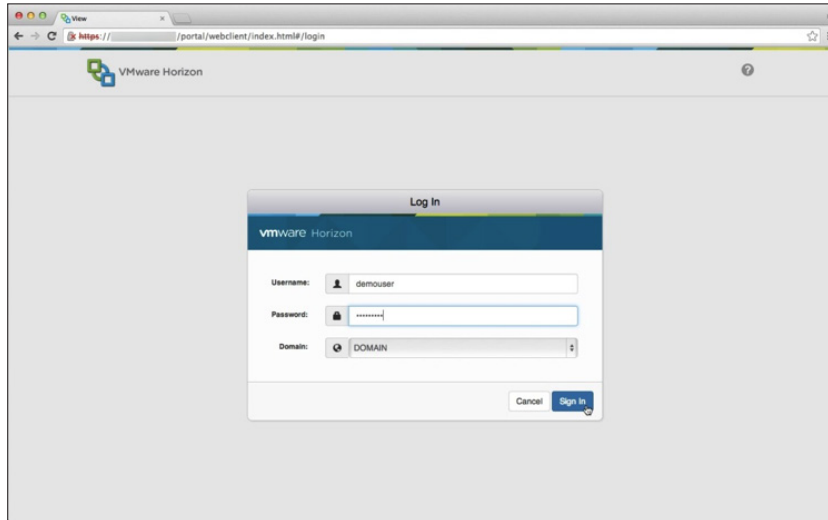
The desktop you are connecting to through HTML must be in a pool with the HTML Access feature enabled, as discussed in Deploy a Linked-Clone Desktop Pool.

1. Open a supported Web browser and navigate to the address of your View Connection Server.
2. Click **VMware Horizon View HTML Access**.



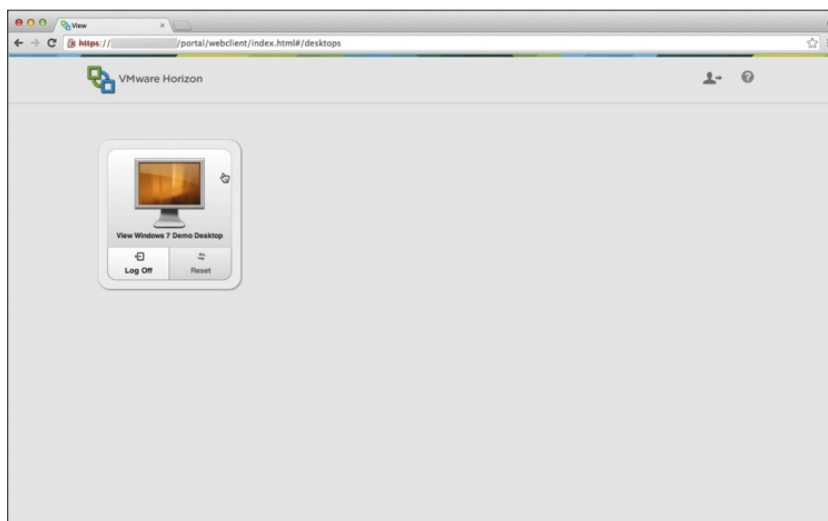
3. Enter your user credentials.

To be able to connect, you must be entitled to a desktop pool or specific desktop.

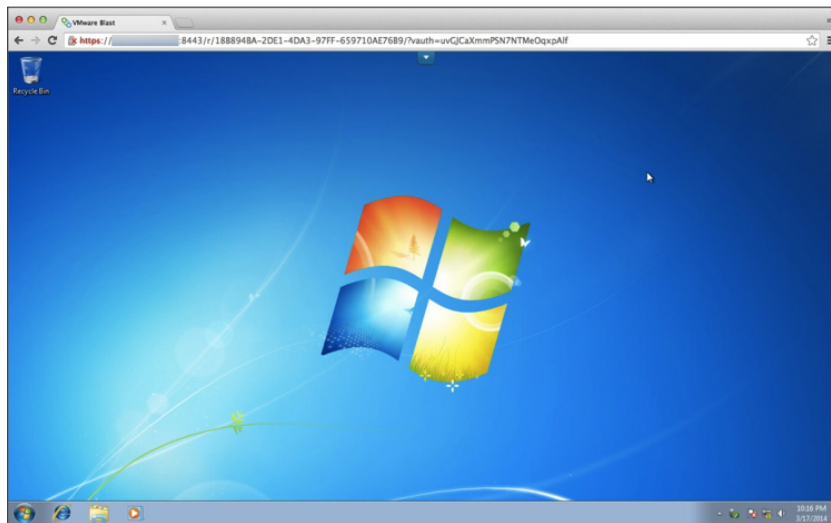


After the credentials are validated, you can see the available desktops.

4. Click the desktop that you want to connect to.

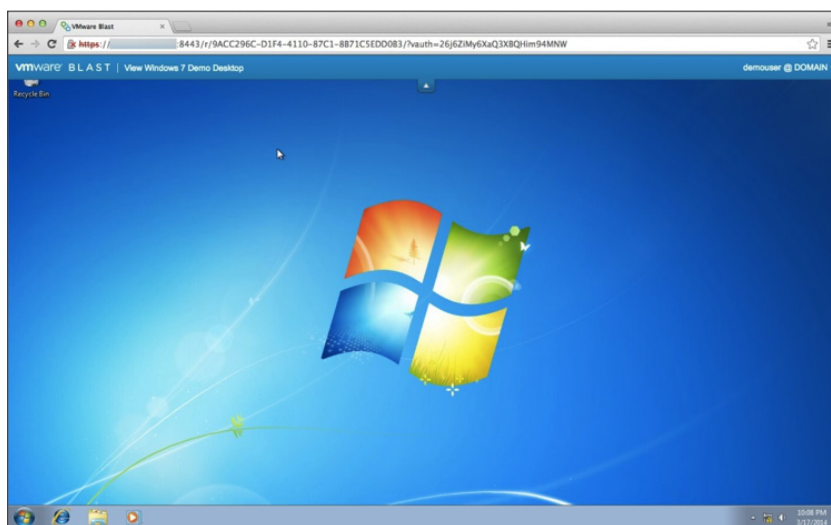


You are connected to your View desktop using HTML Access.

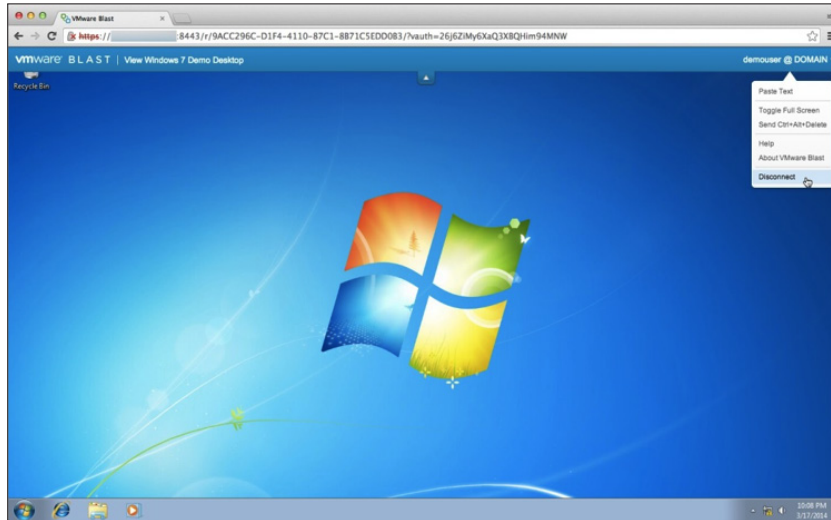


You can navigate and use your desktop as you normally would. The View HTML Access menu hides at the top of the Web browser window.

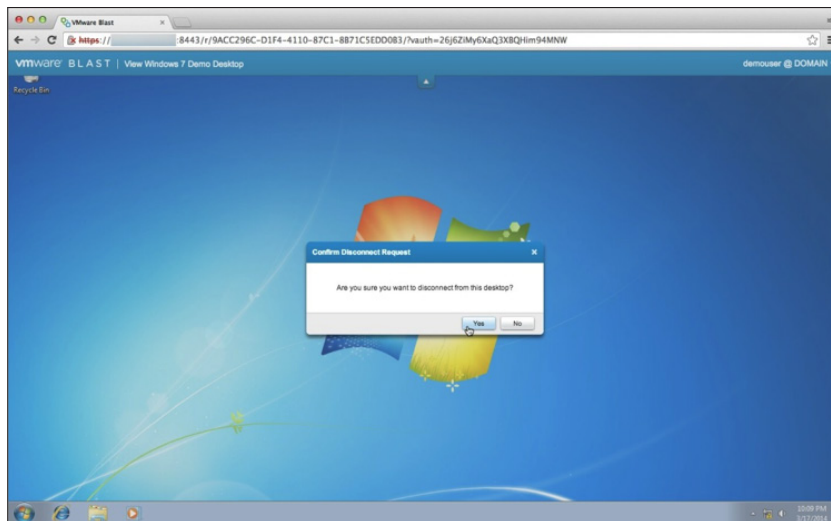
5. Click the down-arrow directly under the URL field to make the View HTML Access menu visible.



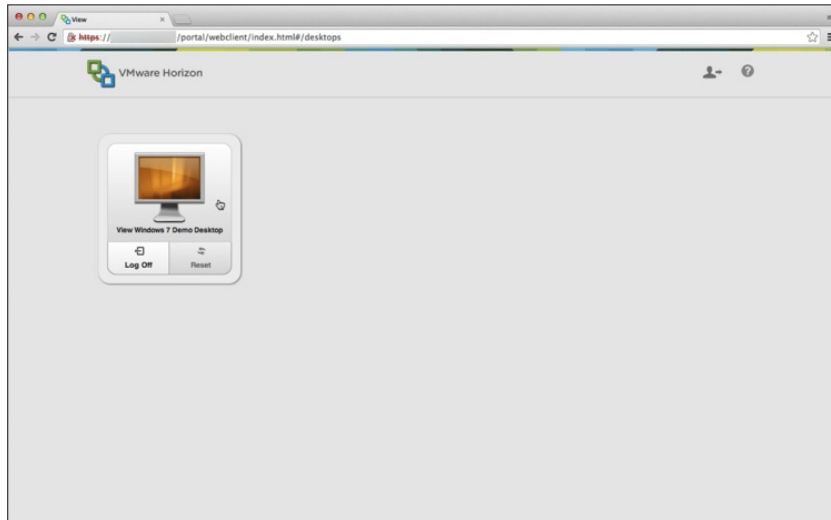
6. To disconnect from your session, click your user name at the top right of the HTML Access menu bar.
7. From the drop-down menu, select **Disconnect**.



8. Confirm that you want to disconnect by clicking **Yes**.



You are returned to your list of available desktops. You can log off or connect to a different View desktop if one is available.

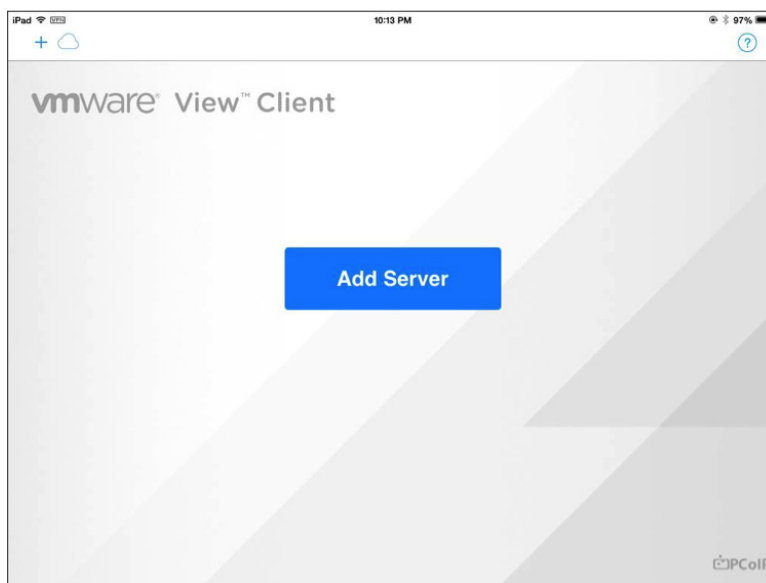


You have now connected to a View desktop using HTML Access. Proceed to the next exercise to connect to View desktops from a mobile client.

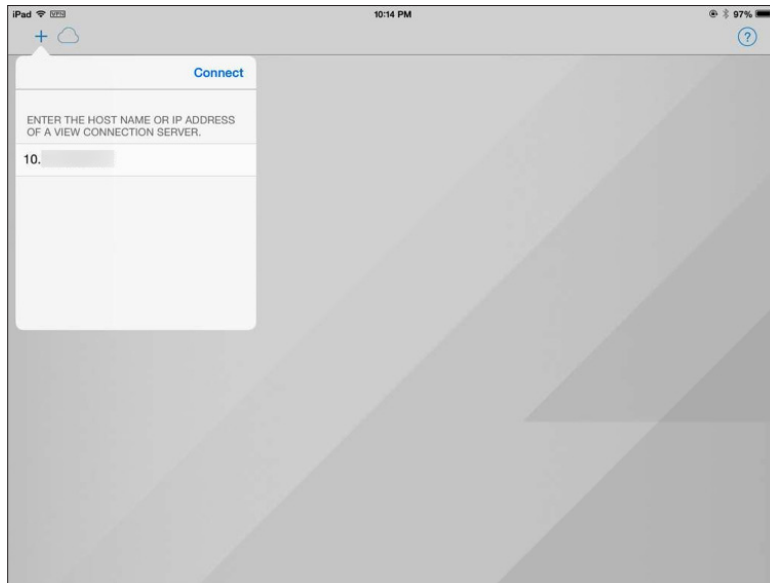
Connect to View Desktops from a Mobile Horizon Client

This exercise shows you how to connect to a View Desktop from the iOS Horizon Client on the iPad. Unity Touch is a Horizon Client feature that is available on Windows, iPhone, iPad, and Android 4.2 or later devices using the View 2.0 or later clients.

1. Launch Horizon Client from your iOS mobile device.
2. Tap **+** in the top left menu bar or the **Add Server** button.

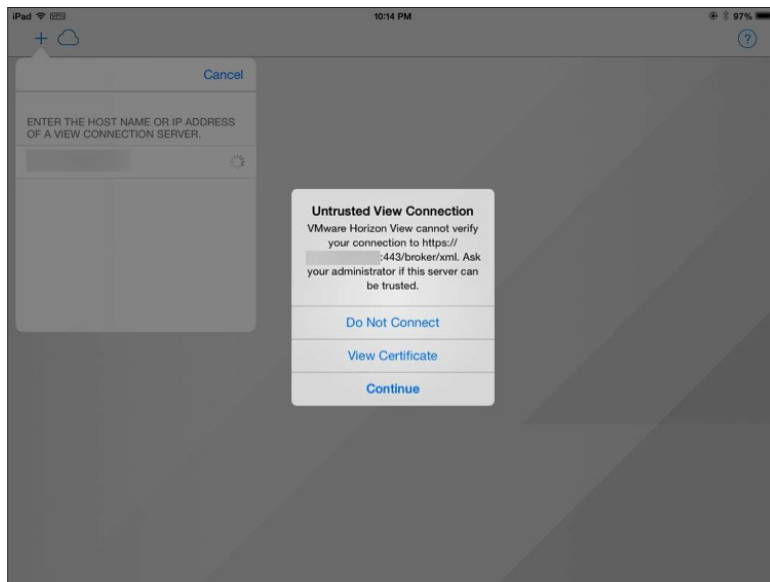


3. Enter the host name or IP address of the View Connection Server and tap **Connect**.



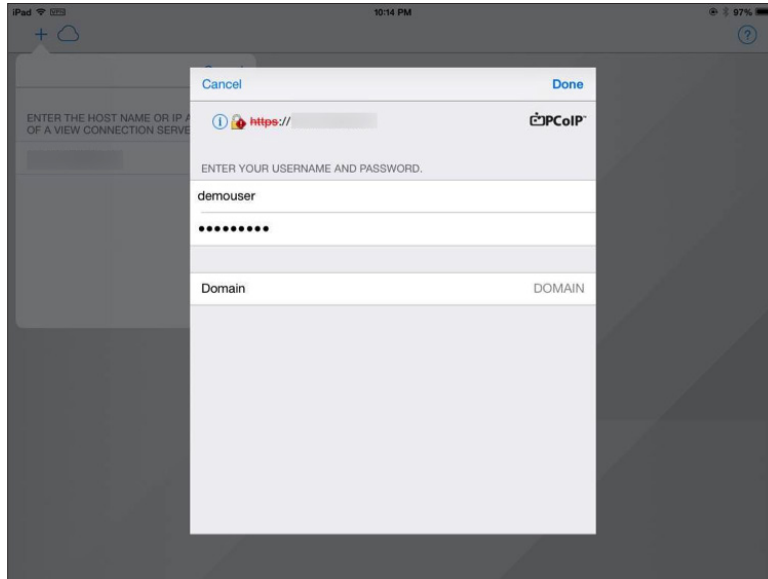
If you are using the default self-signed SSL certificate, an Untrusted View Connection warning appears. You can modify the Horizon Client security settings in the Properties or Preferences menu.

4. Tap **View Certificate** to ensure that the certificate is valid.
5. To accept the certificate, tap **Continue**.



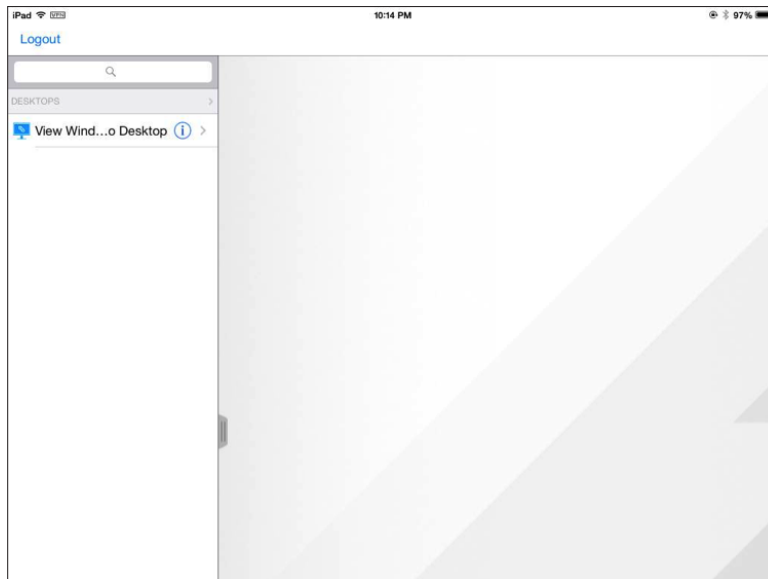
6. Enter your user credentials.

To be able to connect, you must be entitled to a desktop pool.

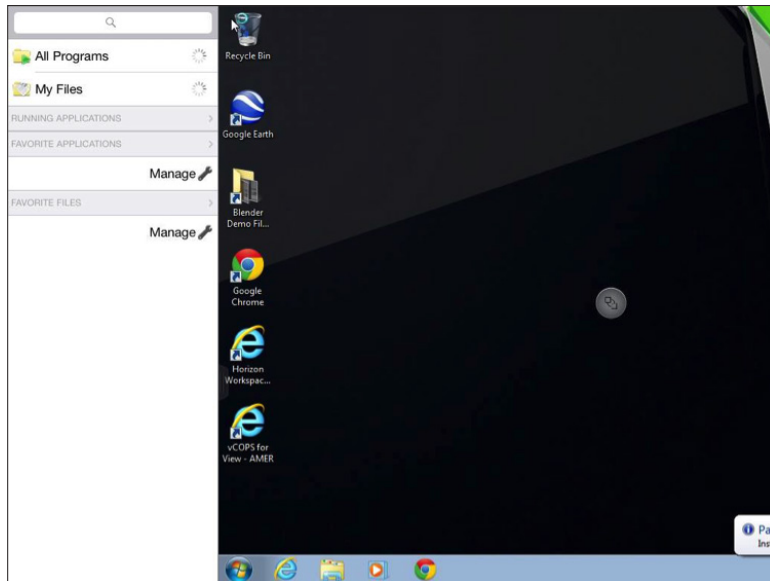


After your credentials are validated, your available desktops are listed.

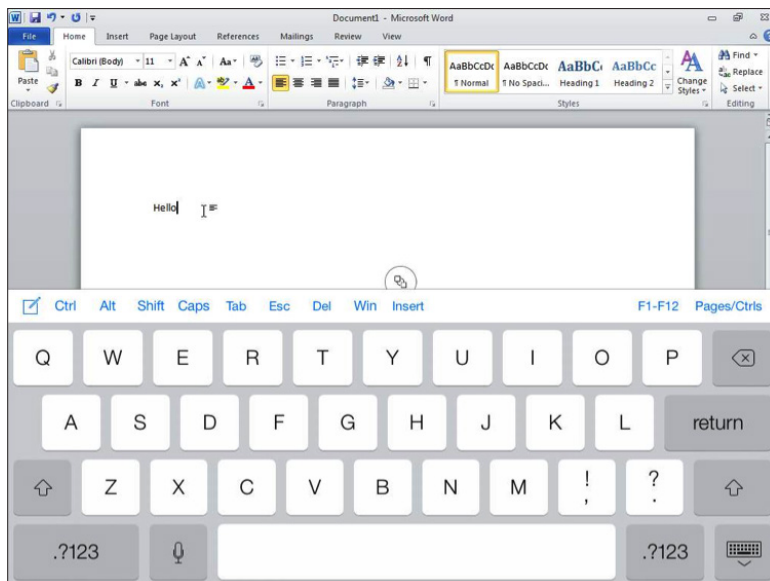
7. Tap the desktop that you want to connect to.



You have connected to your View desktop from the iOS Horizon Client. By default, at first login, the Unity Touch menu appears on the left side. The menu provides the functionality of a typical Windows Start menu without having to maneuver your touch screen to use the Start menu. You can easily and quickly launch applications.

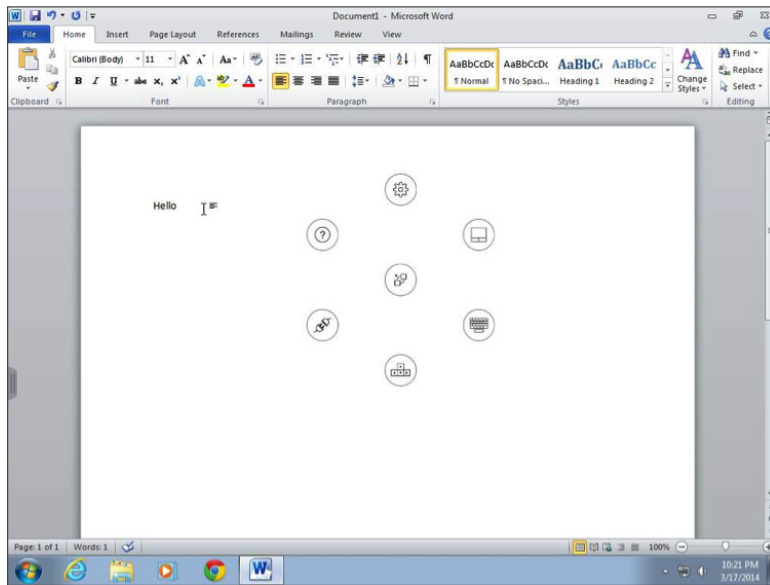


In the example shown, we launched a word-processing application. Interacting with the application triggered the keyboard overlay.



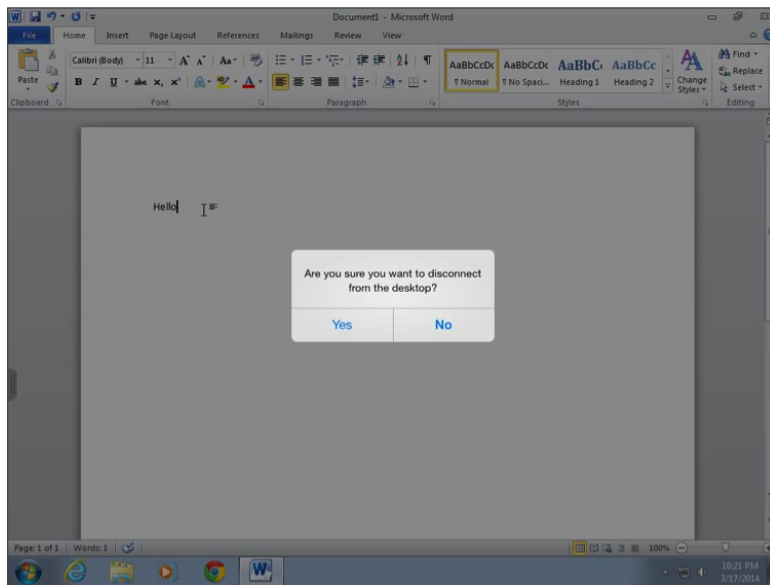
On the iOS Horizon Client, menu buttons, in the form of icons, are placed on your screen. They enable you to perform such tasks as disconnecting from the session or bringing up the keyboard. Use them to perform a variety of actions.

7. Tap the **Disconnect** button to end the session.

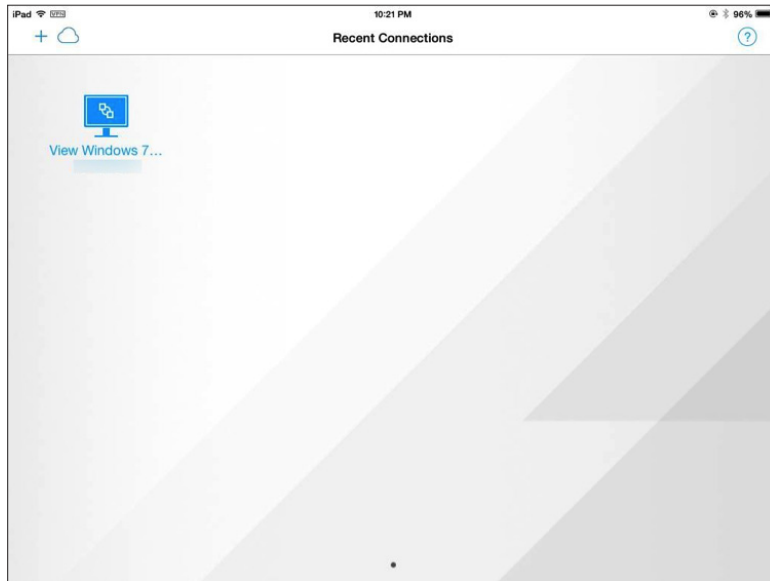


A dialog box appears for you to confirm your session disconnect.

8. Tap **Yes**.



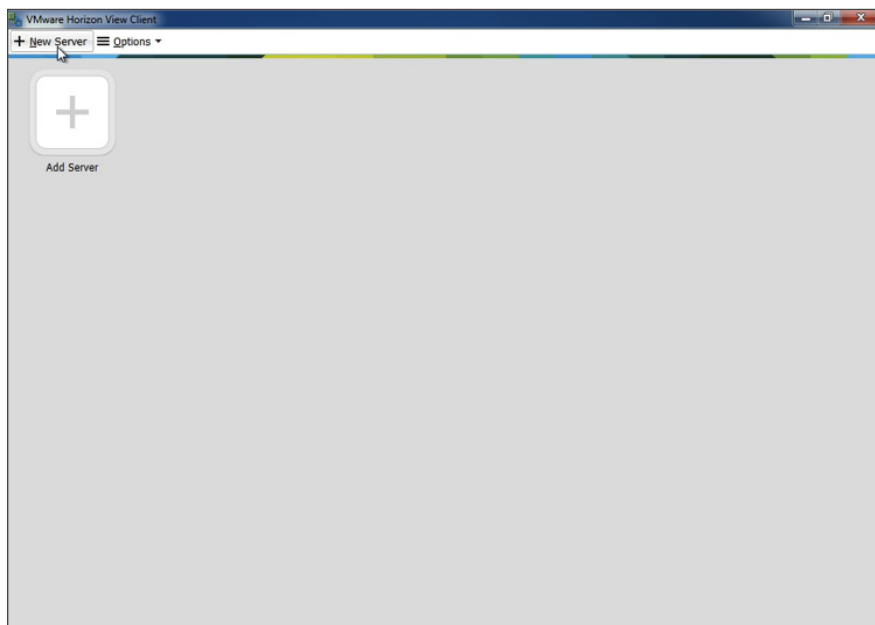
You are disconnected from your View desktop session and returned to the list of available View desktops. You can close the application or reconnect to your View desktop.



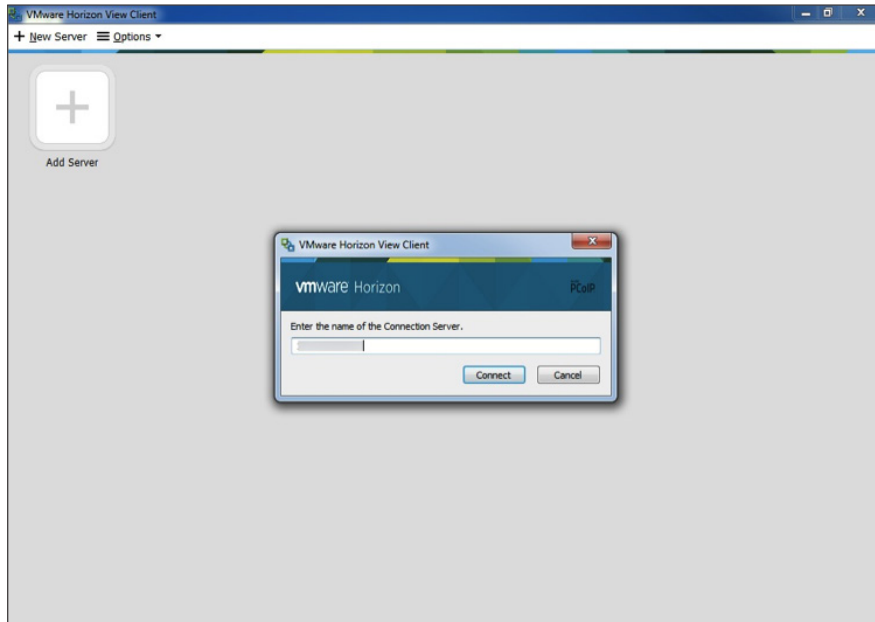
Connect to an Application Using the Horizon Client

You are now going to connect to an application using Horizon Client. The Horizon Client must be installed on either a Windows, Mac OS X, or Linux operating system.

1. Launch Horizon Client.
2. Tap **+ New Server** in the top left menu bar.

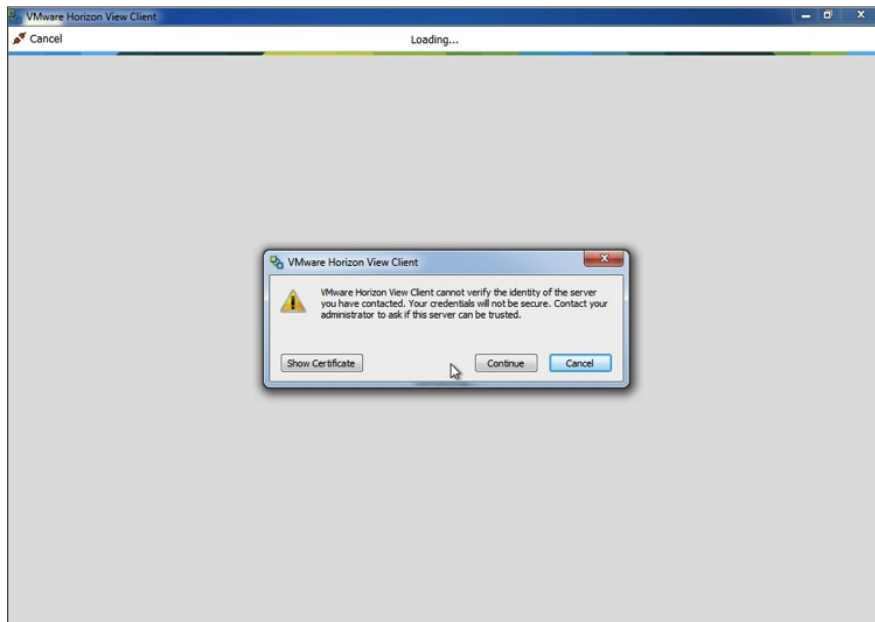


3. Enter the host name or IP address of View Connection Server and tap **Connect**.



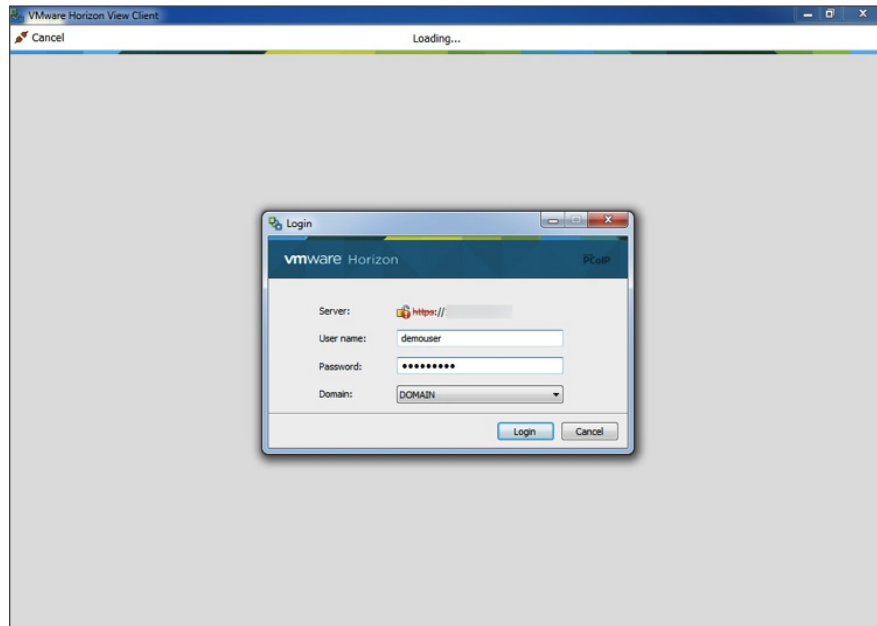
If you are using the default self-signed SSL certificate, an Untrusted View Connection warning appears. You can modify Horizon Client security settings in the Properties or Preferences menu.

4. Tap **Show Certificate** to ensure that the certificate is valid.
5. To accept the certificate, tap **Continue**.



6. Enter your user credentials and tap **Login**.

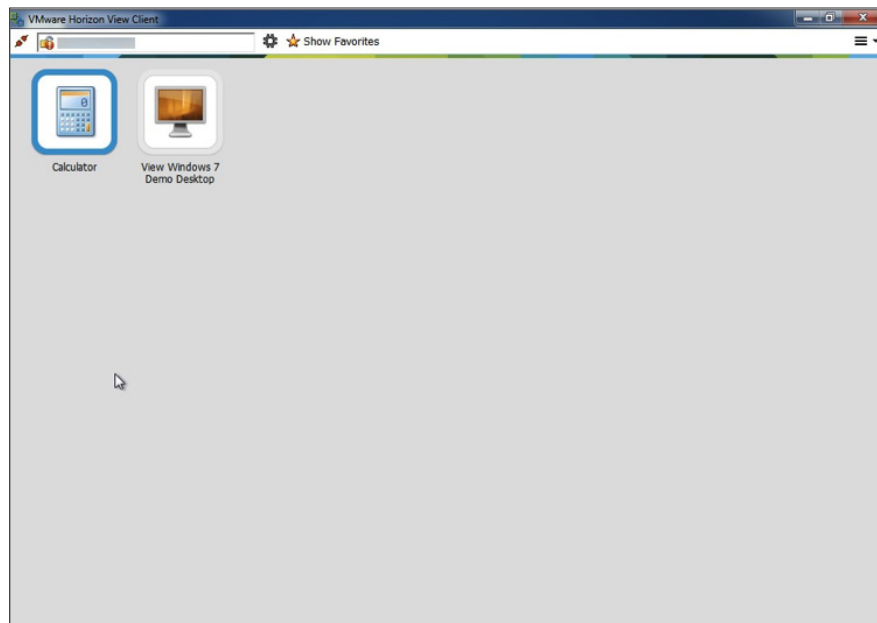
To launch an application, you must be entitled to an application pool.



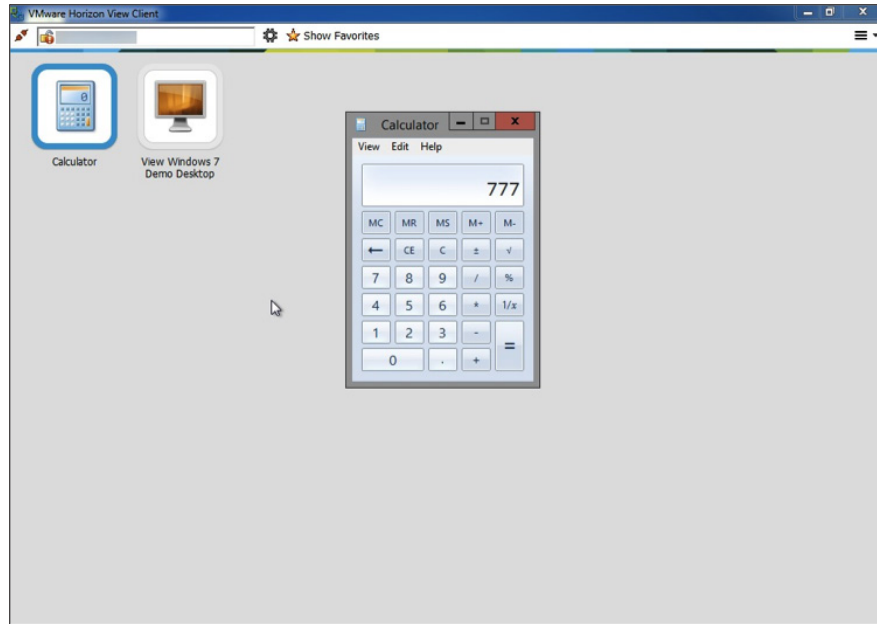
After your credentials are validated, your available applications and desktops appear.

You tap the application that you want to connect to.

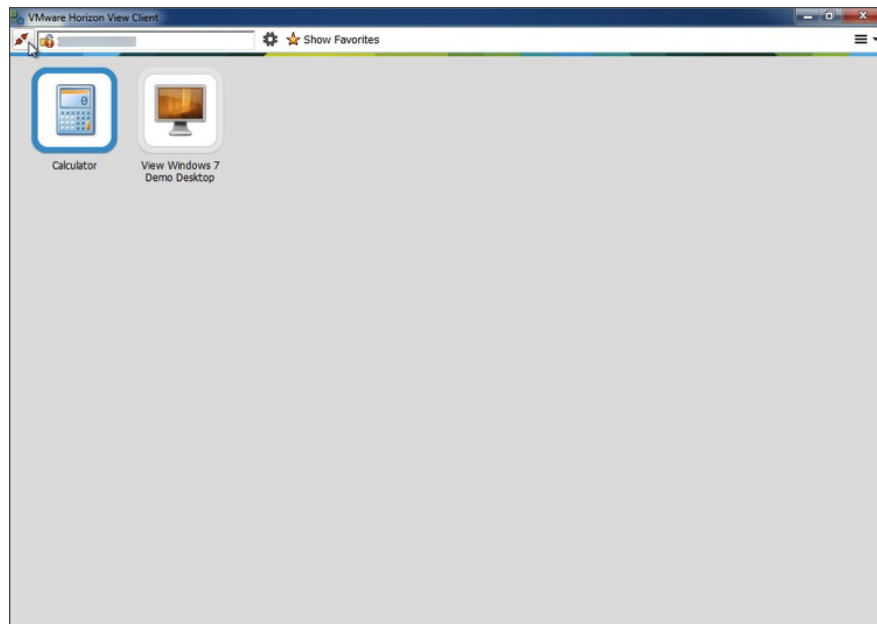
7. For this exercise, tap the **Calculator** icon.



8. Use the application as you normally would.
9. Tap **X** in the menu bar to close the application.

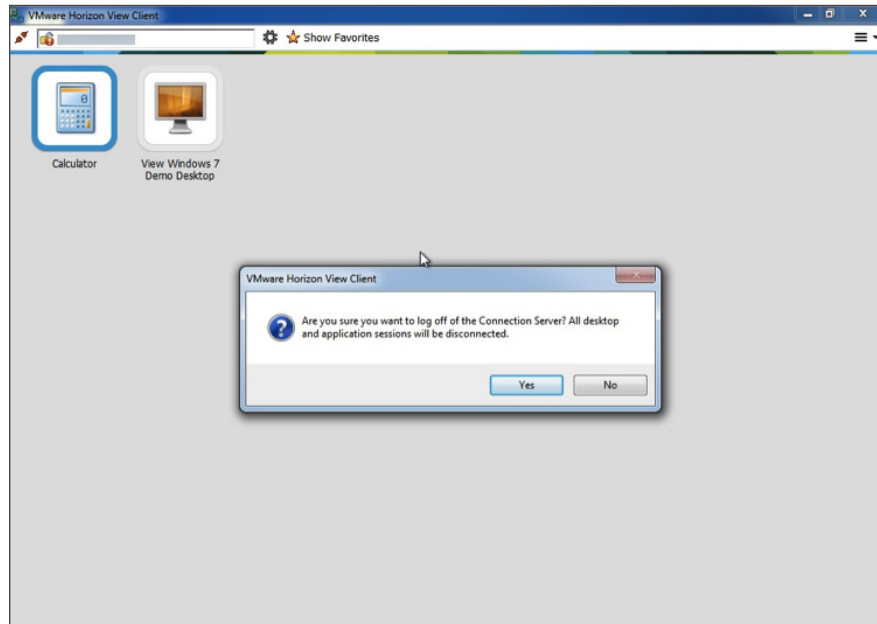


You are returned to the list of all available applications and desktops.



10. Tap the **Disconnect** button to disconnect from Horizon Client.
11. Tap **Yes** to confirm.

You are now disconnected from Horizon Client.



You have completed all the hands-on exercises in this reviewer's guide to evaluate Horizon 6 with View.

Summary

This guide introduces the new features and benefits of VMware Horizon 6 with View through a series of hands-on exercises that show the ease of initial installation, configuration, and use. It also describes the individual components, their interoperability with each other, and external integration with other VMware products.

For more detailed information, see the [VMware Horizon 6 Documentation](#). The [Additional Documentation](#) section of this document also provides access to product downloads and documentation.

Additional Documentation

For more information about topics beyond the scope of this guide:

- [VMware Horizon 6 Documentation](#)
- [VMware Horizon 6 Product](#)
- [VMware Horizon Clients Download Center](#)
- [Horizon 6 Storage Considerations](#)
- [Deploying Hardware-Accelerated Graphics with View Virtual Desktops in Horizon 6](#)
- [View Configuration Tool: automated installation tool for View](#)
- [vRealize Automation](#)
- [vRealize Orchestrator](#)
- [vRealize Orchestrator Plug-Ins Documentation](#)
- [NVIDIA driver for vSphere 5.5](#)
- [Installing async drivers on ESXi 5.x](#)
- [VMware Documentation](#)
- [VMware vSphere Documentation](#)
- [VMware Product Interoperability Matrixes](#)
- [vCenter Server](#)
- [VMware Downloads](#)
- [VMware Support](#)

About the Authors and Contributors

Susan Blau, Technical Writer at VMware, revised the product messaging, clarified certain terminology, and edited this document.

Jason Bassford, Technical Marketing Manager, End-User Computing, VMware, provided invaluable assistance in verifying the accuracy of the technical content, supplied clear explanations for concepts and procedures, and furnished recommendations for the improvement of this guide.

Tina de Benedictis, Group Manager, Technical Marketing Content, End-User Computing, VMware, provided editing oversight and content direction for this guide.

Marilyn Basanta, Product Line Manager and Solutions Architect in End-User Computing, VMware, wrote this document and updated it for Horizon 6.

To comment on this paper, contact the VMware End-User-Computing Technical-Marketing Center of Excellence team at euc_tech_content_feedback@vmware.com.

