



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
What Is Horizon 6 with View?	5
What Is VMware Horizon?	6
Key Features	6
New Features	6
Sunsetted Features	7
Packaging and Licensing	7
Upgrades	7
Architecture and Components	8
View Components	8
View Connection Server	10
View Security Server	10
View Composer Server	10
View Agent	10
Horizon Clients	10
View Persona Management	11
ThinApp	11
vCenter Operations Manager for Horizon	12
vSphere Platform	12
vCenter Server	13
Hands-On Evaluation Exercises	13
Installation Prerequisites	13
Infrastructure Requirements	14
Network Requirements	15
Graphics Card	16
Remote Desktop Session Host Requirements for App Remoting	16
Hardware Requirements	16
Operating System Requirements	17
Create Virtual Machines for View Components	17
Download the View Installer Files	18
Complete the Prerequisite Worksheet	18
Prepare the ESXi Host for vSGA 3D Graphics (Optional)	19

Installing View Components	20
Install View Connection Server.....	21
Install a View Security Server.....	27
Install View Composer Server.....	36
Remote Desktop Session Host Configuration.....	45
Set Up a RDS Host on Windows Server 2012 R2	45
Install View Agent on an RDS Host	53
Configure Group Policy Setting fro RDS Host Sessions	57
Configuring View	71
Add a License	71
Connect vCenter Server Appliance and Configure the View Composer Settings	72
Configure Persona Management Administrative Templates in Active Directory.....	79
Adjust PCoIP Settings for PCoIP Tuning.....	79
Configure Syslog Event Logging	80
Enable Windows Server 2008 R2 SP1.....	81
Create a Farm for Remote Desktop Session Hosts.....	82
Preparing Desktop Images for Linked-Clone Desktop Pool Deployment	84
Create the Parent Virtual Machine for Desktop Deployment	85
Install View Agent.....	85
Install the View Agent Direct-Connection Plug-In (Optional)	90
Optimize the Parent Virtual Machine for Desktop Deployment.....	93
Install Custom Applications and Configure the Parent Virtual Machine Operating System (Optional)	93
Prepare the Parent Virtual Machine for Linked-Clone Deployment.....	94
Preparing a Desktop Image for Full-Clone Desktop Pool Deployment	94
Create a Virtual Machine Template for Desktop Deployment.....	95
Install View Agent on the Desktop Image Virtual Machine	101
Install the View Agent Direct-Connection Plug-In (Optional)	106
Install Custom Applications and Configure the Parent Virtual Machine Operating System (Optional)	109
Prepare the Parent Virtual Machine for Full-Clone Deployment	109
Deploying View Desktops and Applications.....	112
Deploy a Linked-Clone Desktop Pool	112
Deploy a Full-Clone Desktop Pool.....	129
Deploy an RDS Desktop Pool.....	137
Deploy an Application Pool	141

Entitling Users to View Desktops and Applications. 143

 Entitle Users to a Desktop Pool 143

 Entitle Users to an Application Pool 146

Connecting to View Desktops and Applications 149

 Connect to View Desktops Using Horizon Client 150

 Connect to View Desktops Using HTML Access 154

 Connect to View Desktops from a Mobile View Client. 158

 Connect to an Application Using the Horizon Client 163

Summary 167

Additional Documentation. 168

About the Author 168

Introduction

Welcome to the Reviewer's Guide for View in Horizon 6, a self-guided, hands-on review of View. The purpose of this guide is to familiarize you with the new features and capabilities in the context of use case scenarios so that you can evaluate both new and core capabilities.

Audience

The Reviewer's Guide for View in Horizon 6 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™ and 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™ with View documentation](#). You can consult the [VMware Knowledge Base](#) if you have additional questions. For more in-depth technical white papers, see [Horizon with 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 Desktop Images for Linked-Clone Desktop Pool Deployment](#)
- [Preparing a Desktop Image for Full-Clone Desktop Pool Deployment](#)
- [Deploying View Desktops and Applications](#)
- [Entitling Users to View Desktops and Applications](#)
- [Connecting to View Desktops and Applications](#)

Note: In this guide, the term desktop is used to mean a Windows OS-based PC that has been virtualized.

What Is Horizon 6 with View?

Horizon 6 with View (formerly Horizon View or VMware View) is a desktop virtualization solution that delivers virtual desktop services. It is available as a standalone offering—Horizon 6 with View Standard Edition—or as part of the [VMware Horizon](#) family in the Advanced and Enterprise editions. Where security and availability are both high priorities, you can use Horizon 6 with View to simplify and automate the management of desktops and securely deliver desktops as a service to users from a central location. A single administration console provides granular levels of control, allowing you to customize the end-user experience, access, and personalization to support corporate policy. End users get a familiar, personalized environment that they can access from any number of devices anywhere throughout the enterprise or from remote locations. And as an administrator, you have centralized control, efficiency, and security by having desktop data in the data center.

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

What Is VMware Horizon?

Horizon is a family of desktop and application virtualization solutions, which provide a streamlined approach to deliver, protect, and manage Windows desktops and applications to the end user so they can work anytime, anywhere, on any device.

Key Features

Horizon 6 leverages desktop virtualization with View and builds on these capabilities, allowing IT to deliver virtualized and remoted desktop and applications through a single platform and supports users with access to all their Windows and online resources through one unified workspace.

Horizon 6 supports the following key functionalities.

- **Desktops and Applications Delivered Through a Single Platform** – Deliver virtual or remoted desktops and applications through a single platform to streamline management and easily entitle end users.
- **Unified Workspace** – Securely delivers desktops, applications, and online services to end users through a unified workspace, providing a consistent user experience across devices, locations, media, and connections.
- **Closed Loop Management and Automation** – Consolidated control, delivery and protection of user compute resources with cloud analytics and automation, cloud orchestration and self-service features.
- **Optimization with the Software-Defined Data Center** – Allocates resources dynamically with virtual storage, compute, and networking to manage and deliver desktop services on demand.
- **Central Image Management** – Central image management for physical, virtual, and BYO devices.
- **Hybrid-cloud flexibility** – Provides an architecture built for onsite and cloud-based deployment.

For more details, see [VMware Horizon](#).

New Features

In the latest release, Horizon 6 supports the following new features and enhancements.

- **Application Remoting** – RemoteApp enables administrators to make programs that are accessed remotely through a Remote Desktop Session (RDS) server appear as if they are running on the client computer versus a remote desktop.
- **Virtual SAN** – Horizon 6 with VMware Virtual SAN™ is a new storage technology that automates storage provisioning and pools together with server-attached flash drives and hard disks and virtualizes them into reliable storage. Built into the vSphere platform, the technology offers greater performance while simplifying storage management. Virtual SAN eliminates the need to overprovision storage to ensure that end users have enough IOPS per desktop.
- **Cloud pod architecture** – The cloud pod architecture allows organizations to dynamically move and locate View pods across multiple data centers for efficient management of end users across distributed locations.
- **vDGA and vSGA 3D graphics enhancements** – 3D graphics capabilities are enhanced to augment a graphically rich user experience. Using Virtual Dedicated Graphics Acceleration (vDGA), a single virtual machine is mapped to one physical graphics processing unit (GPU) in the ESXi host, providing high-end, hardware-accelerated workstation graphics. Using Virtual Shared Graphics Acceleration (vSGA), multiple virtual machines leverage physical GPUs that are installed locally in ESXi hosts, providing hardware-accelerated 3D graphics to multiple virtual desktops.
- **Unity Touch enhancements** – Enhancements to VMware Unity Touch technology make it easier to connect to View Connection Server or a View security server, log in to remote desktops in the data center, and edit the list of connected servers. Unity Touch for VMware Horizon Client makes it easier to run Windows apps on iPhone, iPad, and Android devices.
- **Additional OS support** – Horizon 6 with View offers Windows Server 2012 R2 OS for server components.

Sunsetted Features

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.

Packaging and Licensing

Horizon 6 is available through the VMware Store and authorized VMware resellers and desktop competency partners and is offered in three editions, Standard, Advanced, and Enterprise. To find out what features are offered in each edition see [Compare Horizon 6 \(with View\) Editions](#).

In addition to the Horizon 6 editions, VMware Mirage™, VMware ThinApp®, VMware Workspace™, vCenter Operations Manager™ for Horizon, and Virtual SAN Desktop are also available as standalone products.

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

Technical support for Horizon 6 is available at Basic (12x5) and Production (24x7) levels for all components in all editions, including vSphere, vCenter, and VMware View Manager™. You can also purchase Business Critical Support, which provides access to a dedicated account team who builds and maintains a profile of your View installation and provides regular account reviews. The VMware Professional Services Organization is also available for consultations or to deploy Horizon in your organization. For more information on technical support, see [VMware Support](#).

For more information on packaging and licensing, see [VMware Horizon Pricing](#).

Upgrades

If you are using an earlier version of Horizon with View (formerly VMware View) with a valid VMware Support and Subscription (SnS) contract, you are eligible to receive a complimentary upgrade to Horizon 6 Standard Edition. If you do not have a current SnS and want to reinstate your contract, contact VMware Support or see [VMware Support](#).

If you have an earlier version of Horizon Suite, you can expand by buying Horizon 6 Enterprise Edition licenses. If you have an earlier version of Workspace, you can upgrade to the Horizon Advanced or Enterprise edition. If you have an earlier version of ThinApp, you can upgrade in a two-step process to either the Thin Client Suite or Horizon 6 Add-ons and then to Horizon Standard Edition. For more information, see [Horizon View Purchasing](#).

Architecture and Components

This section describes the components and VMware products that interact with View.

View Components

View includes seven main components:

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

The diagram provides an architectural overview of a Horizon deployment and shows how the three main components, as well as multiple smaller components, work together to provide the virtual desktop infrastructure.

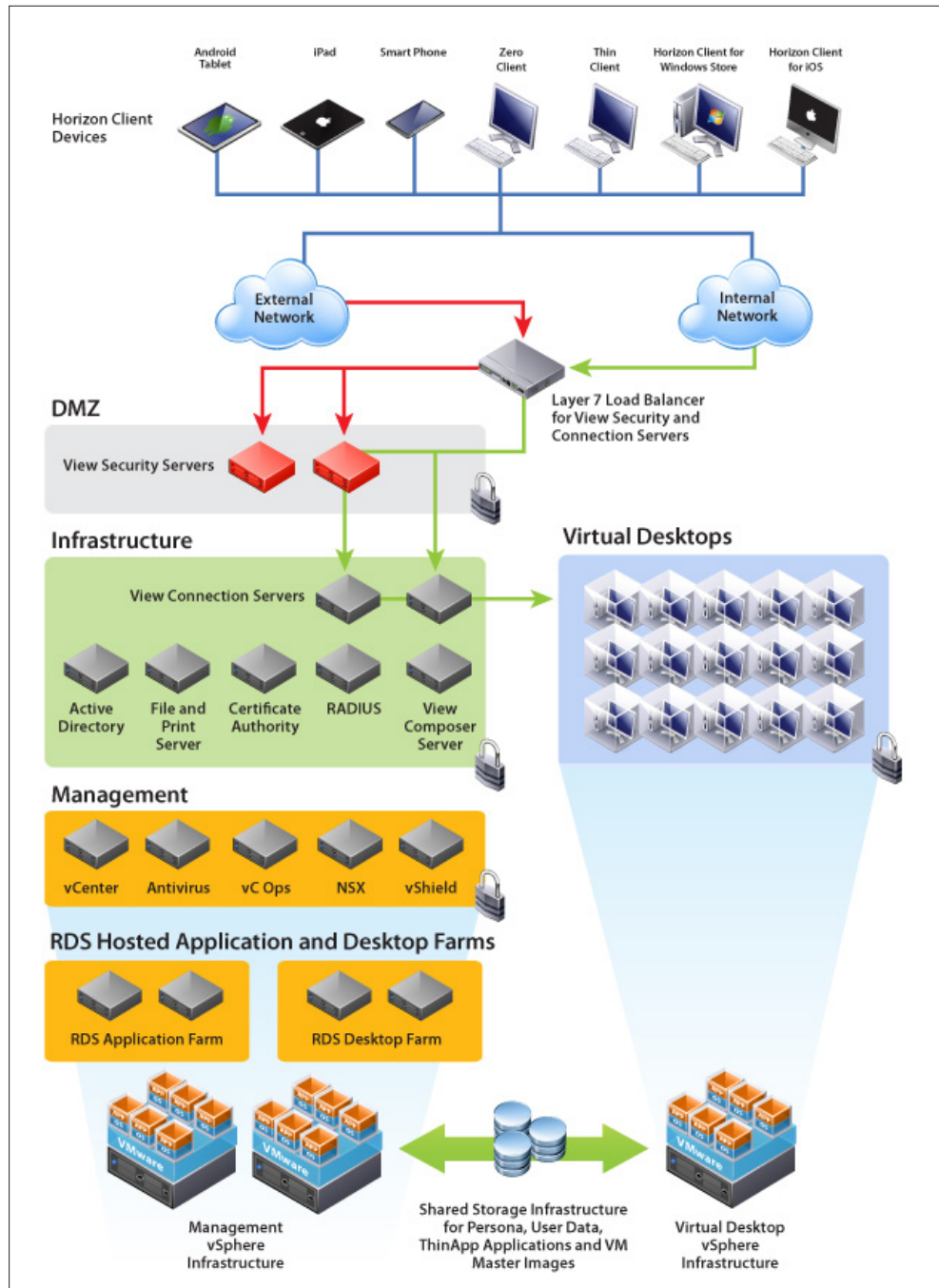


Figure 1: VMware Horizon with View Deployment and Components

View Connection Server

View Connection Server streamlines the management, provisioning, and deployment of virtual desktops. As an administrator, you can centrally manage thousands of virtual desktops from a single console. 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 only access 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 desktop images are one or more copies of a parent virtual machine that share the virtual disks of the parent, but which operate as individual virtual machines. Linked-clone desktop images 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.

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 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 Horizon Portal, the default landing page for View Connection Server. By default, links on the Horizon Portal connect users to the [Download Center](#).

View Persona Management

View Persona Management is an optional component included with Horizon 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.

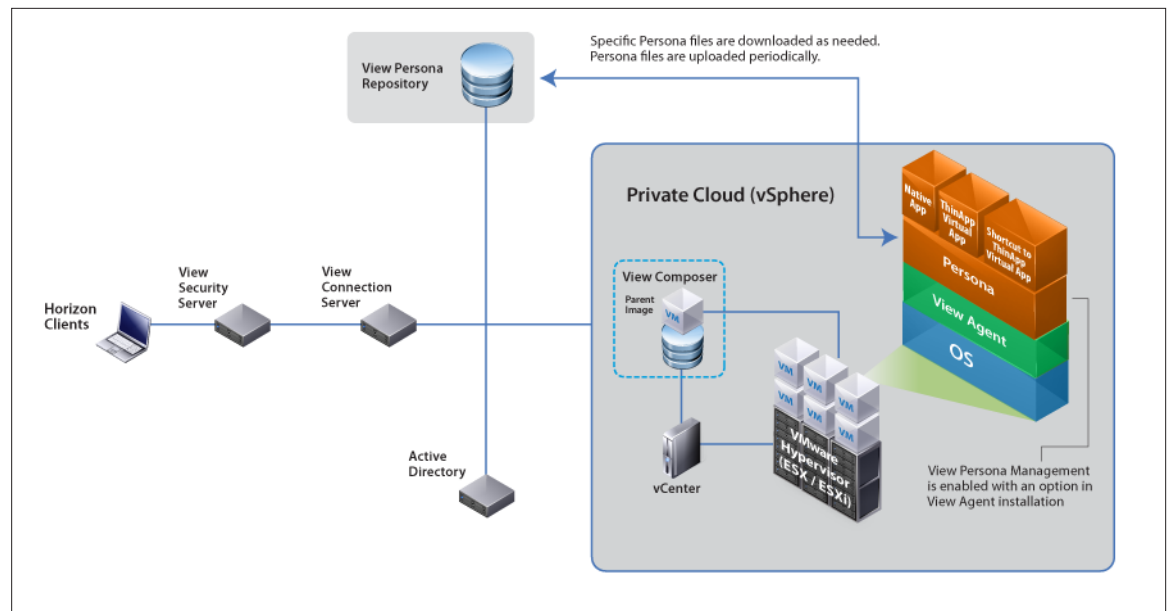


Figure 2: View Persona Management Architecture

ThinApp

ThinApp is an optional software component included with Horizon that creates virtualized applications. In a Horizon implementation, these virtual packages reside on a ThinApp repository in 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 that points to the ThinApp package on the repository. Applications on remote desktops can be natively installed applications, ThinApp virtual applications, or shortcuts to ThinApp virtual applications. You can permanently copy a ThinApp virtual application to a remote desktop or add a shortcut that points to the virtual application on the ThinApp repository. As part of Horizon, ThinApp simplifies repetitive administrative tasks and reduces storage needs for virtual desktops by maintaining applications independent 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.

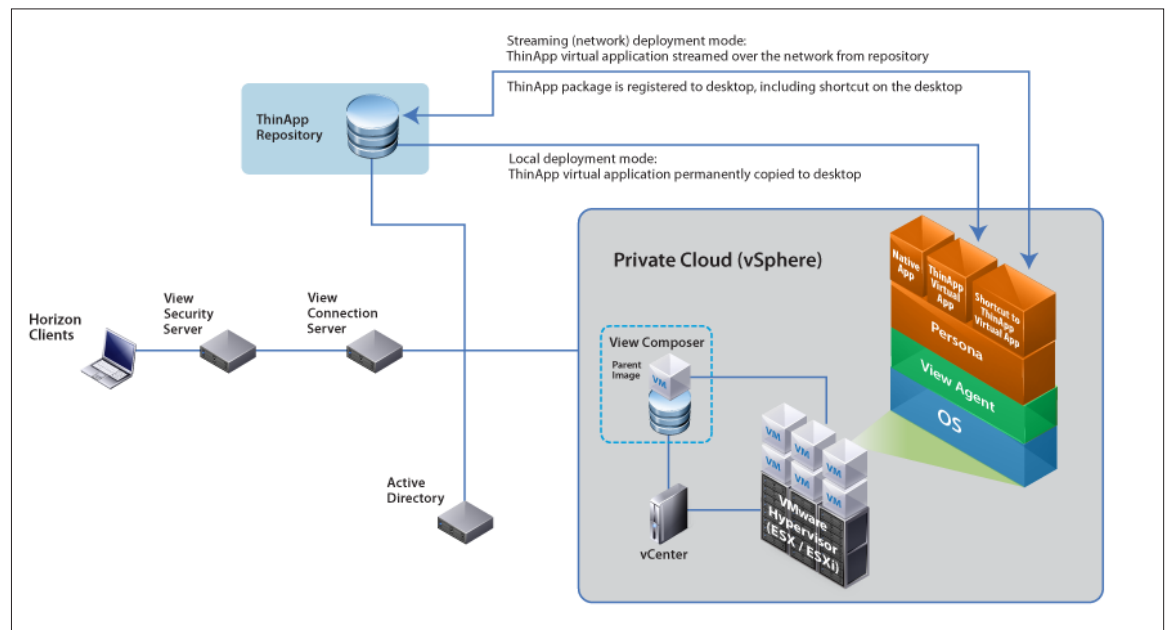


Figure 3: ThinApp Architecture in a Horizon with View Deployment

vCenter Operations Manager for Horizon

VMware vCenter Operations Manager for Horizon 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 Horizon Documentation](#).

vSphere Platform

Designed for desktops, vSphere is a scalable platform for running virtual desktops and applications that offers business-continuity and disaster-recovery capabilities to protect desktop data and availability without the cost and complexity of traditional solutions. 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 [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 Horizon 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 Desktop Images for Linked-Clone Desktop Pool Deployment](#)
- [Preparing a Desktop Image 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 and 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 up-to-date compatibility information, see [VMware Product Interoperability Matrixes](#).

Make sure that your environment has the following prerequisites before your 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 2 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 username	
Base DN password	
Active Directory username with privileges to join computers to the domain	

Table 2: 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 3.

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

Table 3: 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 4.

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 4: 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 1Gbps 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 <http://www.nvidia.com/download/driverResults.aspx/69289/en-us>.

The following GPUs are supported:

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

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

This guide only covers how to deploy vSGA. To deploy vDGA, refer to the instructions in [Graphics Acceleration in VMware Horizon View Virtual Desktops](#). It is recommended that you follow all the 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 RDS host that is already configured, prepare a virtual desktop with Windows Server 2012 R2 installed and configure an RDS host using the [Remote Desktop Session Host Configuration](#) exercises. If you already have an RDS host configured, then you use it when configuring App Remoting in subsequent exercises.

Hardware Requirements

Table 5 shows the minimum and recommended hardware requirements for View components.

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

Table 5: Hardware Requirements

Operating System Requirements

Table 6 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	40GB
Windows Server 2008 R2 SP1	64-bit	Standard and Enterprise	40GB
Windows Server 2012 R2	64-bit		40GB

Table 6: 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 7.

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 7: Virtual Machine Information**Download the View Installer Files**

The first step is to download the installation files and prepare them 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 700MB 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

Now that you have downloaded the View installer files, gather the data 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				

Table 8: Component Worksheet

2. Complete the database worksheet.

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

Table 9: Database Worksheet

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 (Optional)

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, make sure 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](#).

- 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	0.4.0-3vmw.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-ciss	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	5.1.0-0.5.030463	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

- Note the name of the VIB module. You need it later to verify that this driver loaded successfully.
- Follow proper vSphere shutdown procedures, and then reboot your ESXi host from one of the following:
 - vSphere Client
 - Command line by typing `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.
- When your host has powered back on, use SSH to access the ESXi console
- Run the following command to verify that the driver modules can load successfully.

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

For the further instructions or troubleshooting for configuring vSGA, see the [Graphics Acceleration in VMware Horizon View Virtual Desktops guide](#).

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.

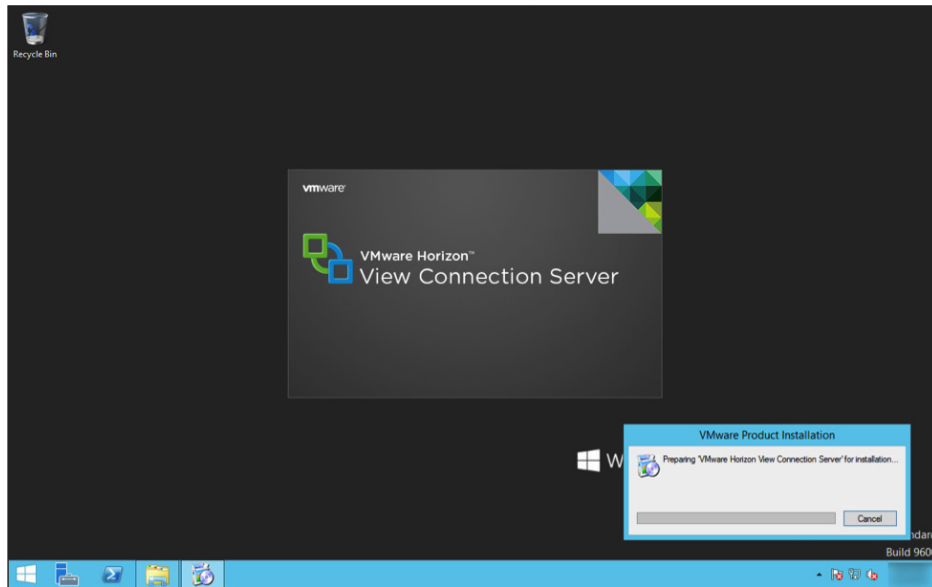
- [Install View Connection Server](#)
- [Install a View security server](#)
- [Install View Composer Server](#)

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

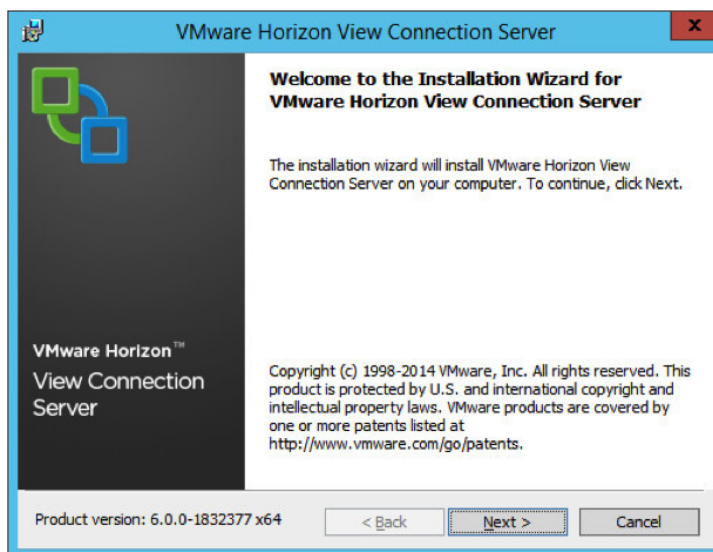
Install View Connection Server

View Connection Server streamlines the management, provisioning, and deployment of virtual desktops. As an administrator, you can centrally manage thousands of virtual desktops from a single console.

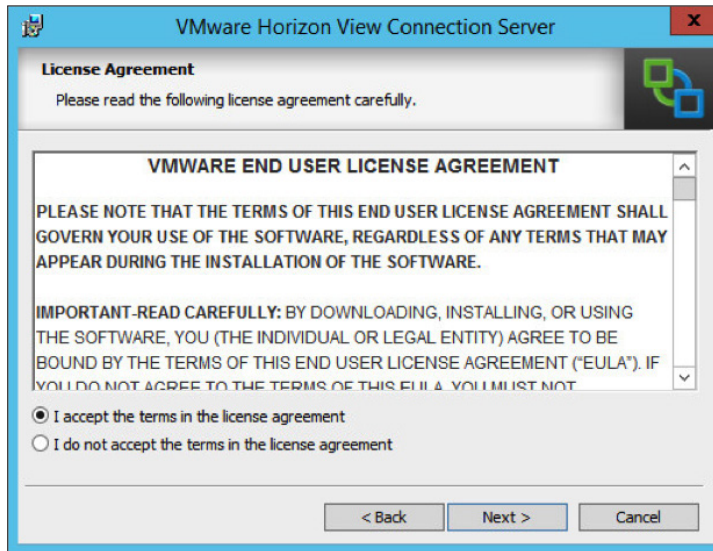
1. Log in to the virtual machine that you prepared as the target for installing View Connection Server.
The virtual machine must meet the requirements detailed in the [Installation Prerequisites](#).
2. Verify that the 64-bit View Connection Server installer is accessible by the operating system of the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



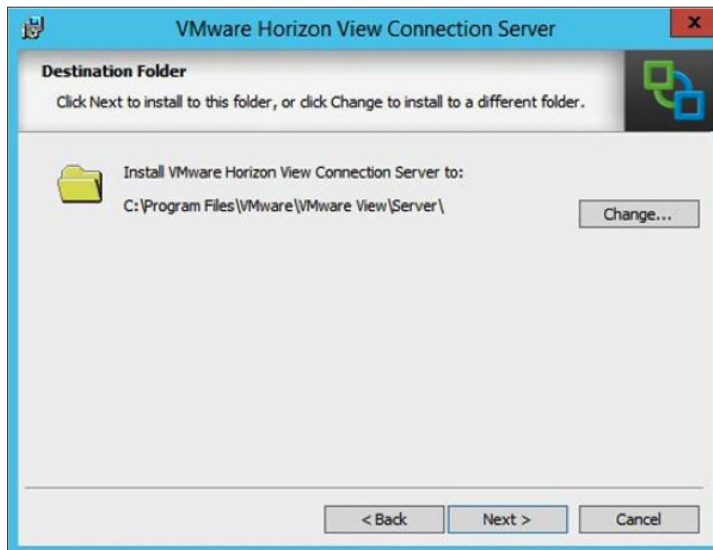
4. When the installer finishes loading, click **Next**.



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



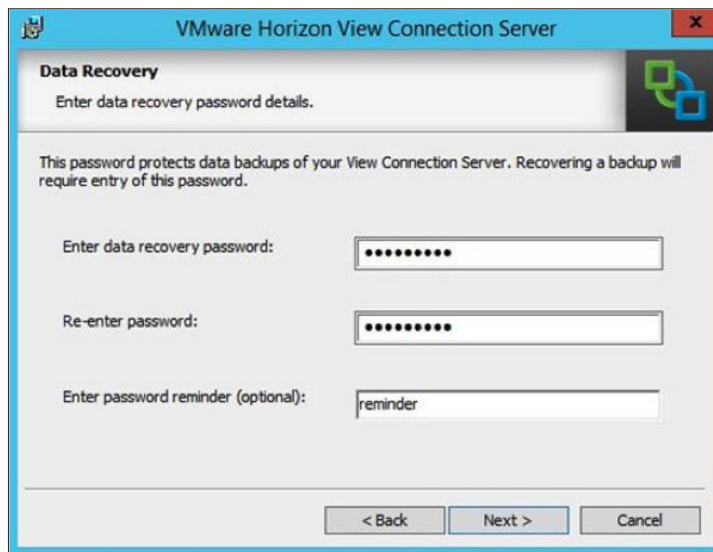
6. Choose where you want to install View Connection Server, and then click **Next**.



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



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



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

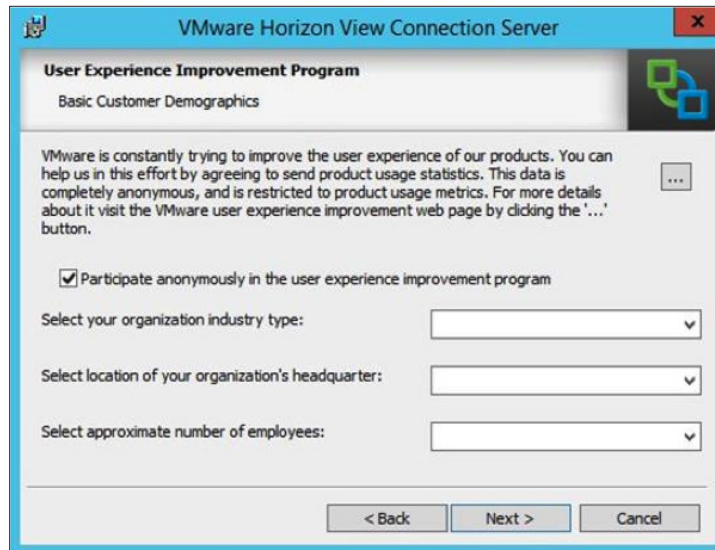


Note: The Windows Firewall ports are required for View Connection Server to function correctly. For the purposes of this exercise, Configure Windows Firewall automatically is selected, but if you want to configure the ports manually, make sure to complete the required port configuration before proceeding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

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

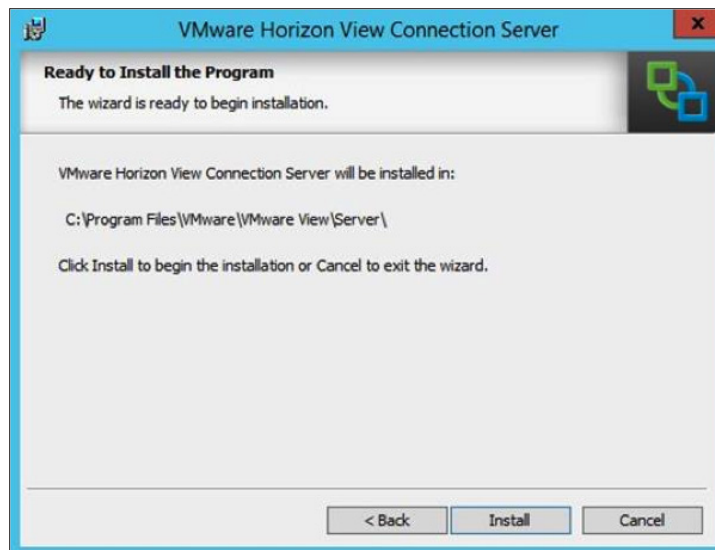


11. Choose whether to participate anonymously in the User Experience Improvement Program, and if so, select your answers from the drop-down menus, and then click **Next**.



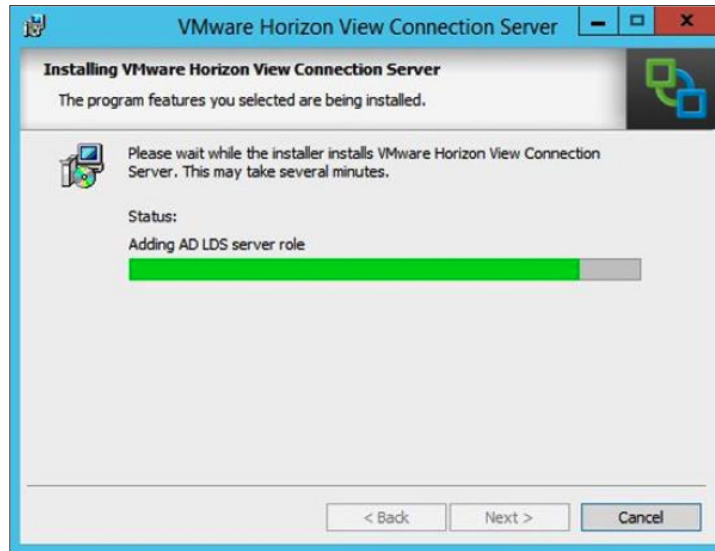
The screenshot shows a window titled "VMware Horizon View Connection Server" with a close button (X) in the top right corner. The window contains a section titled "User Experience Improvement Program" with a sub-header "Basic Customer Demographics". Below this, there is a paragraph of text explaining the program's purpose and a button with three dots (...). A checkbox labeled "Participate anonymously in the user experience improvement program" is checked. Below the checkbox are three drop-down menus labeled "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**.

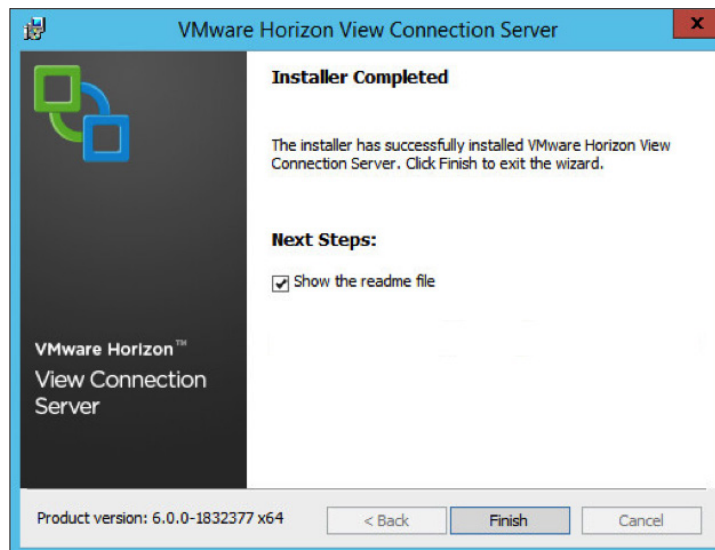


The screenshot shows a window titled "VMware Horizon View Connection Server" with a close button (X) in the top right corner. The window contains a section titled "Ready to Install the Program" with a sub-header "The wizard is ready to begin installation.". Below this, there is a paragraph of text stating "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 then 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

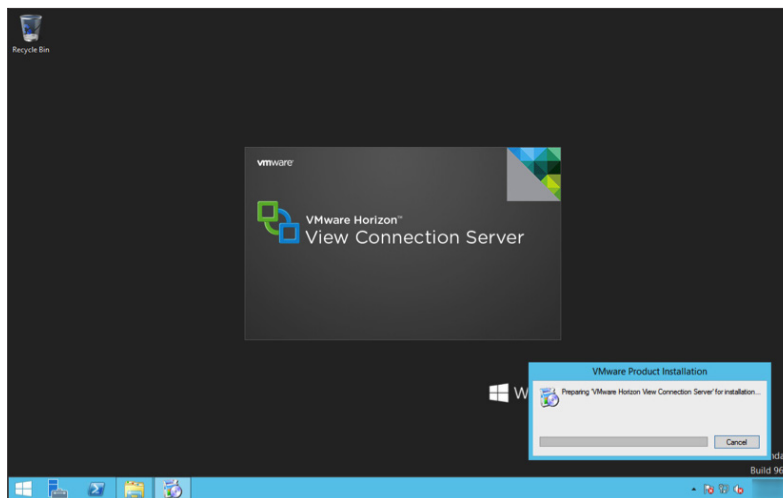
A View security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. Security servers ensure that the only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated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

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

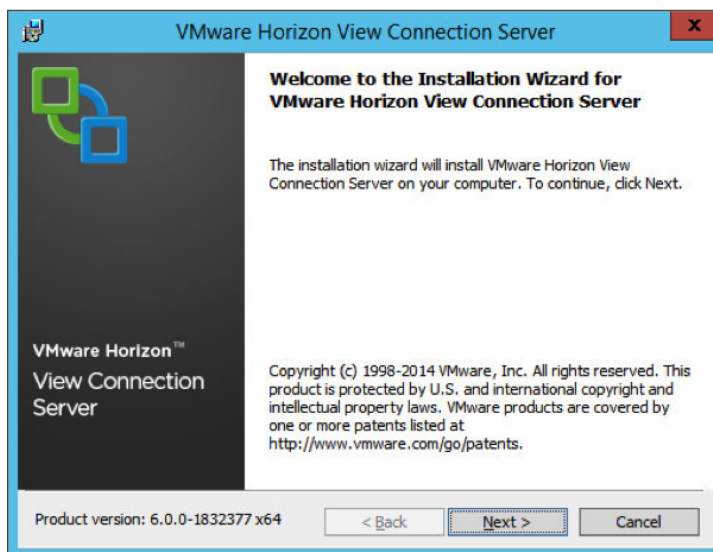
The virtual machine must meet the requirements detailed in the [Installation Prerequisites](#).

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.

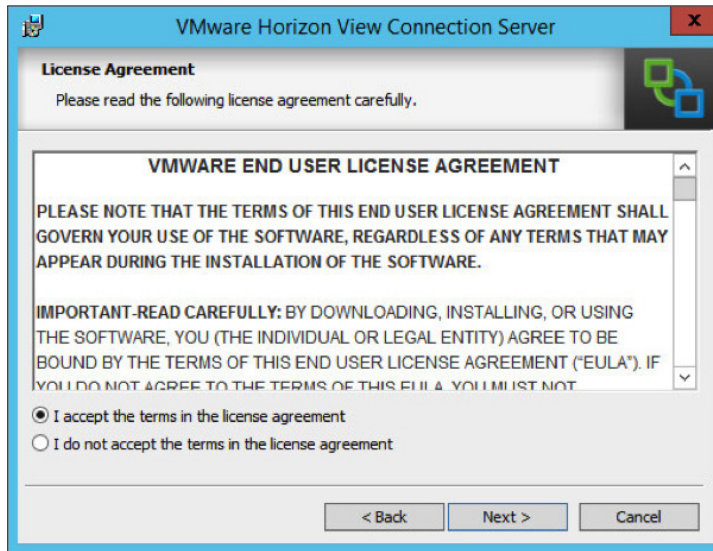
Note: The View security server is an installation option within the View Connection Server installer.



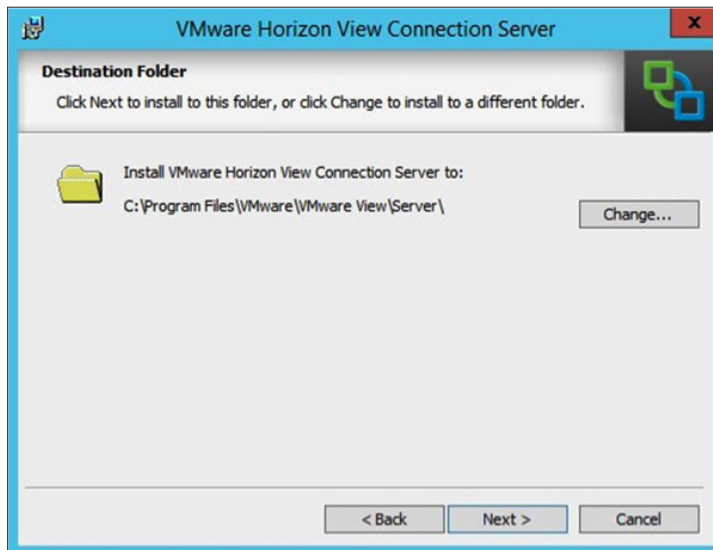
4. When the installer finishes loading, click **Next**.



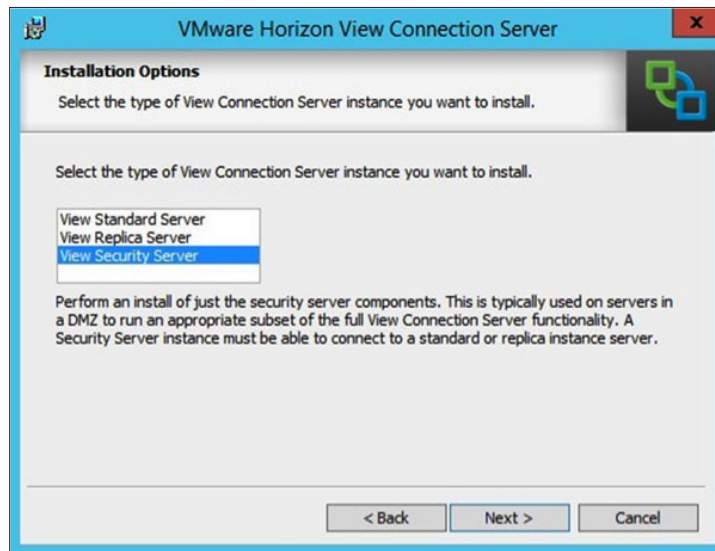
5. Review the license agreement, accept the terms and conditions, and then click **Next**.



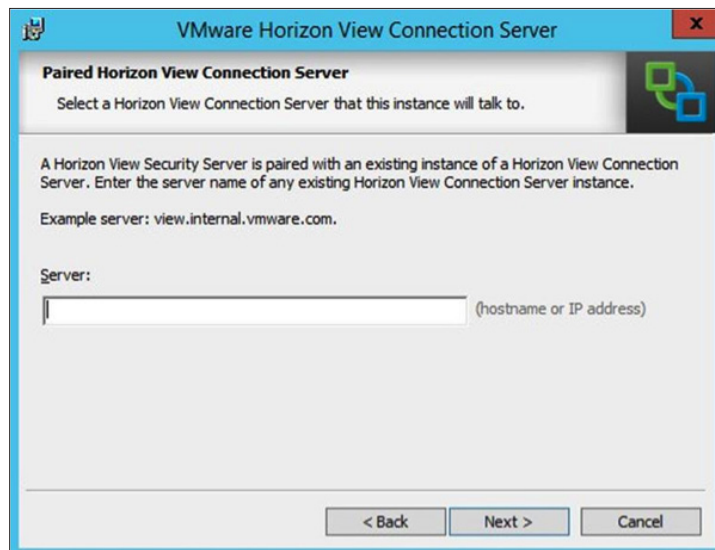
6. Choose where to install the View security server, and then click **Next**.



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

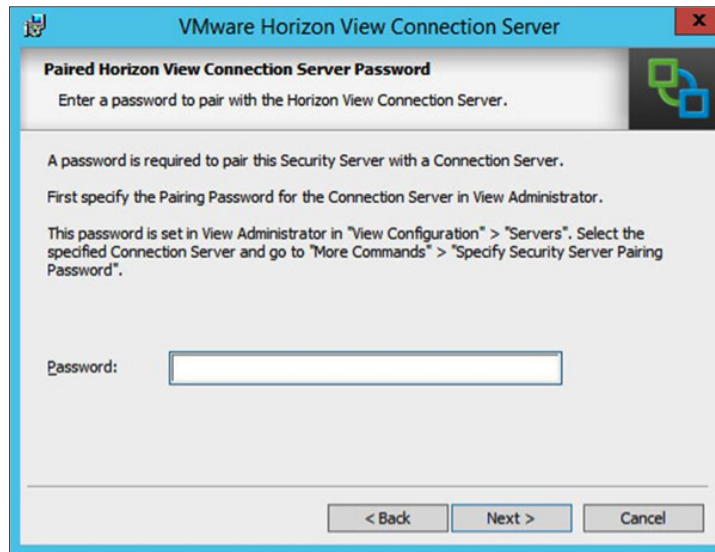


8. In the Server text box, type the FQDN of the View Connection Server installed in [Install View Connection Server](#) to pair to the View security server, and then click **Next**.

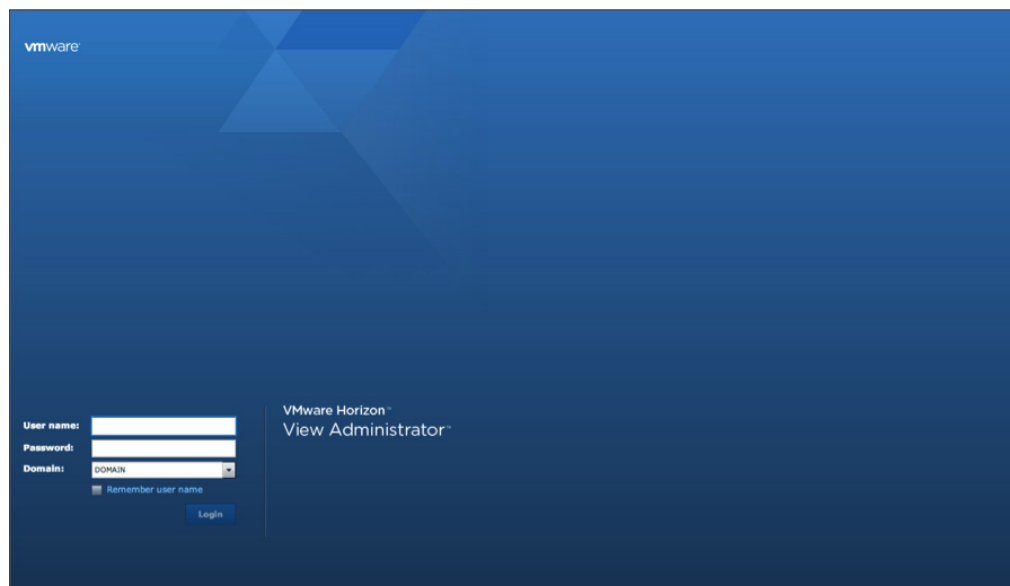


- To enter the pairing password for the View security server to the View Connection Server, you must go to the View Administrator console to create a one-time password for this session.

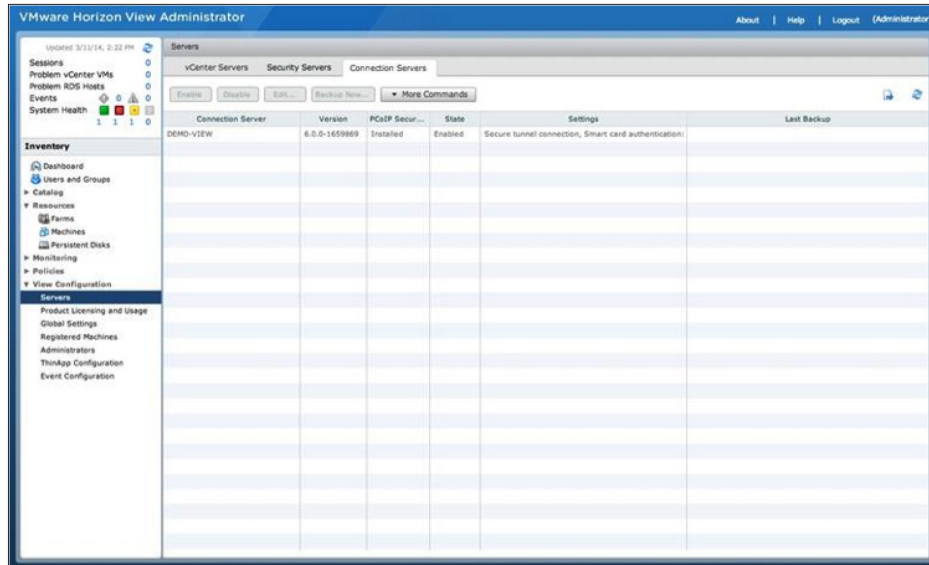
`https://<fqdn-of-view-connection-server>/admin`, where `fqdn-of-view-connection-server` is the fully qualified domain name or the IP address of the View Connection Server.



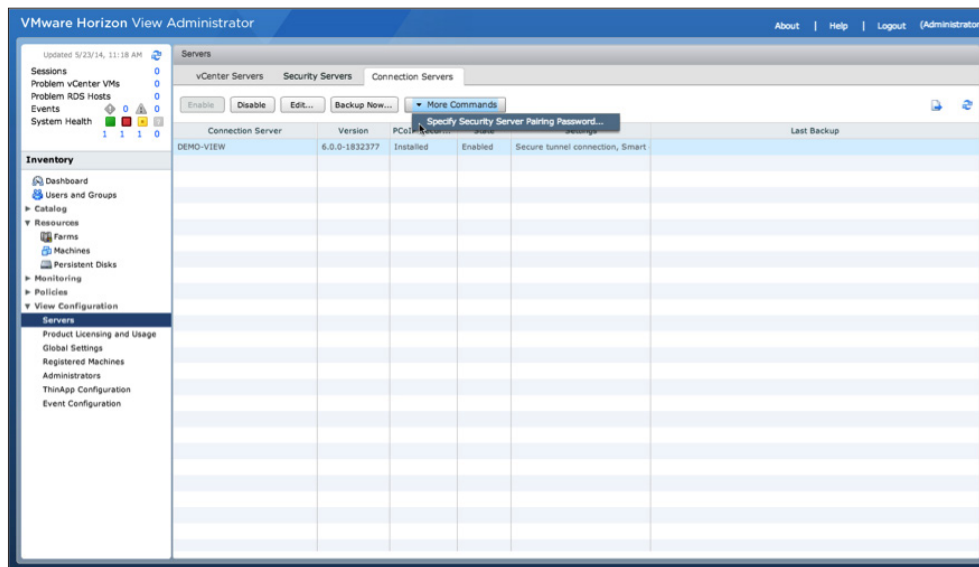
- Log in to the View Administrator console using the credentials you established in [Install View Connection Server](#).



11. In the left menu of the View Administrator console, under View Configuration, click **Servers**. In the Servers window, select the **Connection Servers** tab.

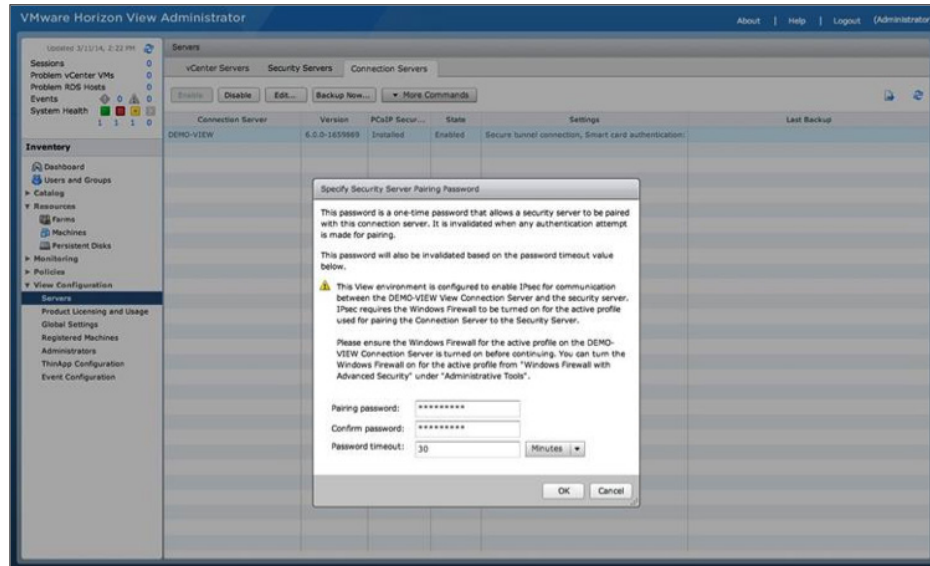


12. Click the View Connection Server that you installed in [Install View Connection Server](#), and then from the More Commands drop-down menu, select **Specify Security Server Pairing Password**.



13. Specify a pairing password and a timeout value, and then 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.

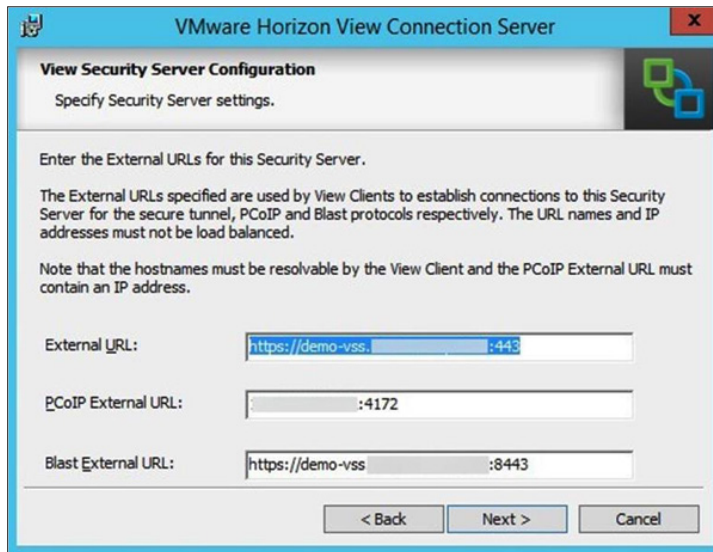
14. In the virtual machine where you are installing the View security server, enter the security server pairing password, and then click **Next**.



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

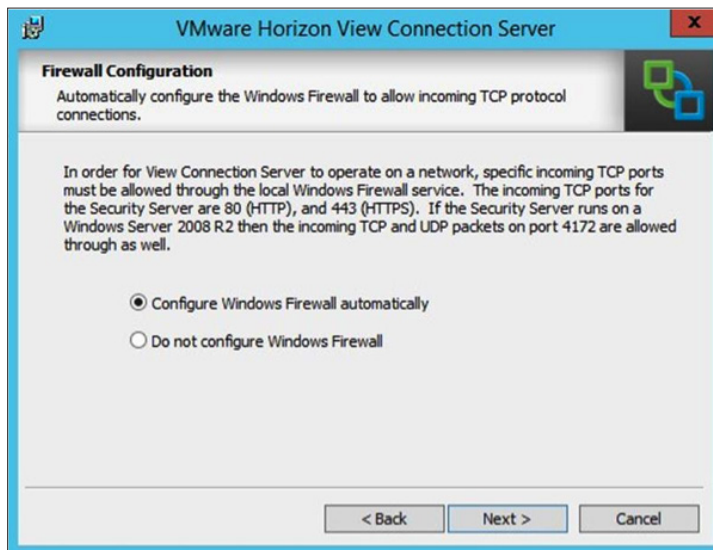
15. In the View Security Server Configuration dialog box, accept the default values for the external URLs or modify them, and then click **Next**.

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.' The main text area contains instructions: 'Enter the External URLs for this Security Server.' followed by '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 a note: 'Note that the hostnames must be resolvable by the View Client and the PCoIP External URL must contain an IP address.' There are three 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'.

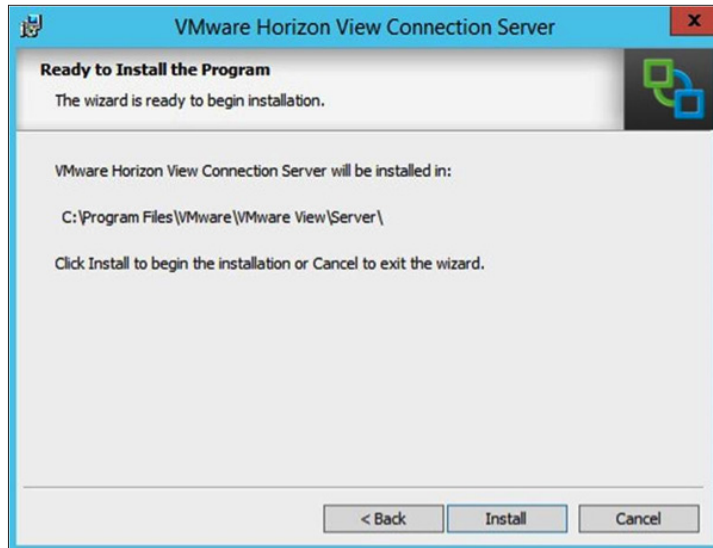
16. Choose whether to configure the Windows Firewall automatically, and then click **Next**.



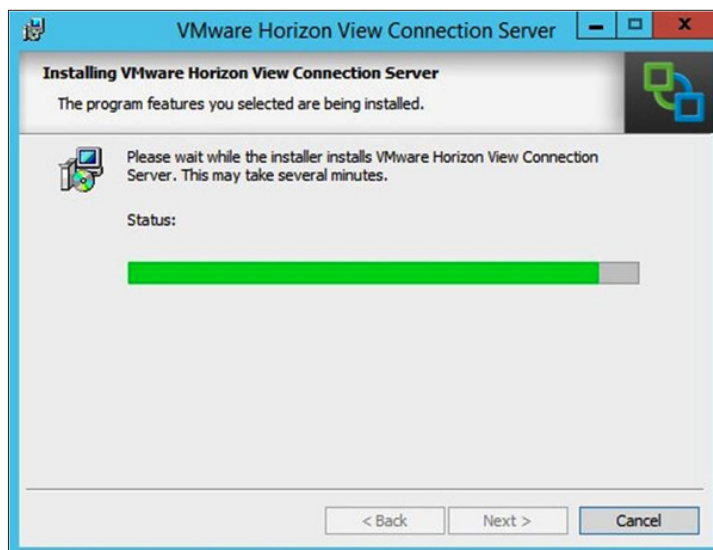
The screenshot shows the 'Firewall Configuration' dialog box. It has a title bar 'VMware Horizon View Connection Server' and a subtitle 'Firewall Configuration'. Below the subtitle is the instruction 'Automatically configure the Windows Firewall to allow incoming TCP protocol connections.' The main text 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 buttons: '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.

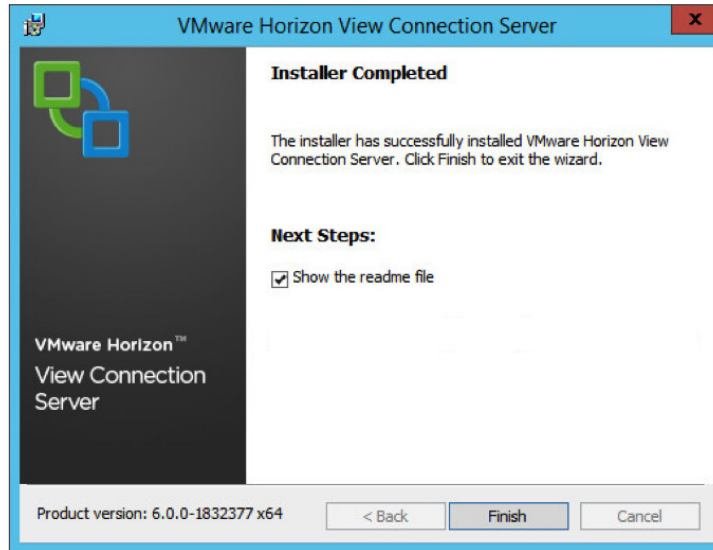
17. Click **Install** to complete the installation.



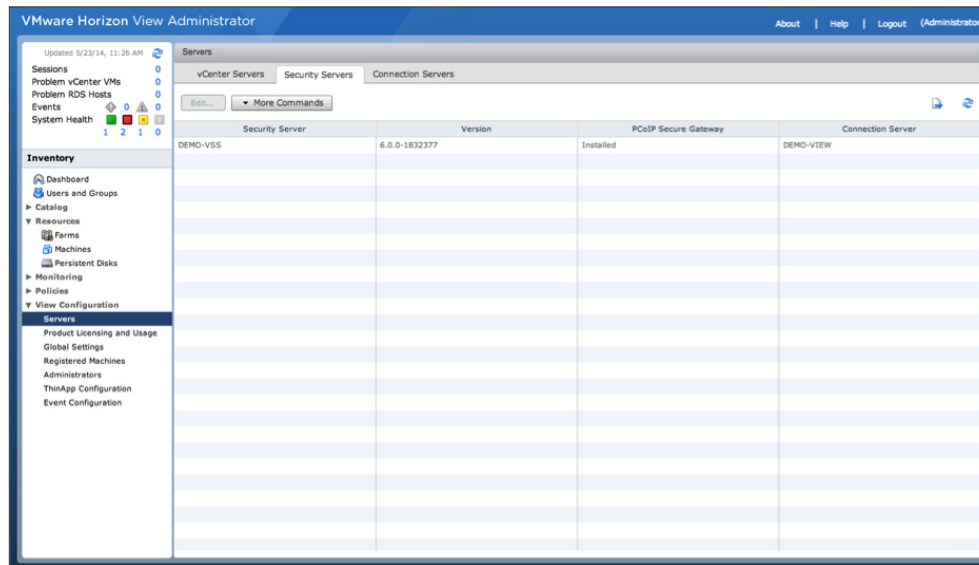
You can monitor the installation as it progresses.



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



19. To verify the View security server installation and pairing, go to the View Administrator console. Under **View Configuration > Server**, 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 “like” desktops, called linked-clone desktops. Linked-clone desktop images can optimize your use of storage space and facilitate updates.

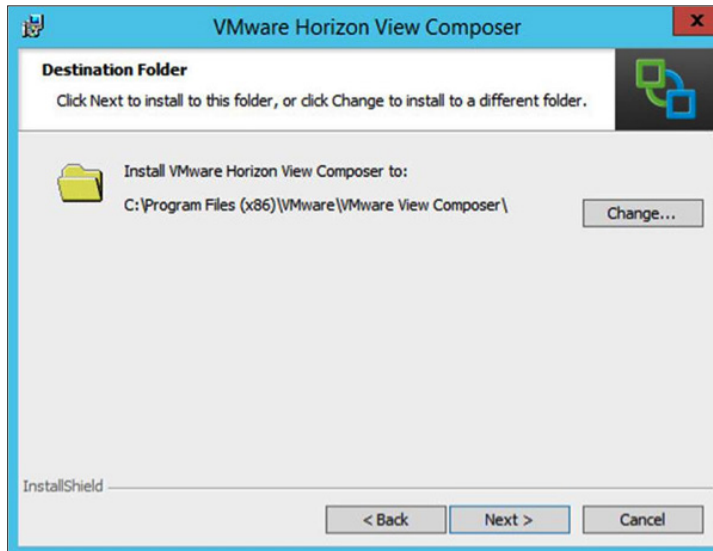
1. Log in to the virtual machine that you prepared as the target for installing View Composer Server.
Verify that the virtual machine meets the prerequisites listed in [Installation Prerequisites](#) and that the appropriate native SQL driver is installed for your database.
2. Verify that the 64-bit 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 then click **Next**.



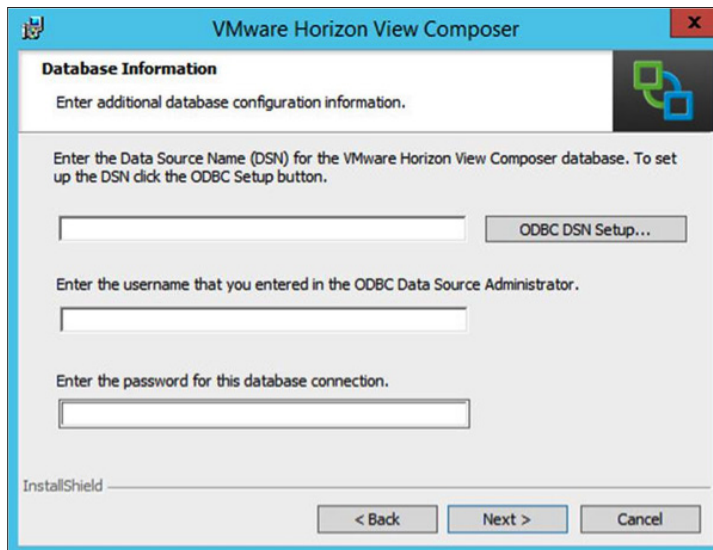
4. Review the license agreement, accept the terms and conditions, and then click **Next**.



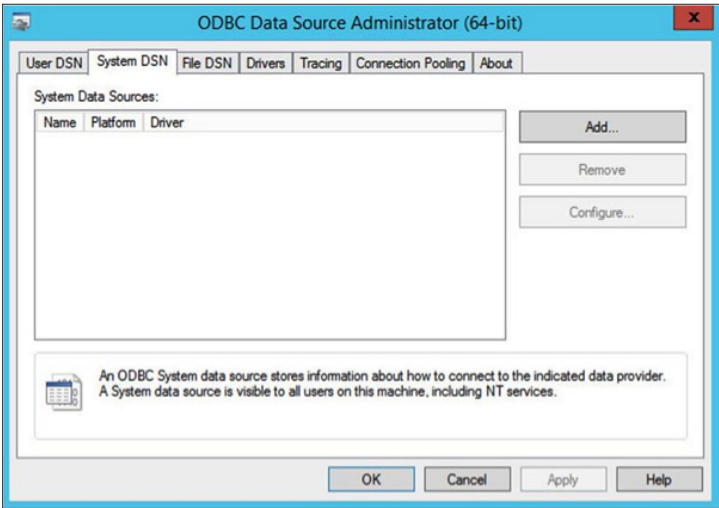
5. Choose where you want to install the View Composer Server, and then click **Next**.



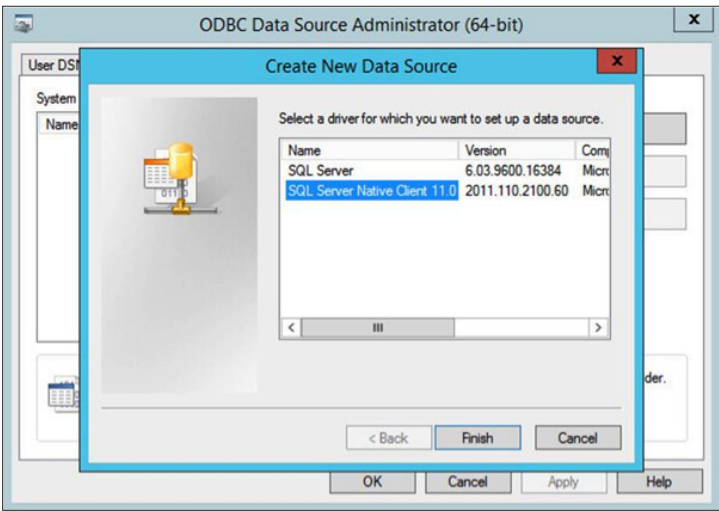
6. Click **ODBC DSN Setup** to establish a new Data Source Name to define the connection between View Composer Server and your database.



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



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

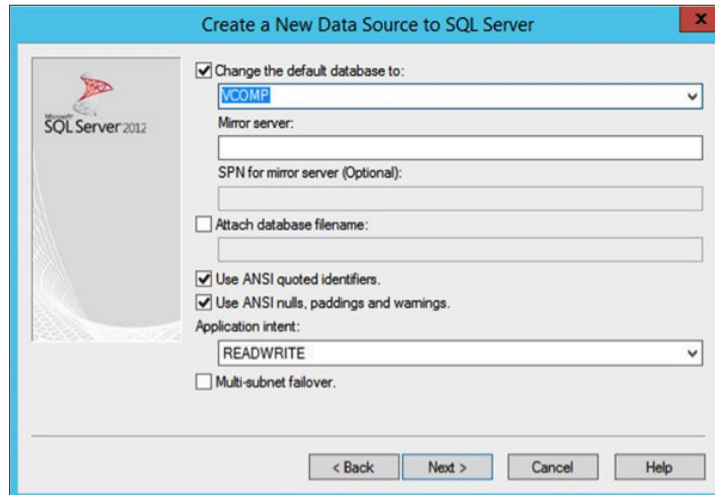


9. In the Create a New Data Source to SQL Server dialog box, type the required information for your data source, and then click **Next**.

- Name:** Unique name that refers to the data source you are connecting to
- Description:** Optional
- Server:** Address of your SQL Server in the format FQDN/SQLInstanceName or IP/SQLInstanceName.

10. Enter the SQL Server login ID and password, and then click **Next**.

11. Select the **Change the default database** check box, and from the drop-down menu, select the database you created for View Composer Server data, and then 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:

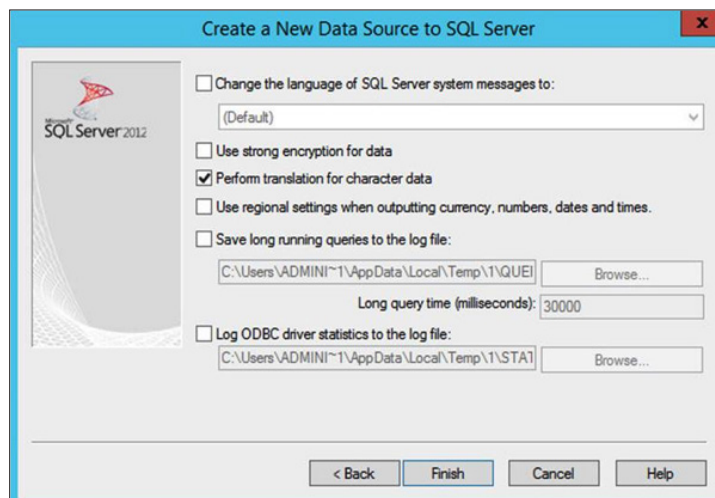
☒ Use ANSI quoted identifiers.
☒ Use ANSI nulls, paddings and warnings.

Application intent:
 READWRITE

☐ Multi-subnet failover.

< Back Next > Cancel Help

12. Additional database options are available, but are not required for the View Composer Server database. After selecting the options you want, click **Finish**.



Create a New Data Source to SQL Server

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

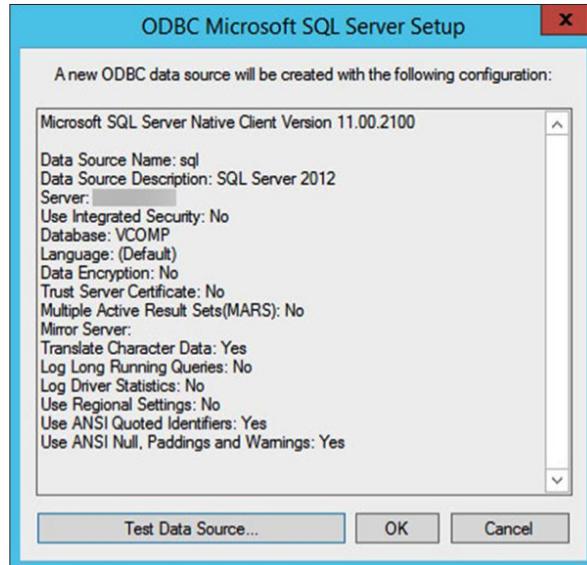
☐ Use strong encryption for data
☒ Perform translation for character data
☐ Use regional settings when outputting currency, numbers, dates and times.

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

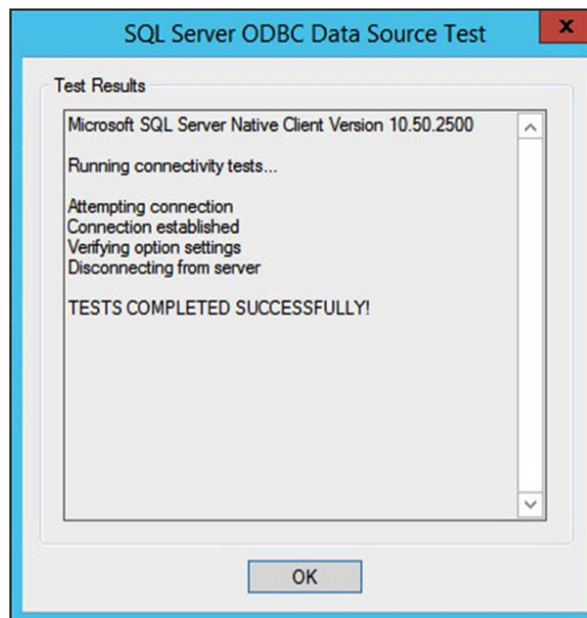
☐ Log ODBC driver statistics to the log file:
 C:\Users\ADMINI~1\AppData\Local\Temp\1\STA1 Browse...

< Back Finish Cancel Help

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

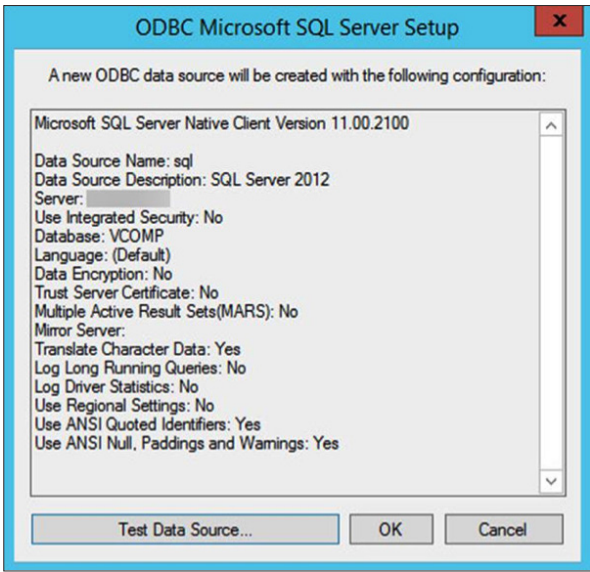


14. Verify that the test completed successfully.

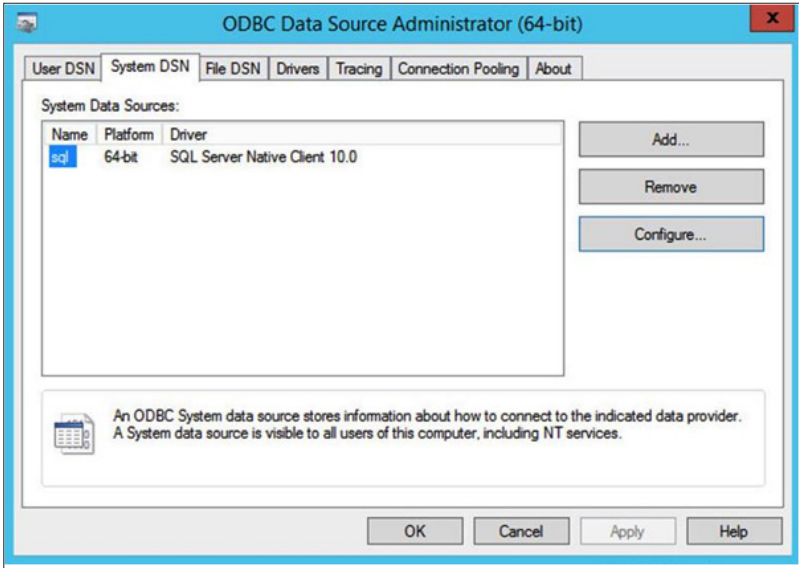


- If your connection test completed successfully, click **OK** to continue.
- If your connection test was unsuccessful, click **OK** and then **Cancel** in the next window to go back and change the parameters in the previous windows, and retest until the test results are successful.

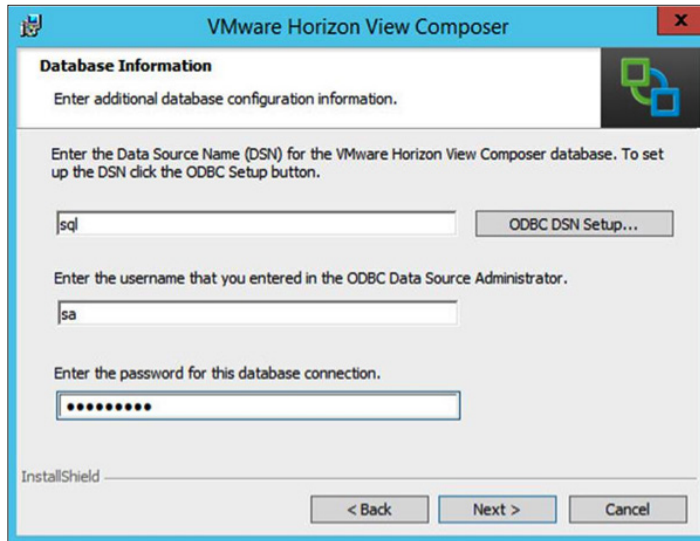
15. Click **OK** to add the System DSN to your ODBC Data Source Administrator List.



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

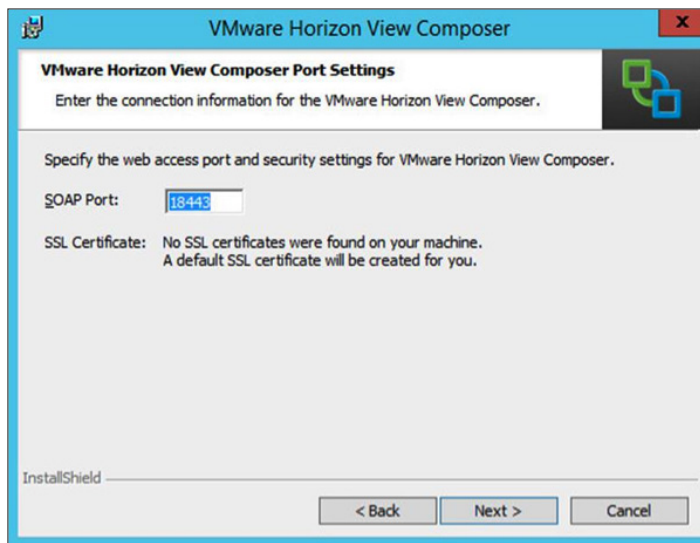


17. After the System DSN is created and the Setup Wizard brings you back to the View Composer Server installer, type the System DSN name, username, and password, and then click **Next**.



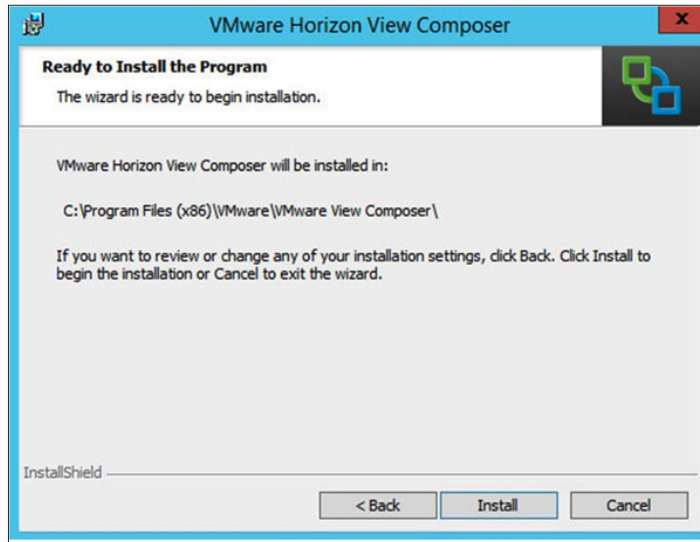
The screenshot shows the 'VMware Horizon View Composer' window with the 'Database Information' tab selected. The window title bar includes the VMware logo and a close button. The main content area has a header 'Database Information' and a sub-header 'Enter additional database configuration information.' Below this, there is a text box for the Data Source Name (DSN) containing 'sql', followed by an 'ODBC DSN Setup...' button. The next section is for the username, with a text box containing 'sa'. The final section is for the password, with a masked text box showing ten dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

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



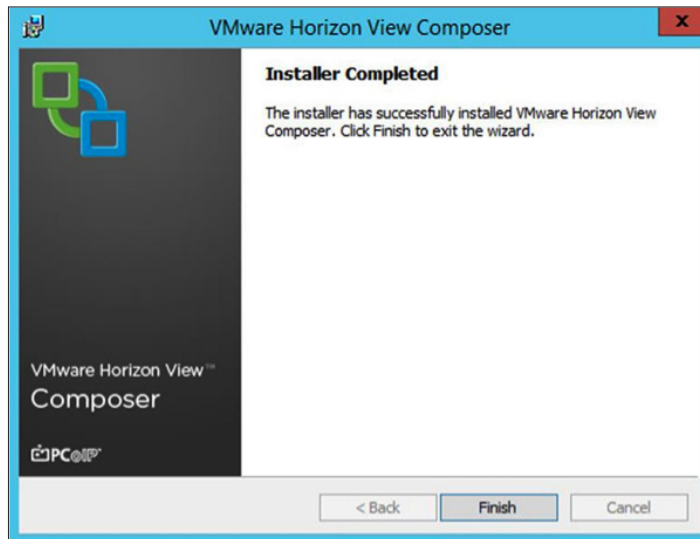
The screenshot shows the 'VMware Horizon View Composer' window with the 'VMware Horizon View Composer Port Settings' tab selected. The window title bar includes the VMware logo and a close button. The main content area has a header 'VMware Horizon View Composer Port Settings' and a sub-header 'Enter the connection information for the VMware Horizon View Composer.' Below this, there is a text box for the SOAP Port containing '18443'. The next section is for the SSL Certificate, with a message stating 'No SSL certificates were found on your machine. A default SSL certificate will be created for you.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

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

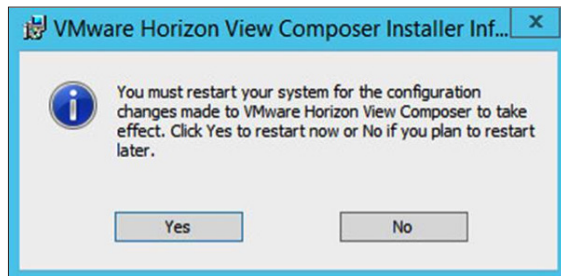


You can monitor the installation progress.

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



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



You are now ready proceed to set up a RDS host to use for application and desktop remoting.

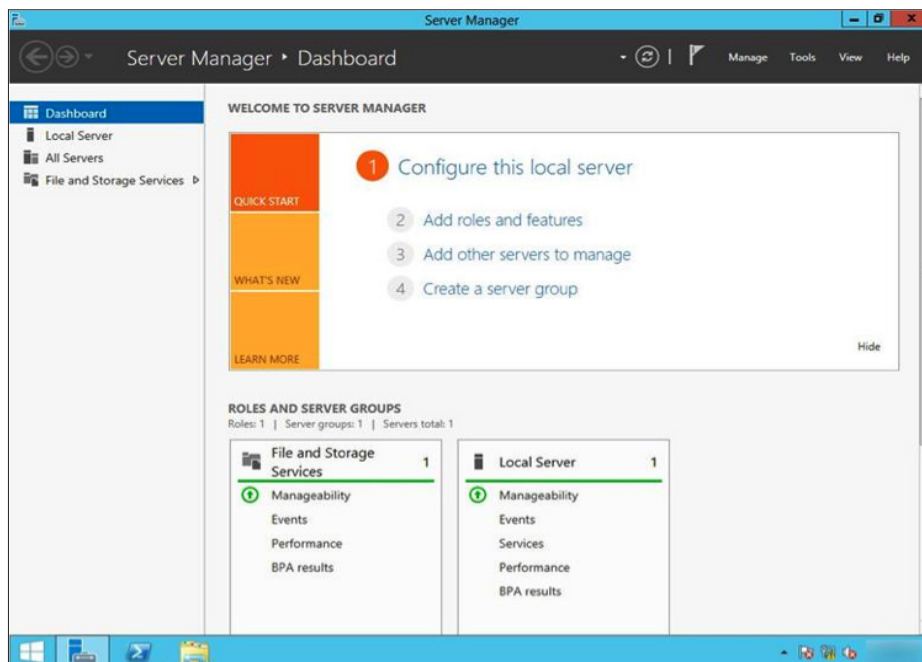
Remote Desktop Session Host Configuration

After installing the View components, you can set up an RDS host. The host is required for setting up RDS desktop and application pools. If you have an existing RDS host that is already configured, you can skip these exercises and proceed to [Configuring View](#). This section contains the following exercises:

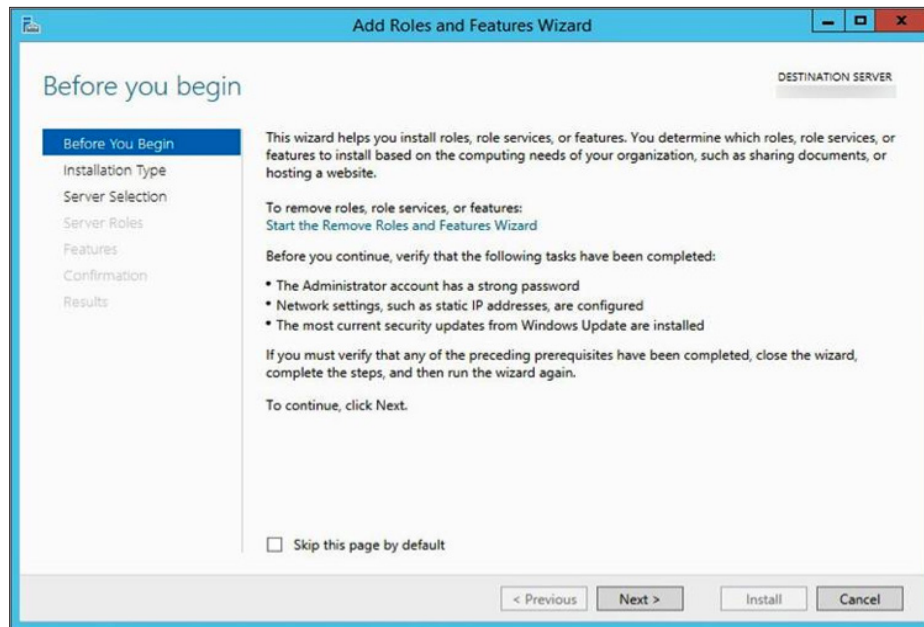
- Set Up a RDS Host on Windows Server 2012 R2
- Install View Agent on an RDS Host

Set Up a RDS Host on Windows Server 2012 R2

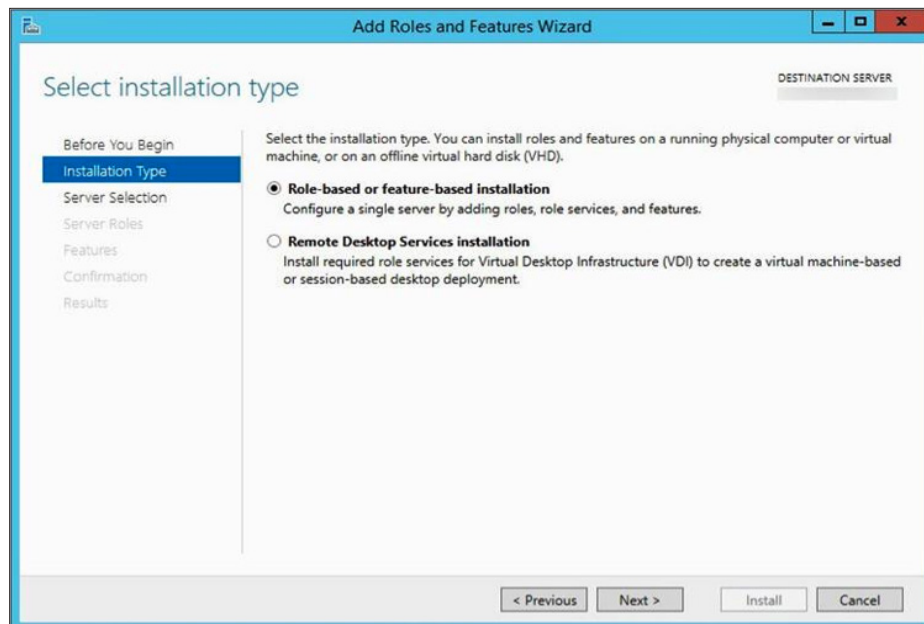
1. Log in as the administrator to the virtual machine that you prepared as your target RDS host and start the Server Manager tool.
2. Click **Add roles and features**.



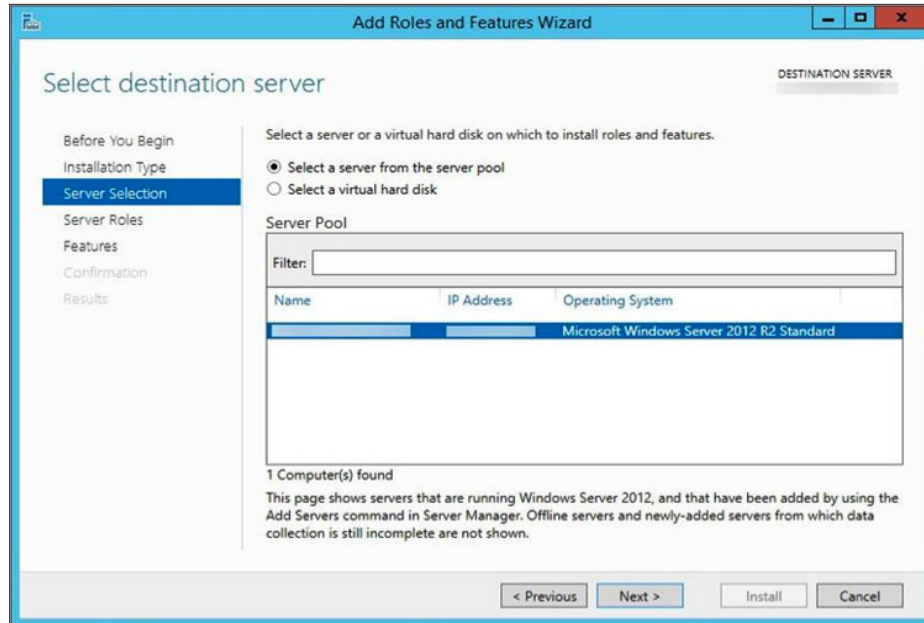
3. To start the Add Roles and Features Wizard, click **Next**.



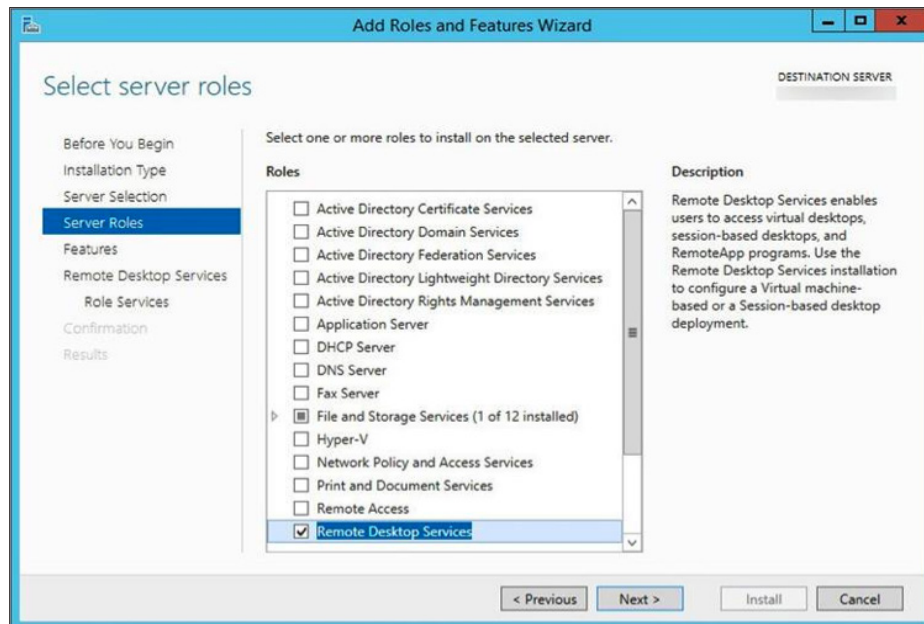
4. To install the RDS role to your server, select **Role-based or feature-based installation**, and then click **Next**.



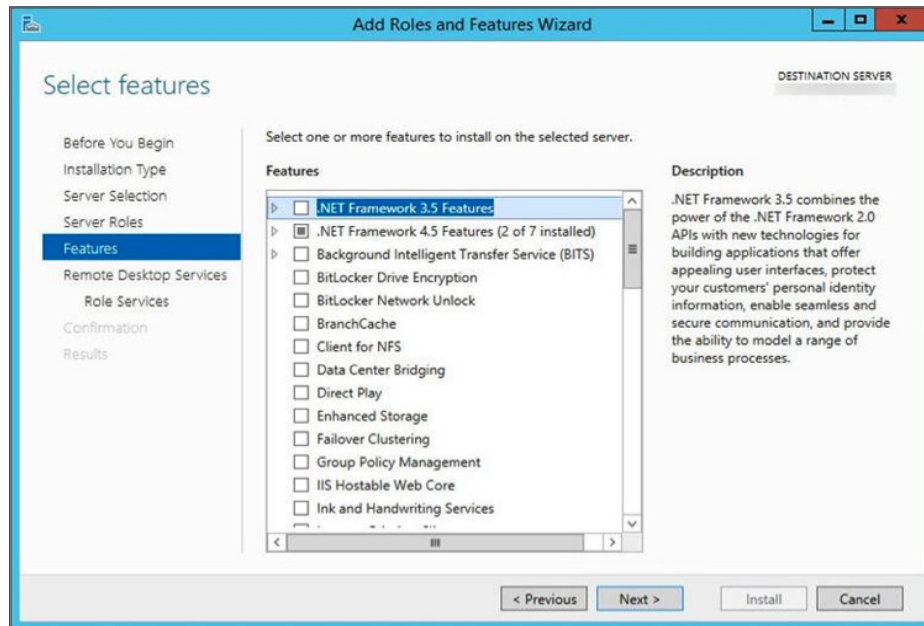
5. Select where to add the role. Because you are installing this role on the server on which you are running the wizard, choose **Select a server from the server pool**, click the name of the server you are logged in to, and then click **Next**.



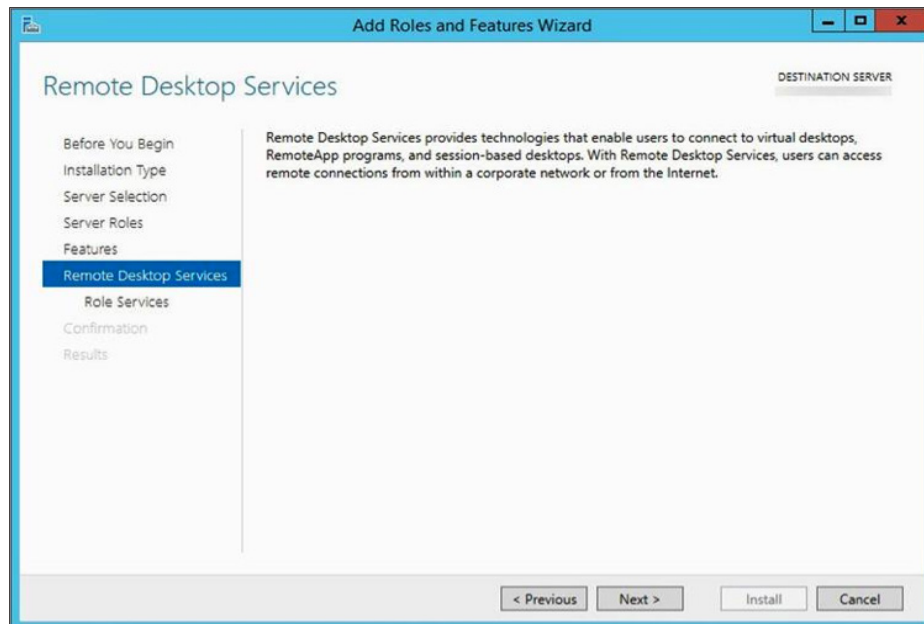
6. In the Roles list, select **Remote Desktop Services** and click **Next**.



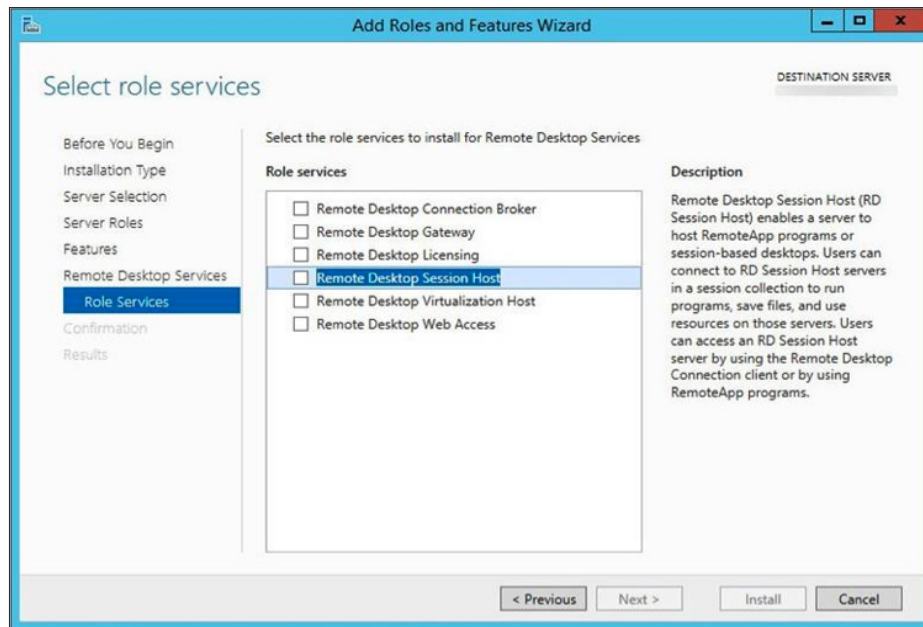
7. On the Select Features page, accept the default features by clicking **Next**.



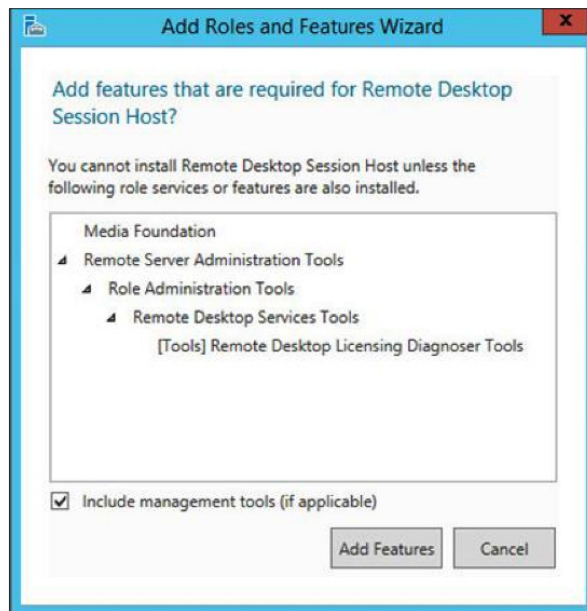
8. Review the Remote Desktop Services role and then click **Next**.



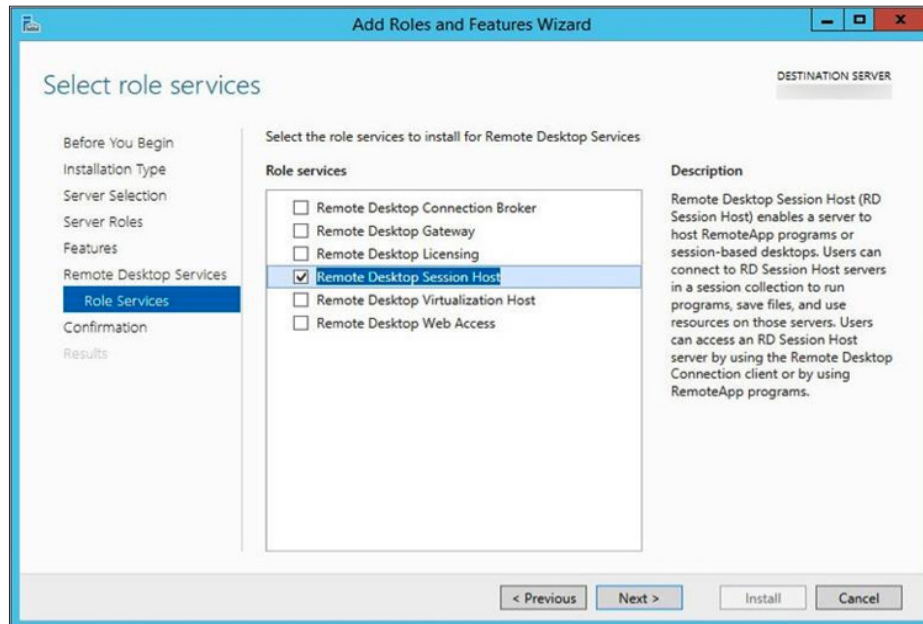
9. In the Role services list, click **Remote Desktop Session Host**.



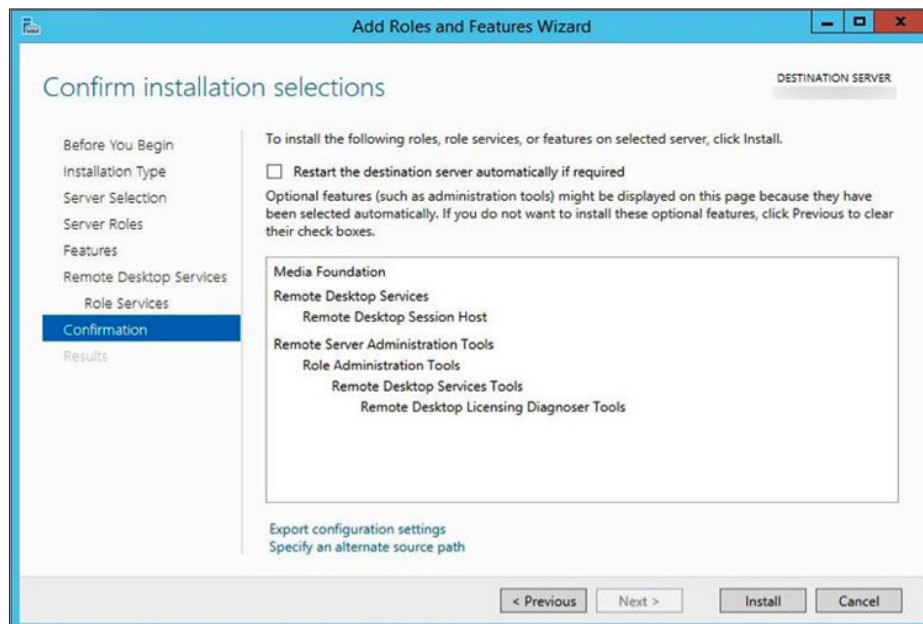
10. The Add Roles and Features Wizard dialog box appears. Click **Add Features**.



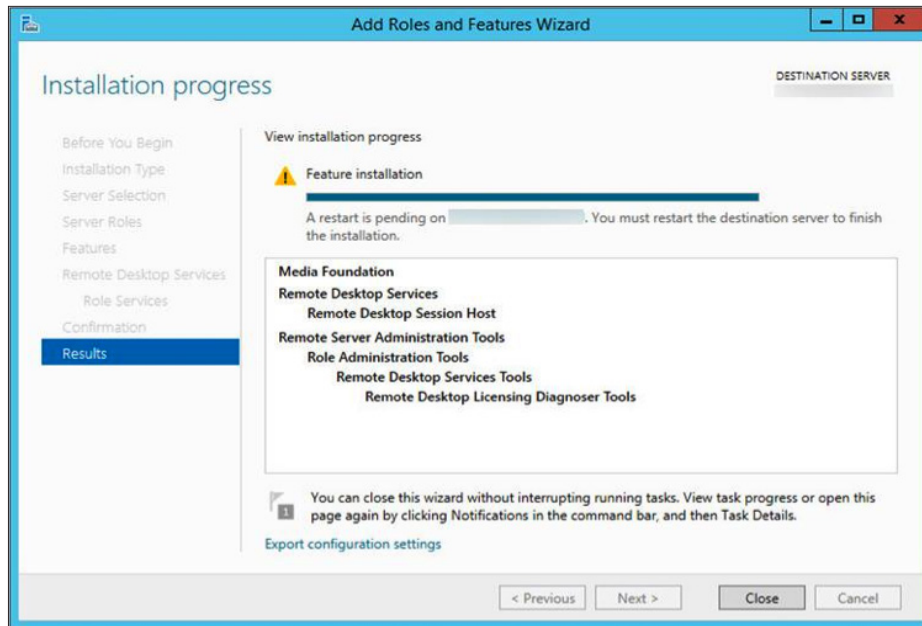
11. The Select role services page appears again with Remote Desktop Session Host highlighted. Click **Next**.



12. Review your selections, and then click **Install**. To make changes, click **Previous**.



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

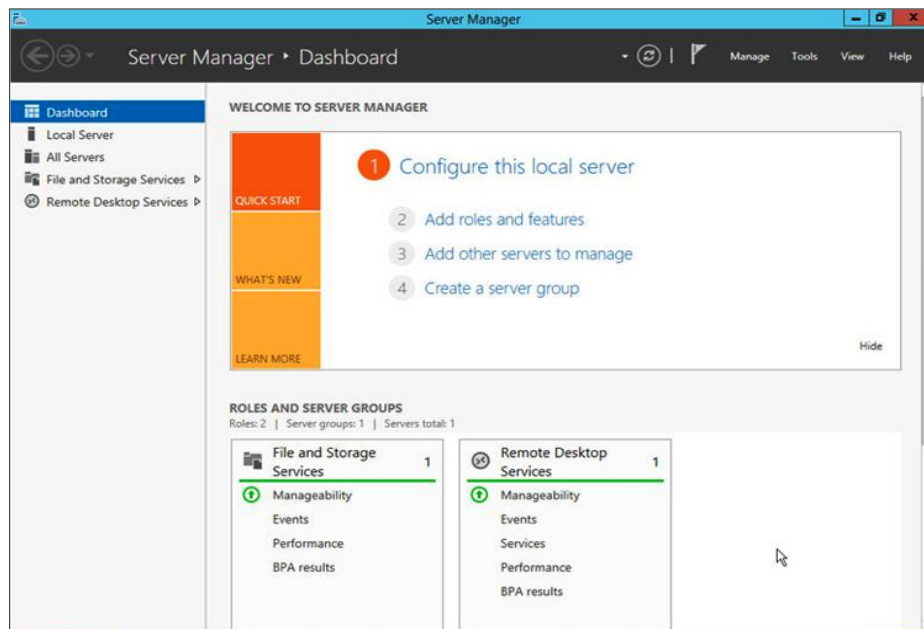


14. Do not turn off your computer while the system is completing the installation.



15. When the installation is finished, log in to your system as administrator and launch the Server Manager to confirm that your installation has completed successfully. The Remote Desktop Services role now appears the Server Manager dashboard.

Note: Be sure to properly license your host. See the article on RD Session Host Licensing at <http://technet.microsoft.com/en-us/library/cc754487.aspx>.

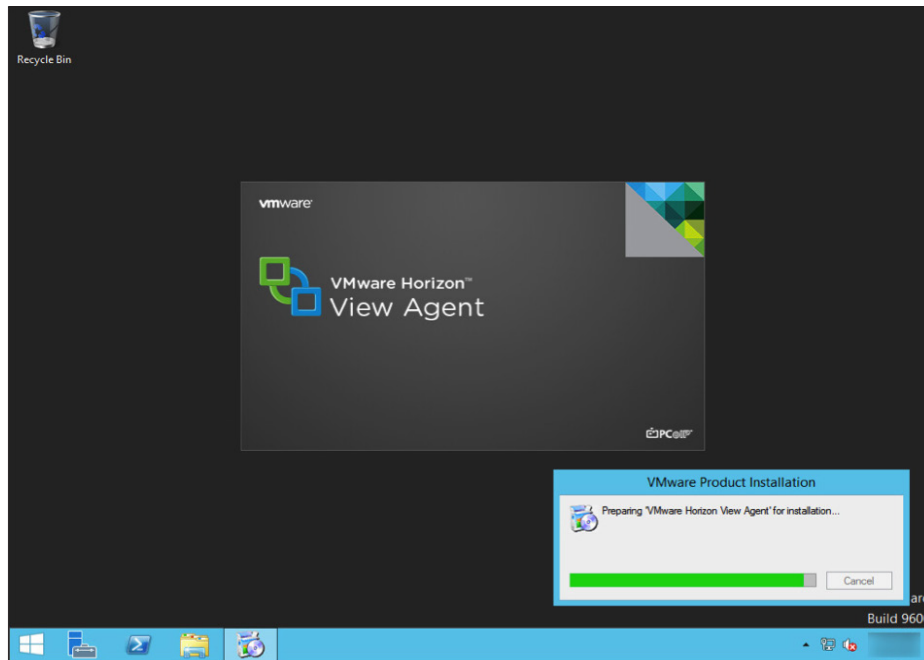


You have successfully configured your RDS host. The next step is to install View Agent on the RDS host.

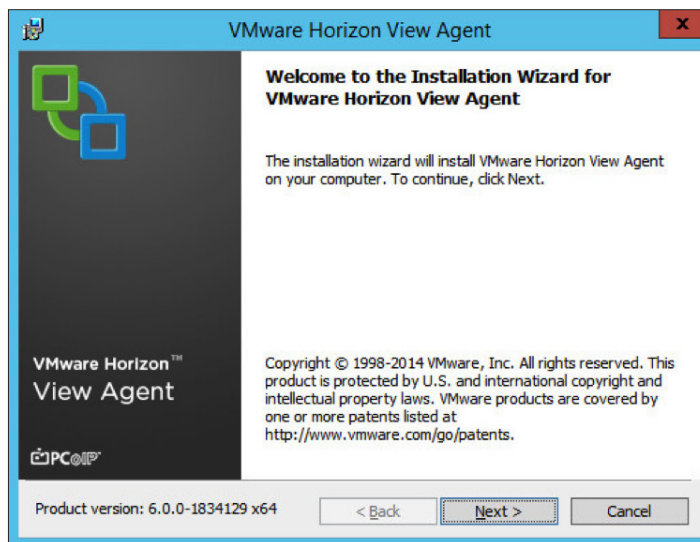
Install View Agent on an RDS Host

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.



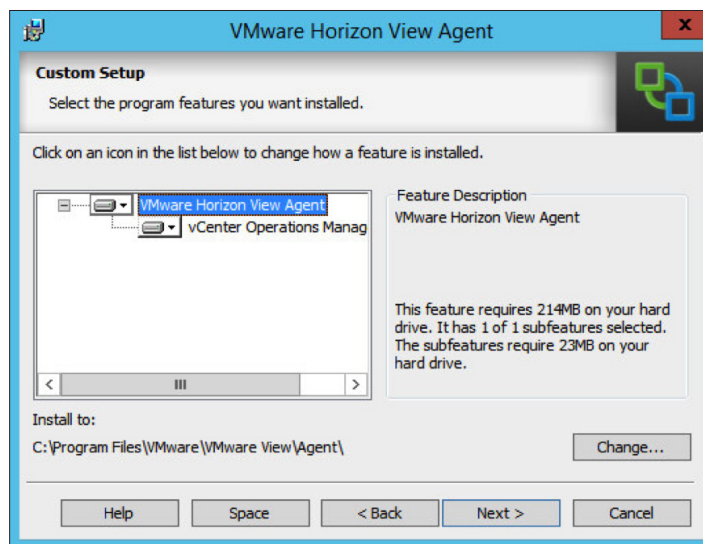
2. When the installer has loaded, click **Next**.



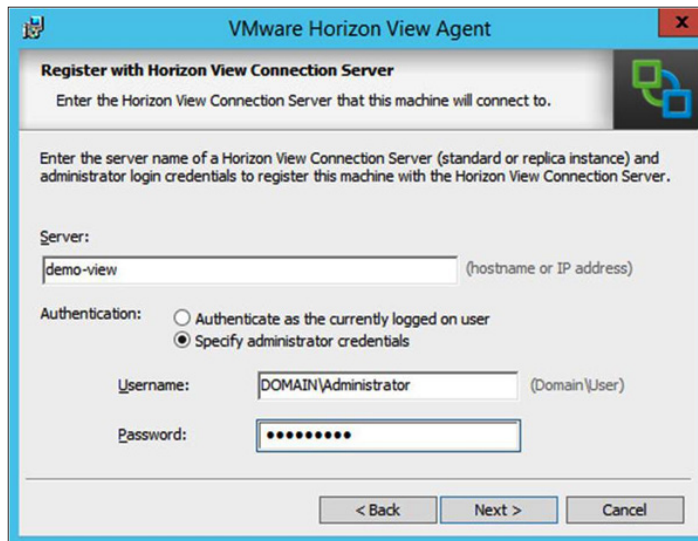
3. Read the license agreement, accept the terms and conditions, and click **Next**.



4. The Custom Setup window lists the features that you can install for View Agent. You can use the default settings. Choose where to install View Agent, and then click **Next**.

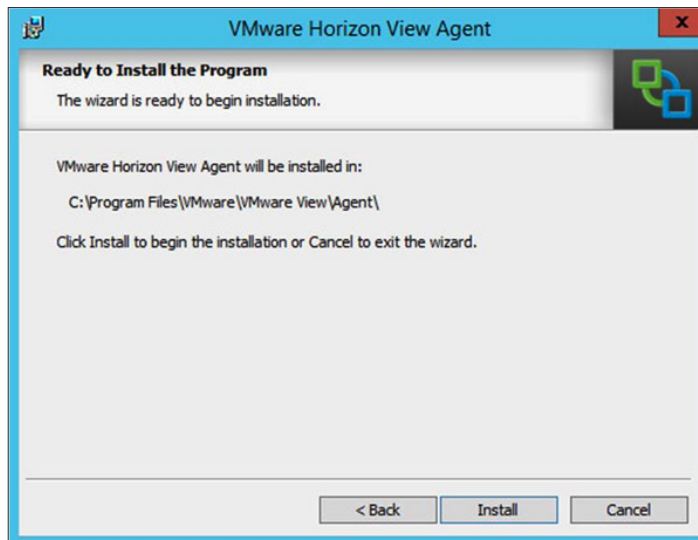


5. Register the RDS host with your View Connection Server.
 - a. In the Server text box, enter the View Connection Server host name.
 - b. Select an authentication method. If you select **Specify administrator credentials**, enter the user name and password.
 - c. Click **Next**.



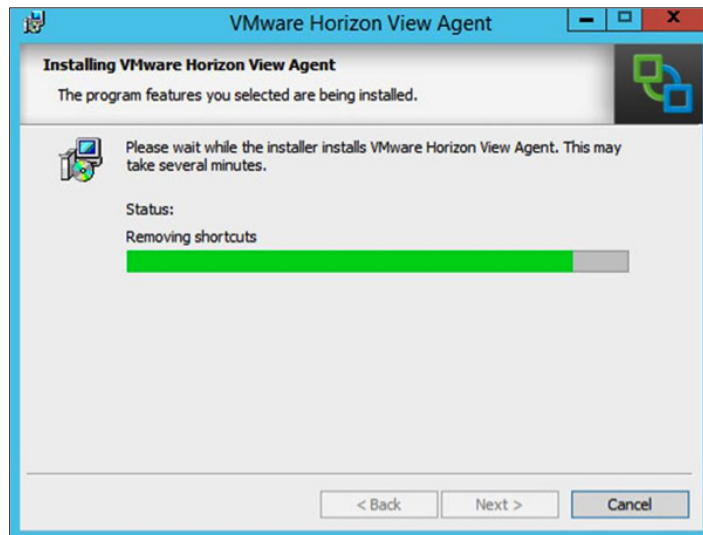
The screenshot shows the 'Register with Horizon View Connection Server' dialog box. The title bar is 'VMware Horizon View Agent'. The main heading is 'Register with Horizon View Connection Server' with a sub-instruction: 'Enter the Horizon View Connection Server that this machine will connect to.' Below this, a text box labeled 'Server:' contains 'demo-view' with a placeholder '(hostname or IP address)'. Under the 'Authentication:' section, the radio button for 'Specify administrator credentials' is selected. The 'Username:' field contains 'DOMAIN\Administrator' with a placeholder '(Domain\User)', and the 'Password:' field is masked with dots. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

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

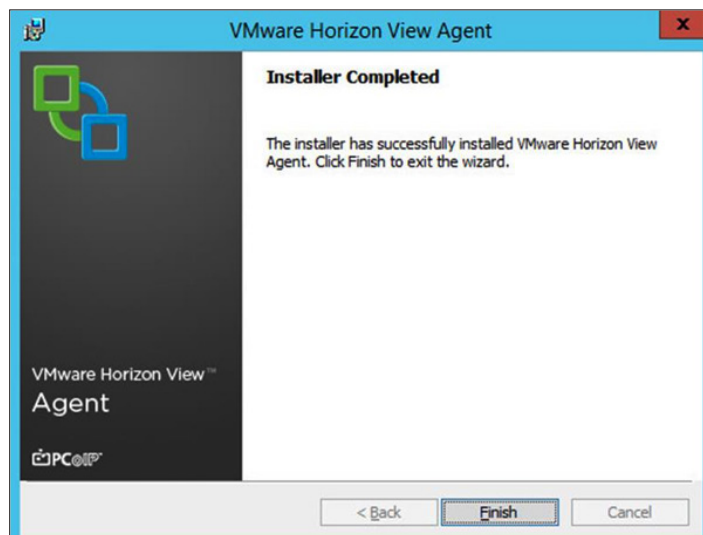


The screenshot shows the 'Ready to Install the Program' dialog box. The title bar is 'VMware Horizon View Agent'. The main heading is 'Ready to Install the Program' with a sub-instruction: 'The wizard is ready to begin installation.' Below this, it states 'VMware Horizon View Agent will be installed in:' followed by the path '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 are buttons for '< Back', 'Install', and 'Cancel'.

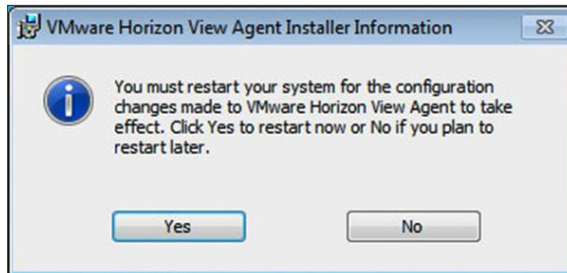
7. Monitor your installation status as it progresses.



8. The Installer Completed window appears when the installation is finished. Click **Finish** to close the View Agent installer.



- To complete the installation, you must restart the operating system. Click **Yes** to initiate the restart.

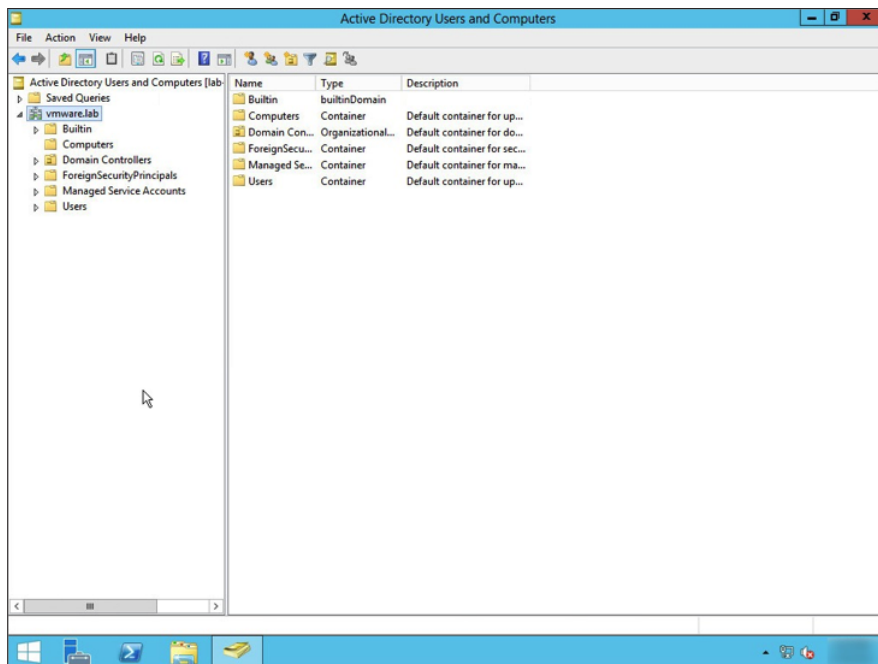


You have now completed installing the RDS Host. The next series of exercises walks you through configuring View.

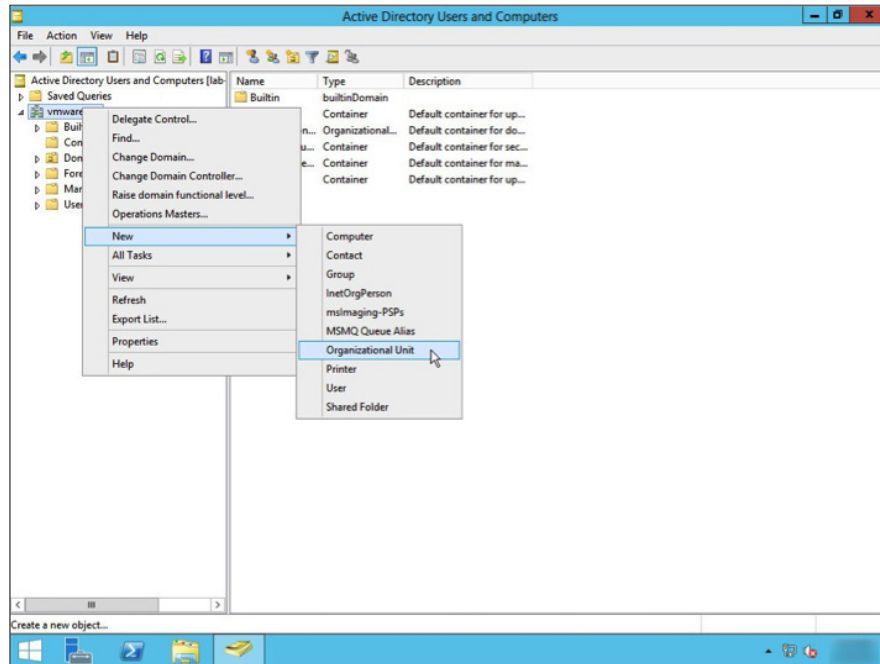
Configure Group Policy Setting fro RDS Host Sessions

After we have deployed and configured our Remote Sessions Host, we must configure user security and access setting for Remote Desktop Session services. We will define these settings as Group Policy Objects.

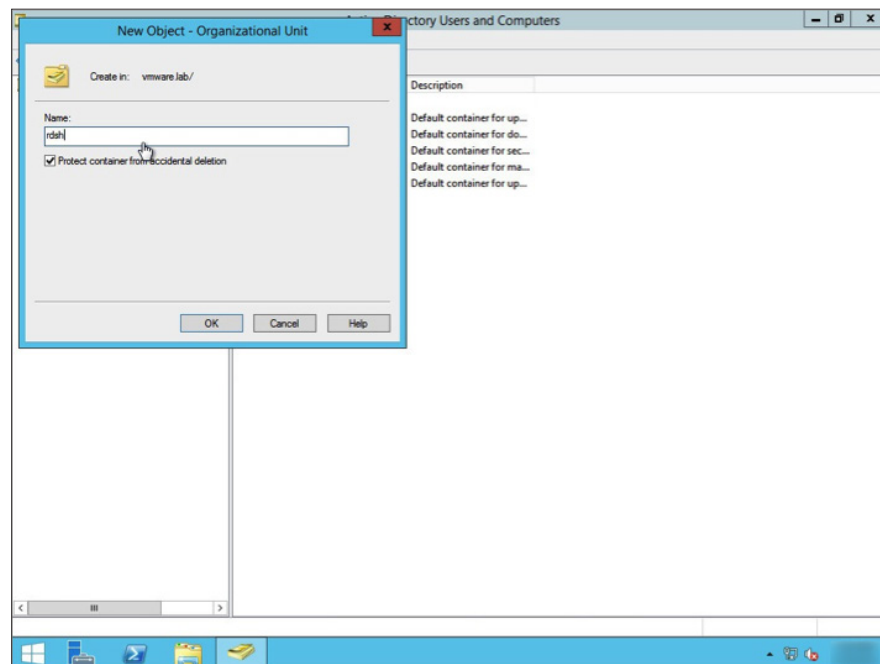
- First we will create an Organizational Unit (OU) for oru RDS Hosts. Log in as the Administrator to your Active Directory Users and Computers and highlight the domain.



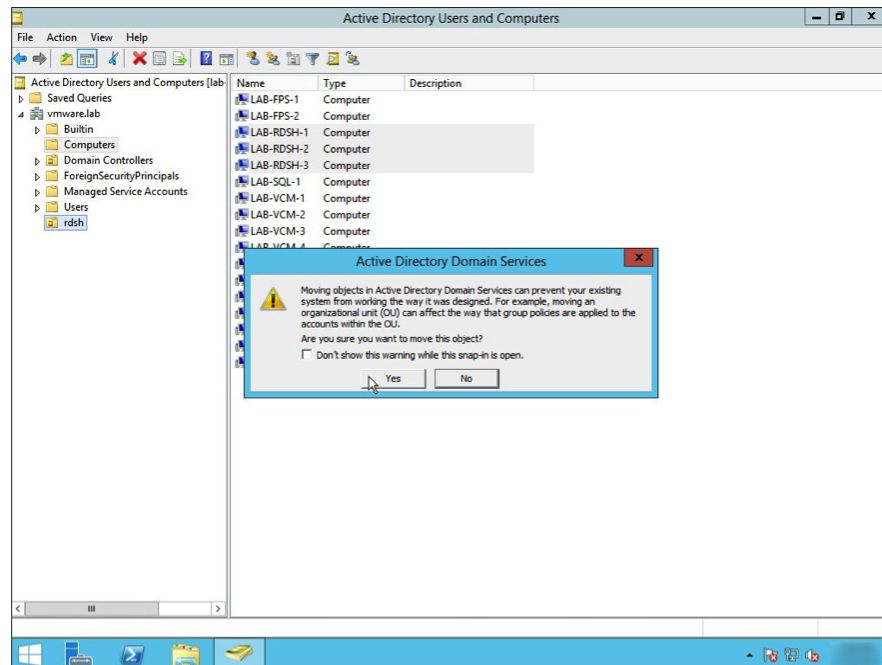
2. Right-click your target domain and go to **New > Organizational Unit**.



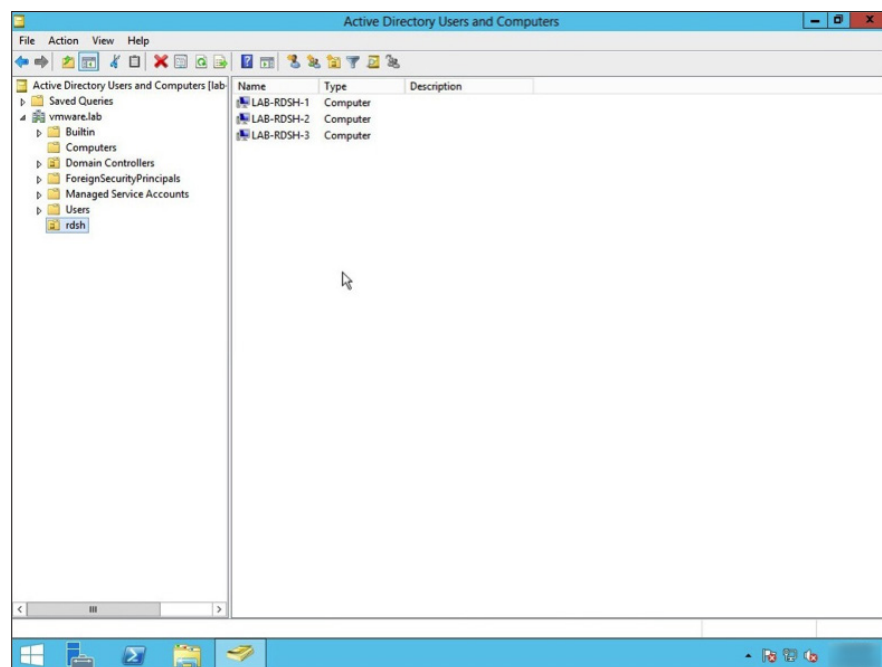
3. Fill in a name for your Organization and click **OK**.



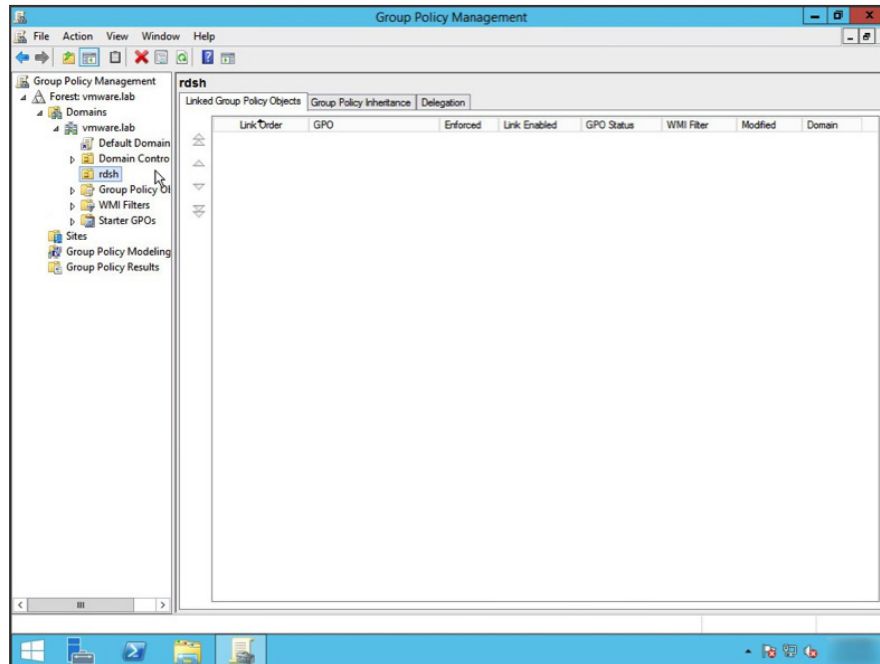
- Under your domain, you will see that the OU Group was created. Click the **Computers** folders for your domain, highlight the Computer Names for your RDS Host(s), and drag and drop them to your new OU Group. A warning message appears. Click **Yes**.



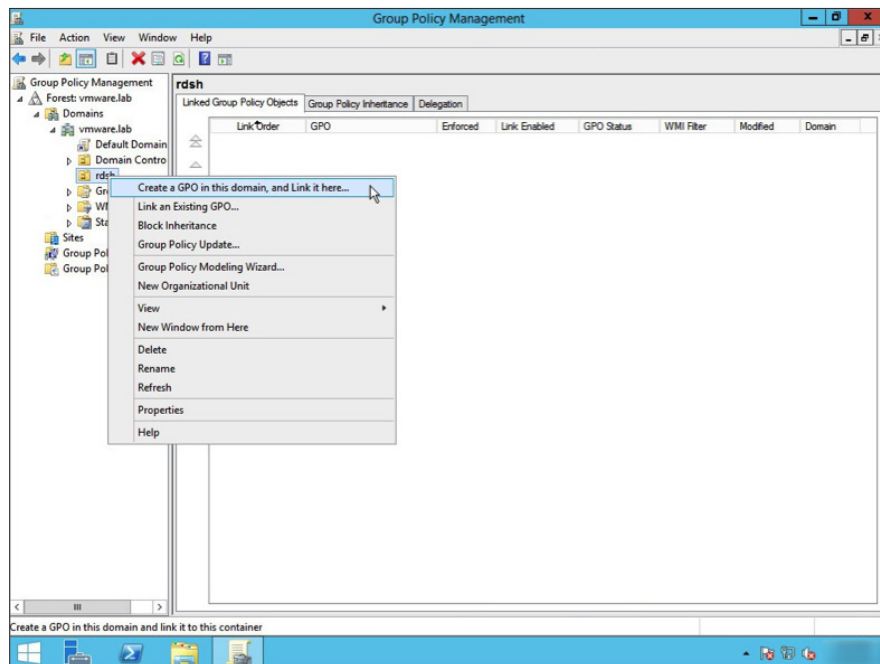
- Click the Organizationa Unit (OU) Group that you created to verify that all your Remote Desktop Session Hosts are now part of the OU Group.



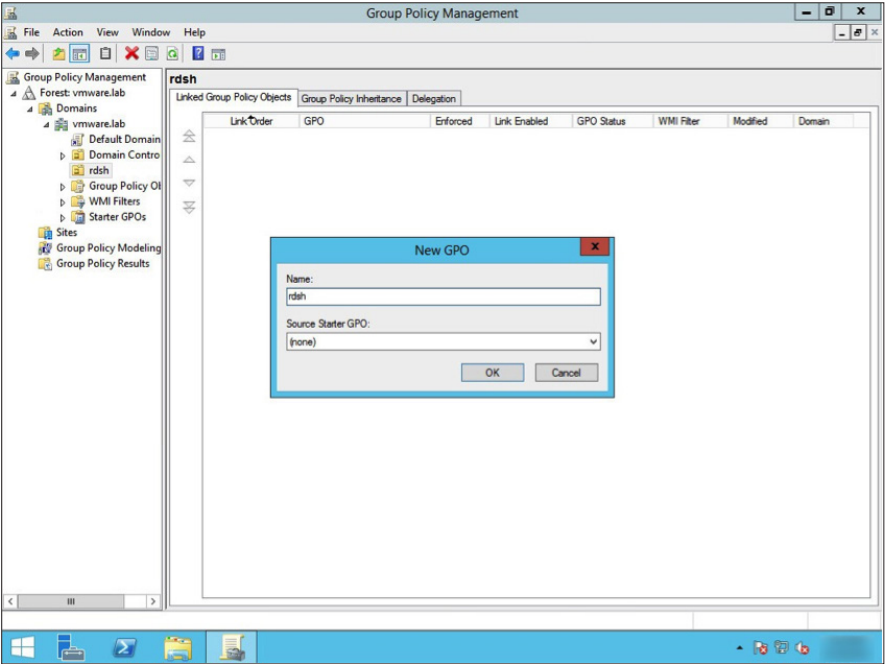
6. Launch the Group Policy Management utility. Expand the tree hierarchy for your domain and highlight the RDS Host Organizational Unit (OU) Group that you created in the previous steps.



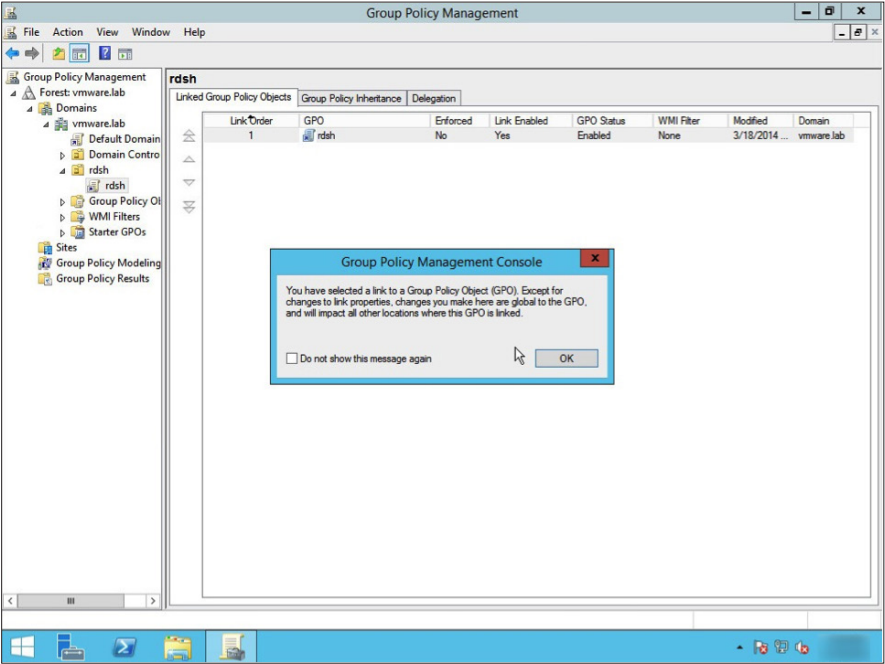
7. Right-click the OU Group and select **Create a GPO in this domain, and Link it here...**



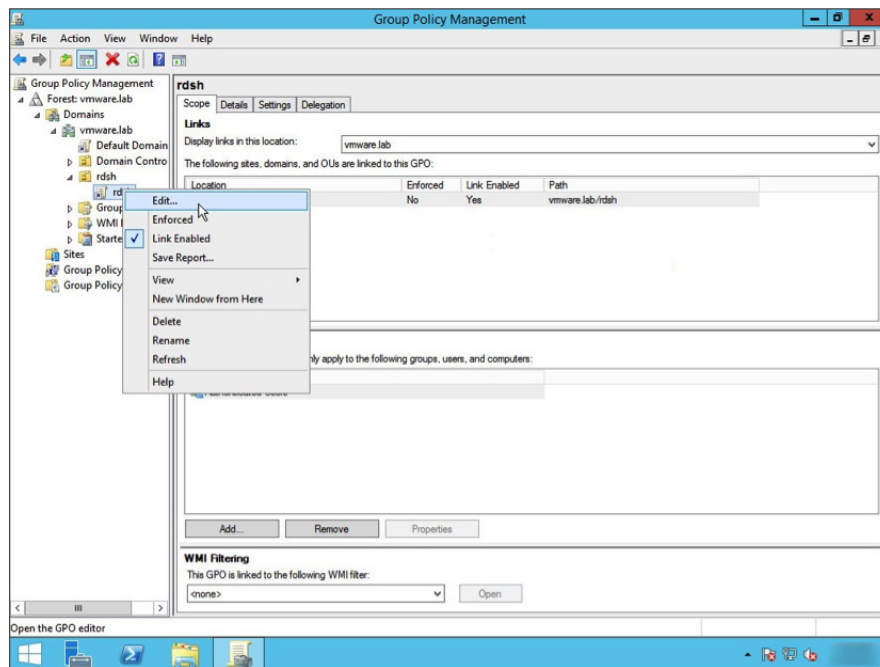
8. Enter a name for the new GPO and click **OK**.



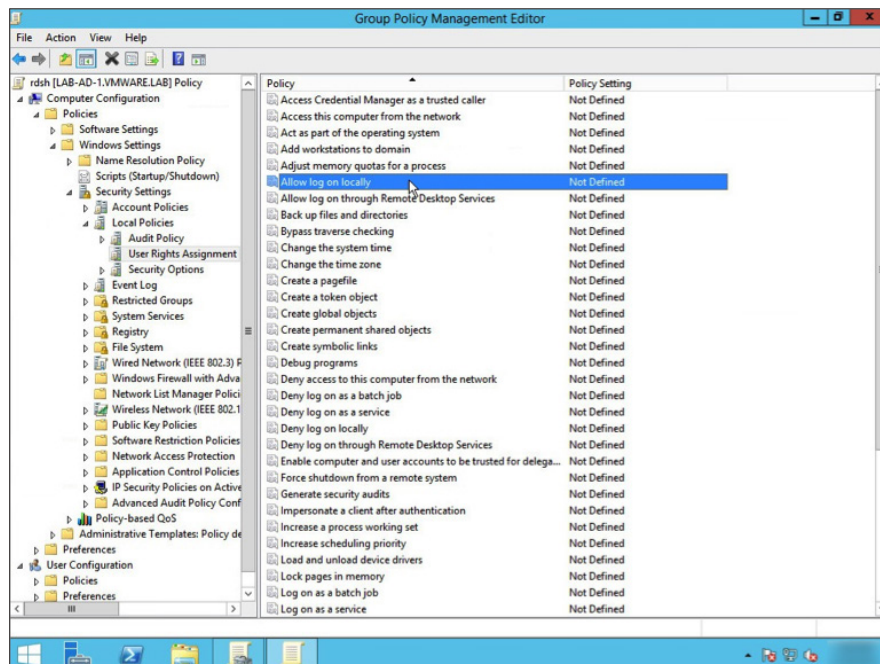
9. A Group Policy Management Console warning appears about GPO links. Click **OK**.



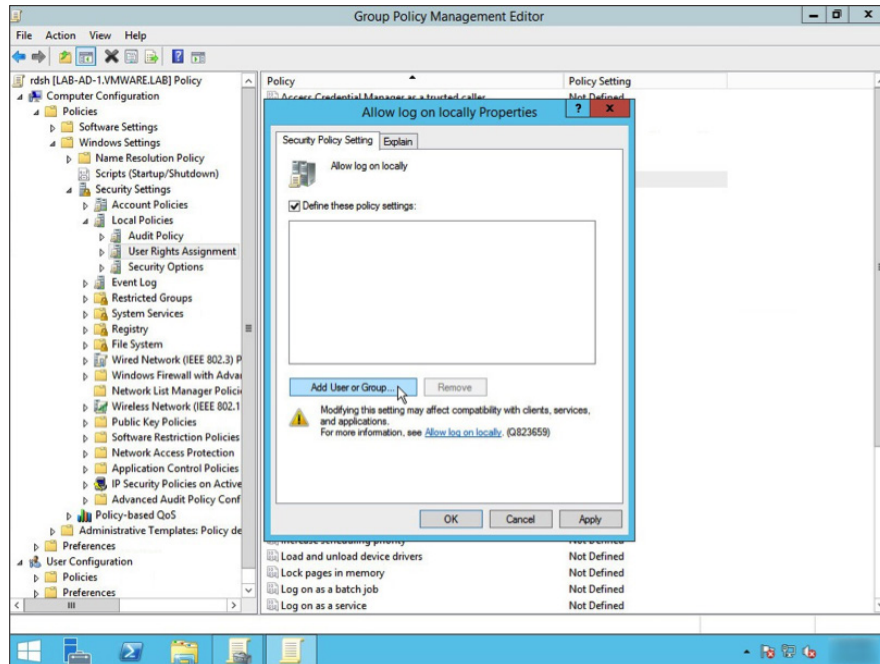
10. Right-click your Group Policy Object, and click **Edit...**



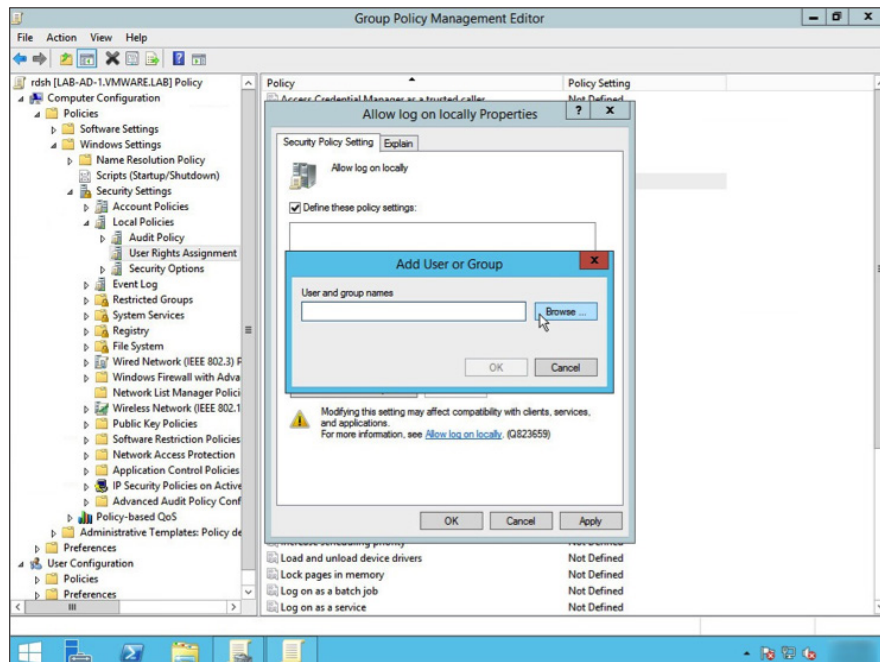
11. You will now be in the Group Policy Management Editor for your Remote Desktop Session Host policy. Navigate to **Computer Configuration > Policies > Window Settings > Security Settings > Local Policies > User Rights Assignment**. Click **Allow log on locally**.



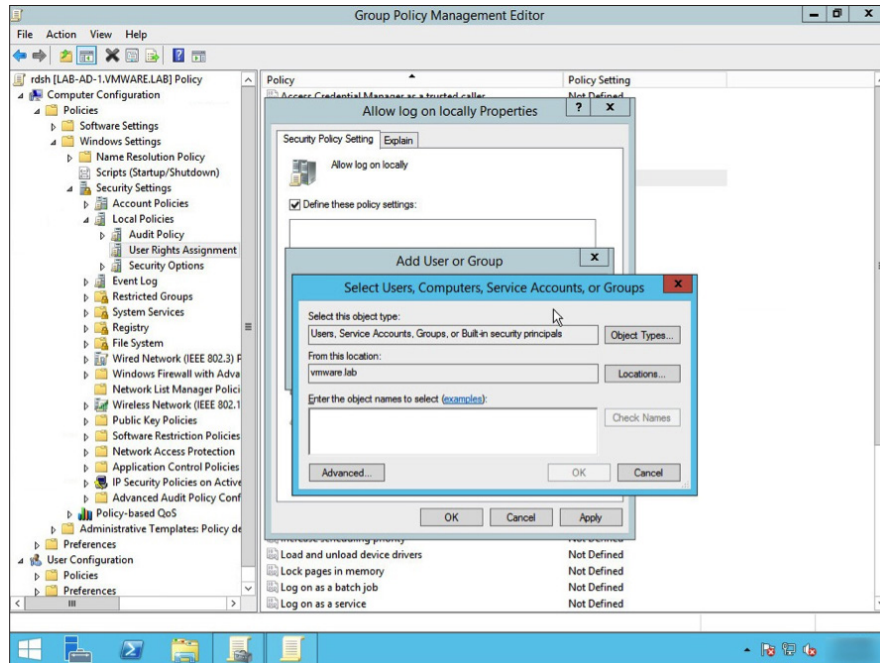
12. The Allow log on locally Properties menu appears. Ensure the check box for **Define these policy settings** is checked and click **Add User or Group...**



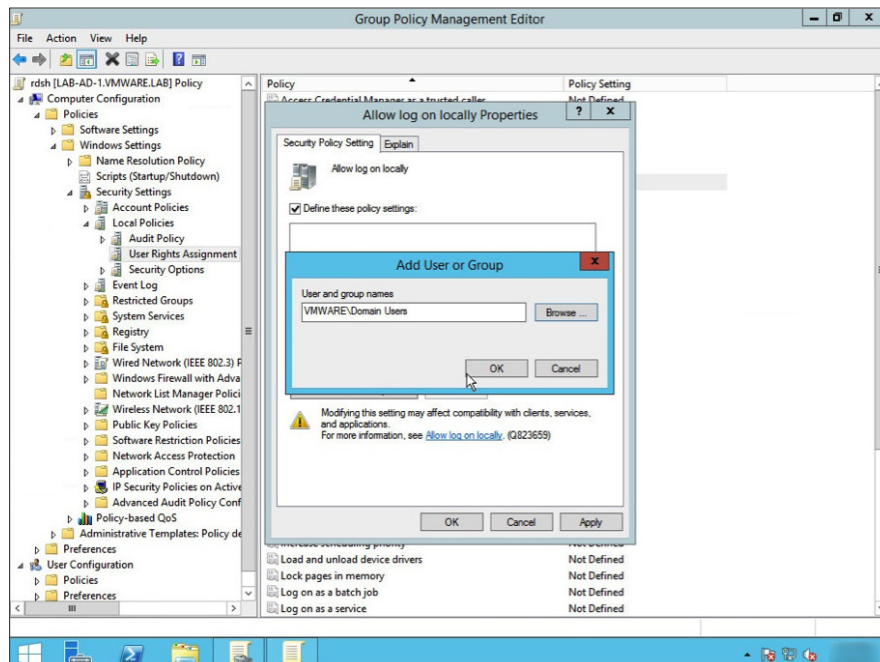
13. Now you will define which users or groups you will give access to allow local log in. Click **Browse**.



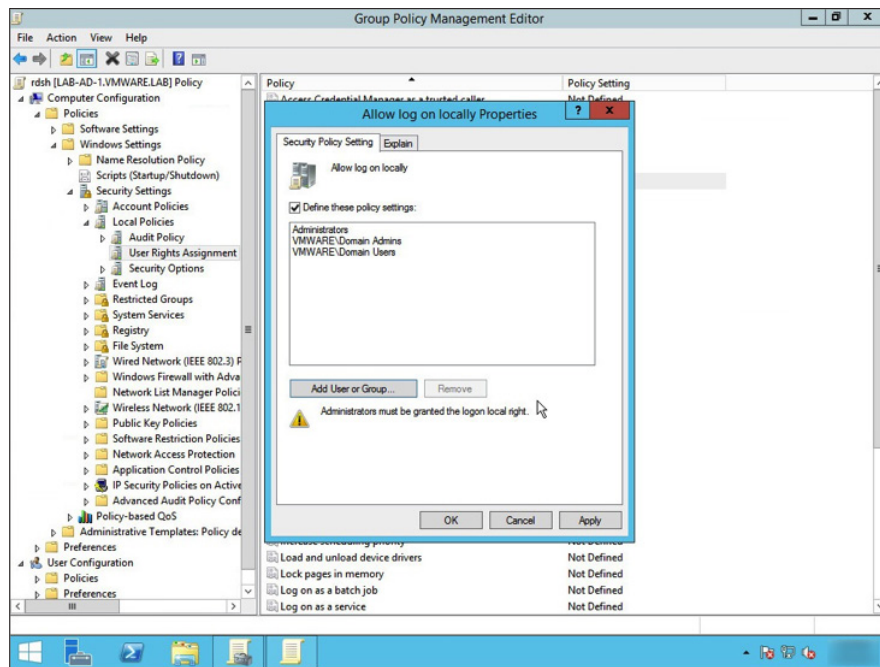
14. Enter the names of the users or groups that you will allow access in the **Enter the object names to select** field and click **OK**.



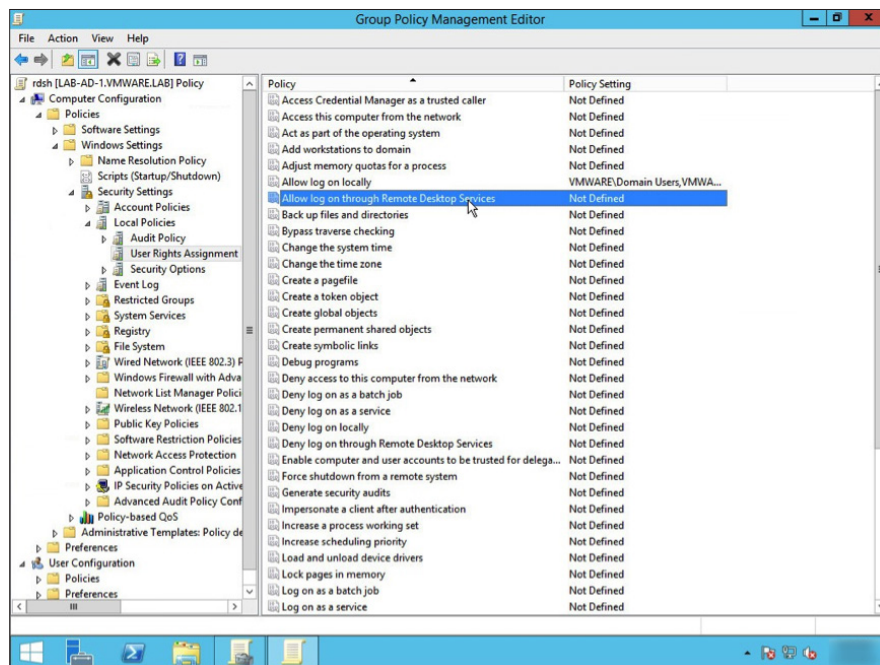
15. Verify that you are adding the correct users or groups, then click **OK**.



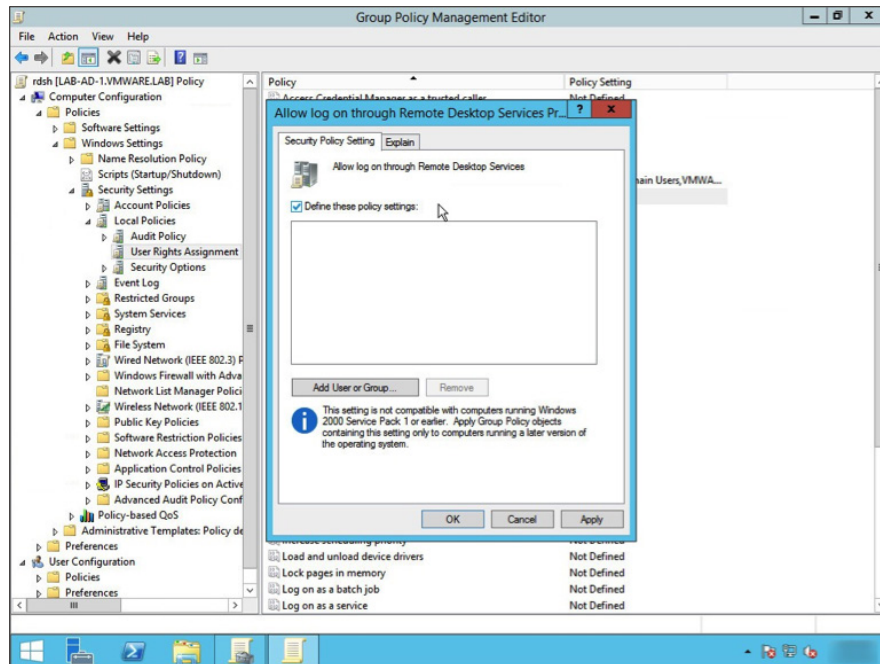
16. Verify that you have added all the users or groups you wish to authorize and click **OK**. If you need to add additional users or groups, click **Add User or Groups...** to go through the previous menus and make the necessary changes.



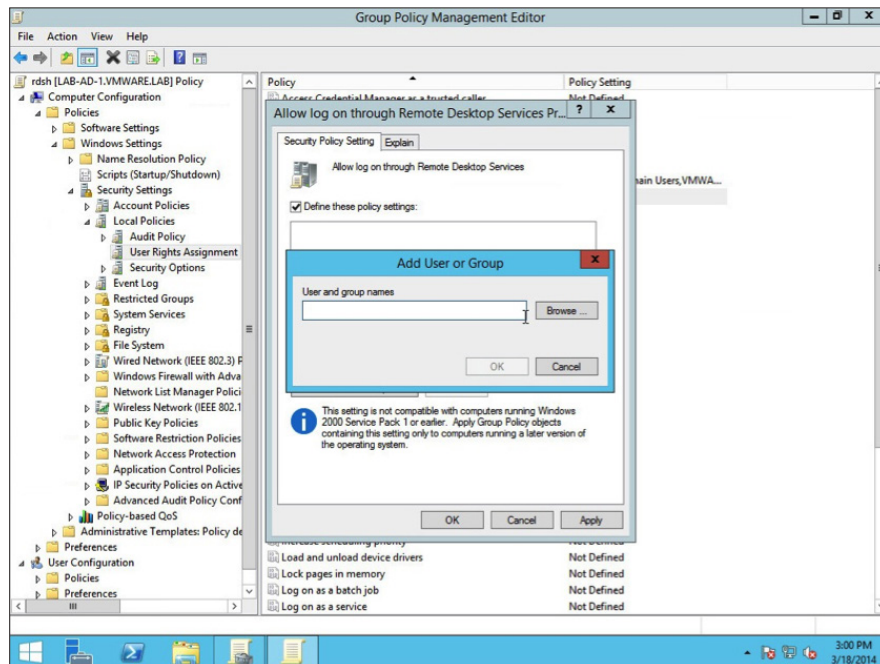
17. You will return to the Group Policy Management Editor. Click the policy **Allow log on through Remote Desktop Services**.



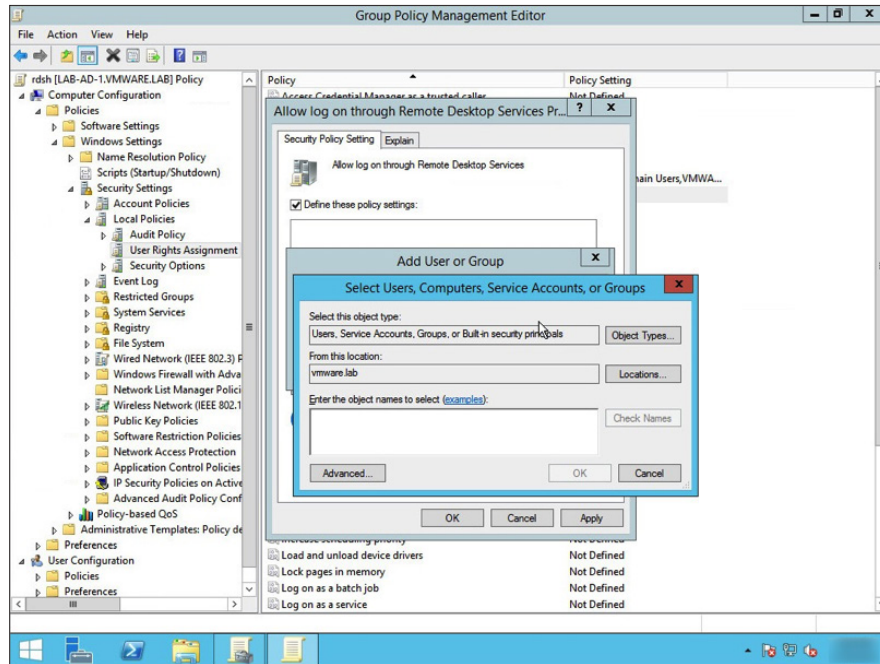
18. The Allow log on locally Properties menu will appear. Ensure the check box for **Define these policy settings** is checked and click **Add User or Group...**



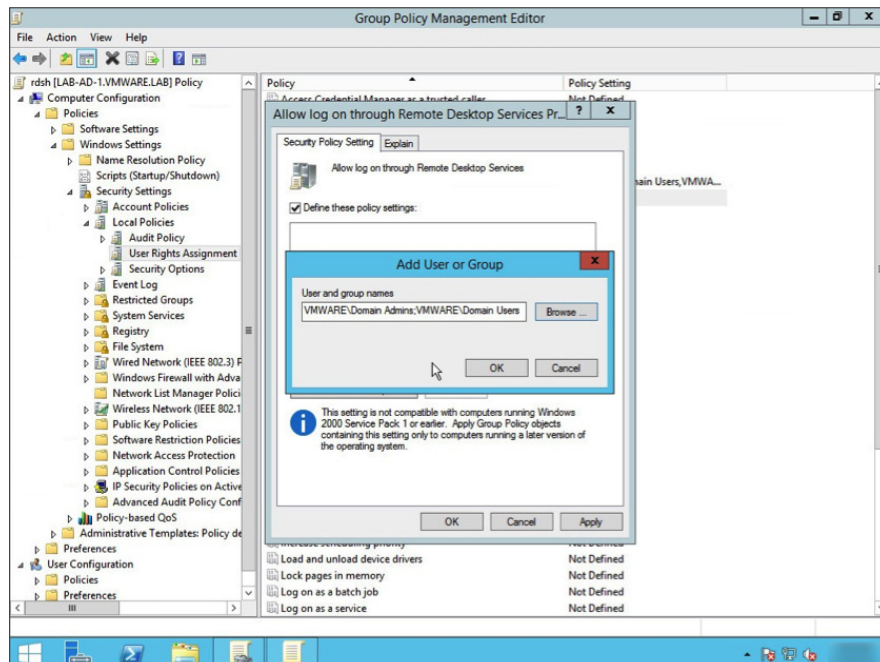
19. Now we will define which users or groups we will allow for this policy. Click **Browse**.



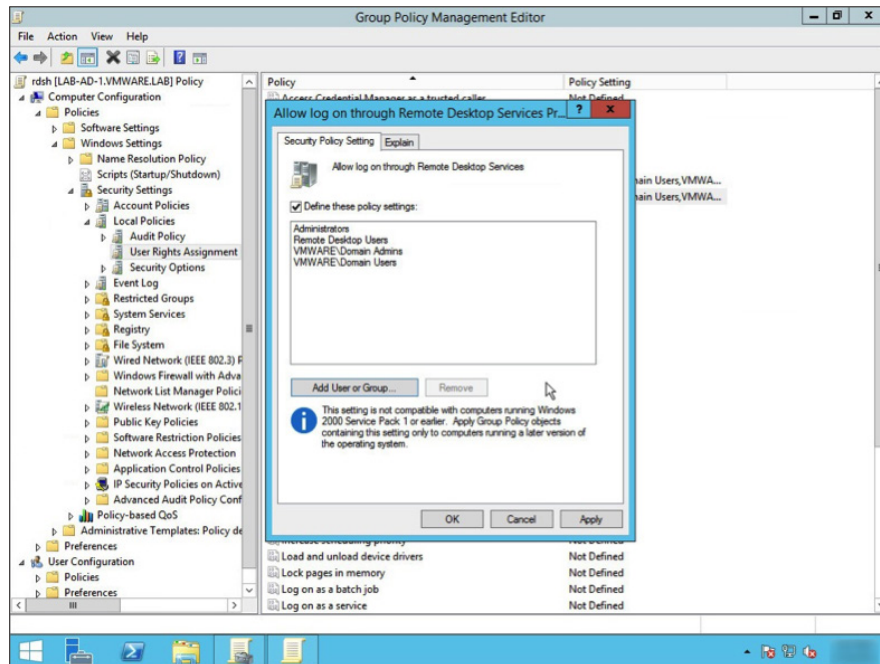
20. Enter the names of the user or groups that you will allow access in the **Enter the object names to select** field and click **OK**.



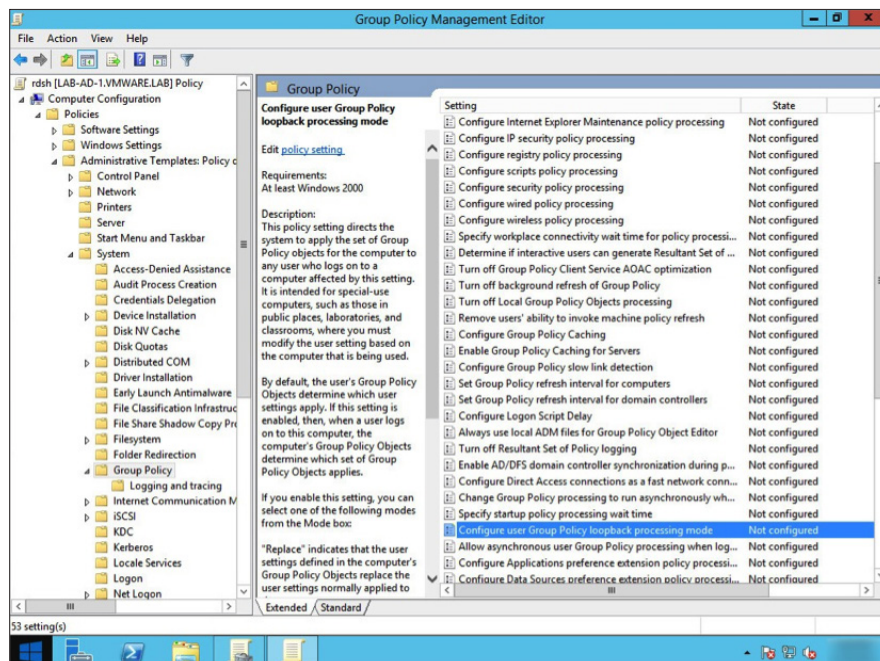
21. Verify that you are adding the correct users or groups, then click **OK**.



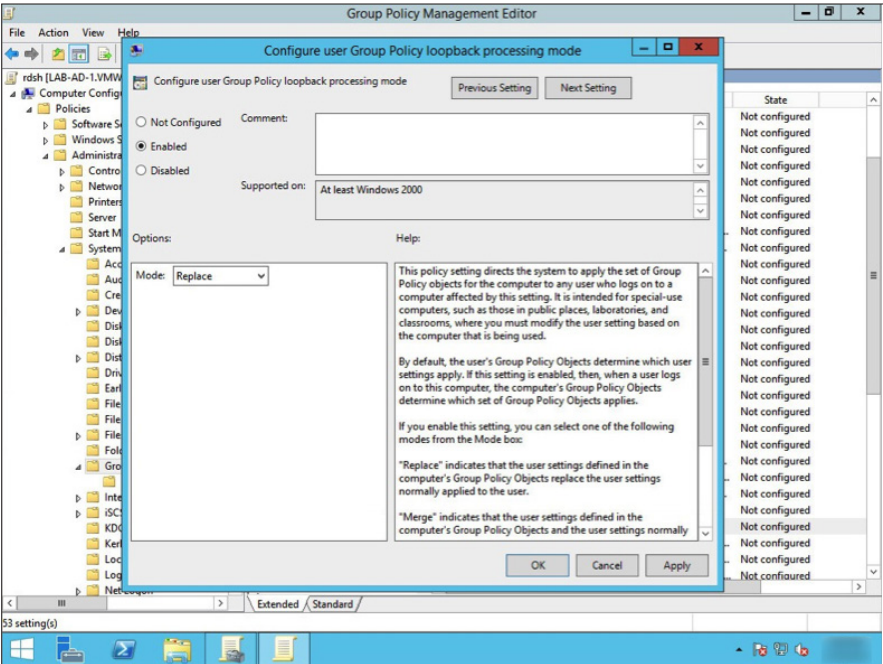
22. Verify that you have added all the users or groups you wish to authorize and click **OK**. If you need to add additional users or groups click **Add User or Group...** to go through the previous menus and make the necessary changes.



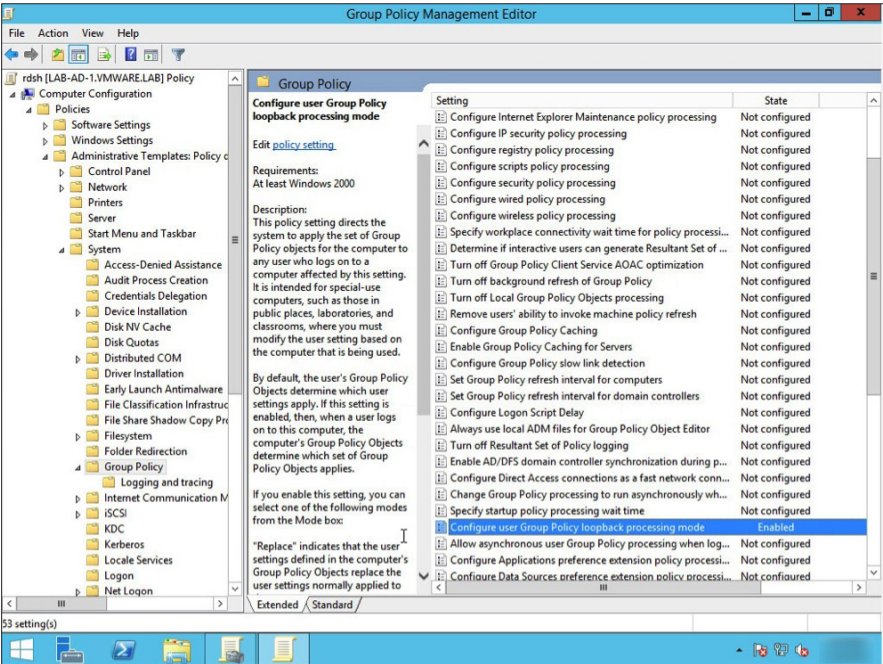
23. You will return to the Group Policy Management Editor. Navigate to the **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine. > System > Group Policy**. Click the policy **Configure user Group Policy loopback processing mode**.



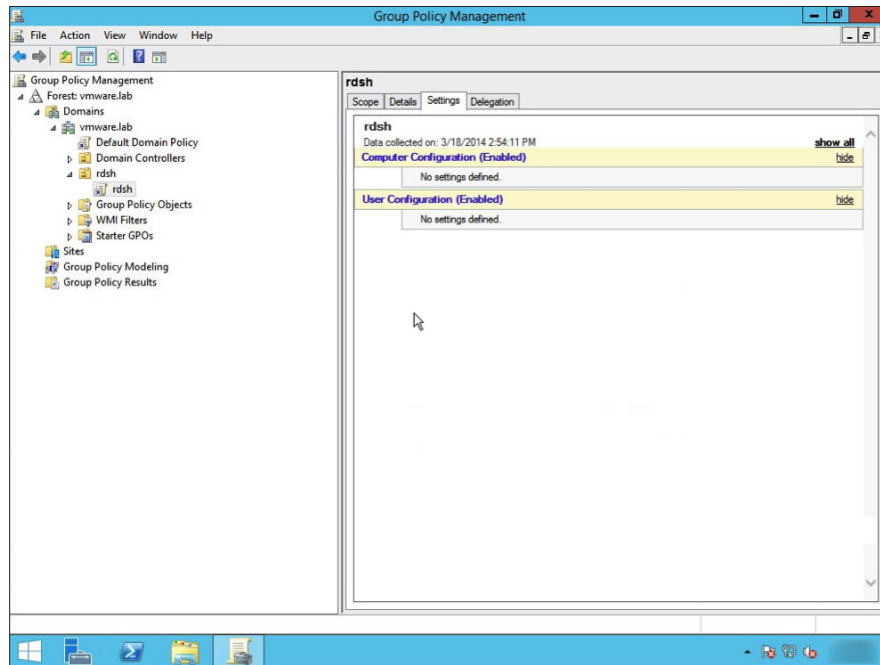
24. Click **Enabled** to enable this policy. Click **OK**.



25. You will return to the Group Policy Management Editor. Verify that your policy is enabled by ensuring the that the State value for the policy has change to Enabled.



26. Now you may close the window for the Group Policy Management Editor. You will return to the Group Policy Management window.



Now you have successfully configured the Group Policy Setting for user access to Remote Desktop Session services.

Configuring View

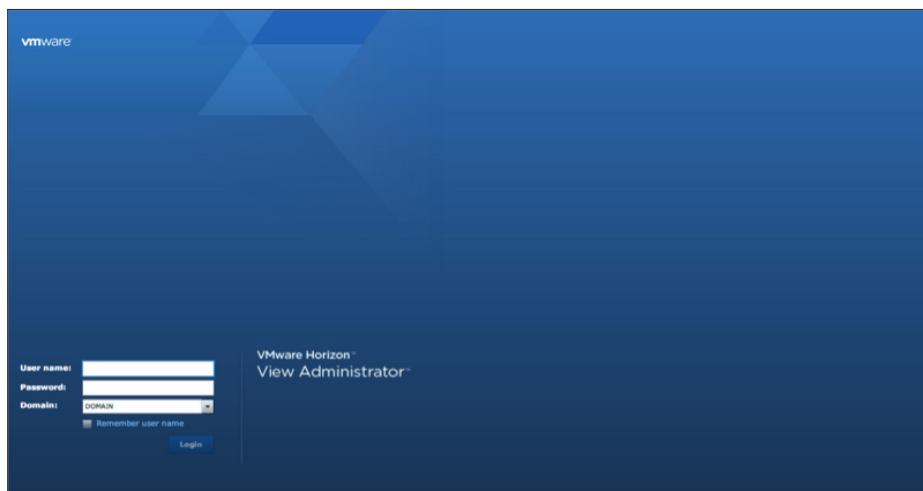
After you have installed the View component servers, you are ready to configure View. This section contains the following exercises:

- [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](#)

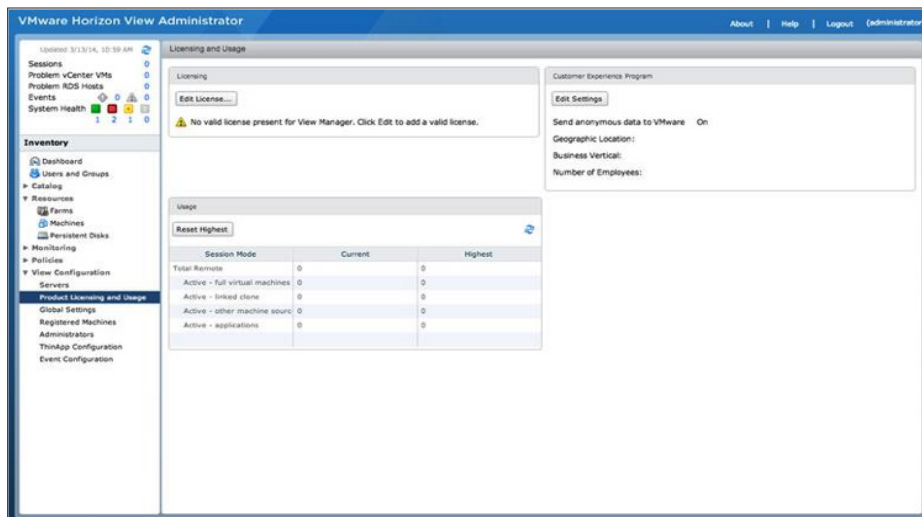
Add a License

You must have a valid license to use View.

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



2. In the left menu, click **Product Licensing and Usage**, and then click **Edit License** in the Licensing section.

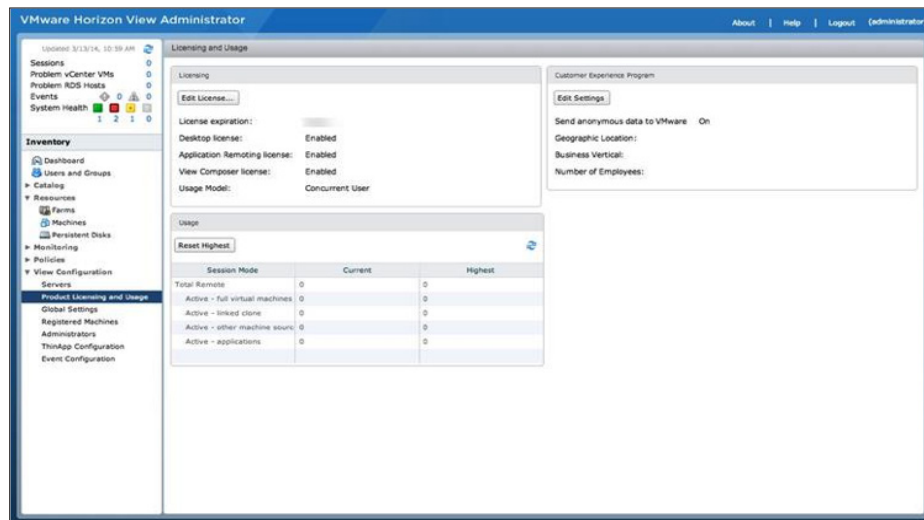


3. Enter a valid license serial number and click **OK**.



The 'Edit License' dialog box has a title bar 'Edit License'. Below the title bar, there is a label 'License serial number:' followed by a red asterisk and a text input field. At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

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



The screenshot shows the 'VMware Horizon View Administrator' interface. The left sidebar contains a navigation tree with 'View Configuration' expanded and 'Servers' selected. The main pane is titled 'Licensing and Usage'. It contains two sections: 'Licensing' and 'Usage'.

Licensing Section:

- License expiration: (button)
- Desktop license: Enabled
- Application Remoting license: Enabled
- View Composer license: Enabled
- Usage Model: Concurrent User

Usage Section:

Reset Highest (button)

Session Mode	Current	Highest
Total Remote	0	0
Active - full virtual machines	0	0
Active - linked clone	0	0
Active - other machine source	0	0
Active - applications	0	0

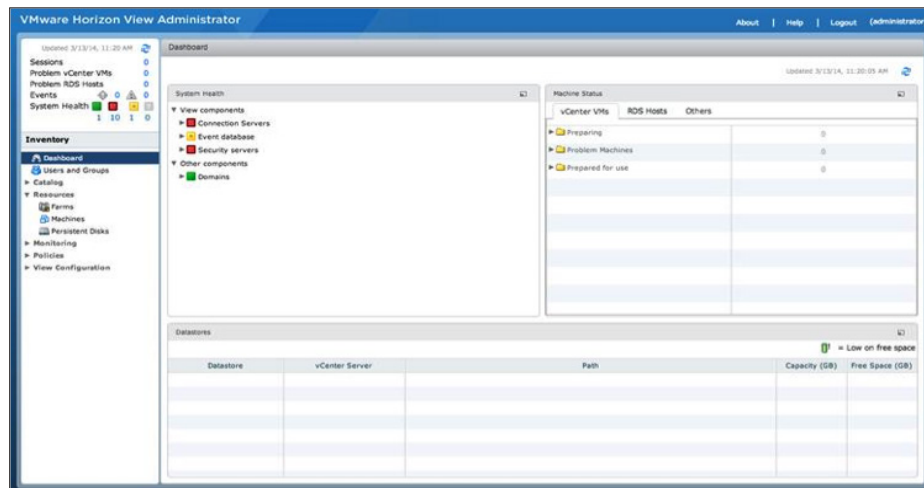
Customer Experience Program Section:

- Edit Settings (button)
- Send anonymous data to VMware: On
- Geographic Location: (button)
- Business Vertical: (button)
- Number of Employees: (button)

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

1. On the View Administrator Dashboard, select **View Configuration > Servers**.



The screenshot shows the 'VMware Horizon View Administrator' interface. The left sidebar contains a navigation tree with 'View Configuration' expanded and 'Servers' selected. The main pane is titled 'Dashboard'.

System Health Section:

- View components:
 - Connection Servers
 - Event database
 - Security servers
 - Other components
 - Domains

Machine Status Section:

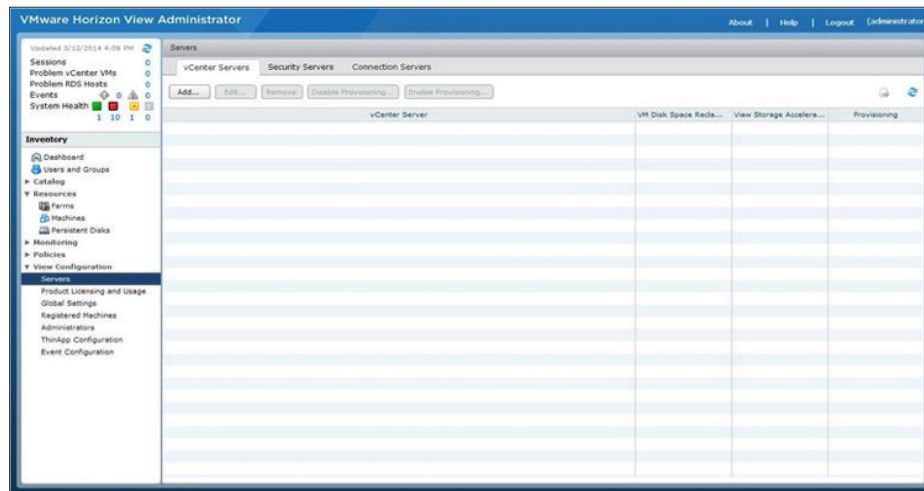
Machine Status	vCenter VMs	RDS Hosts	Others
Preparing	0	0	0
Problem Machines	0	0	0
Prepared for use	0	0	0

Databases Section:

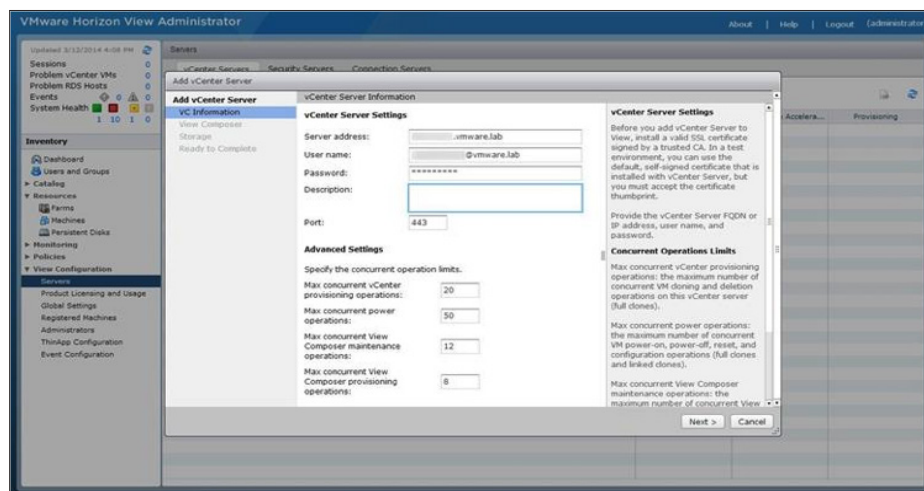
Database	vCenter Server	Path	Capacity (GB)	Free Space (GB)

Legend: Low on free space (icon)

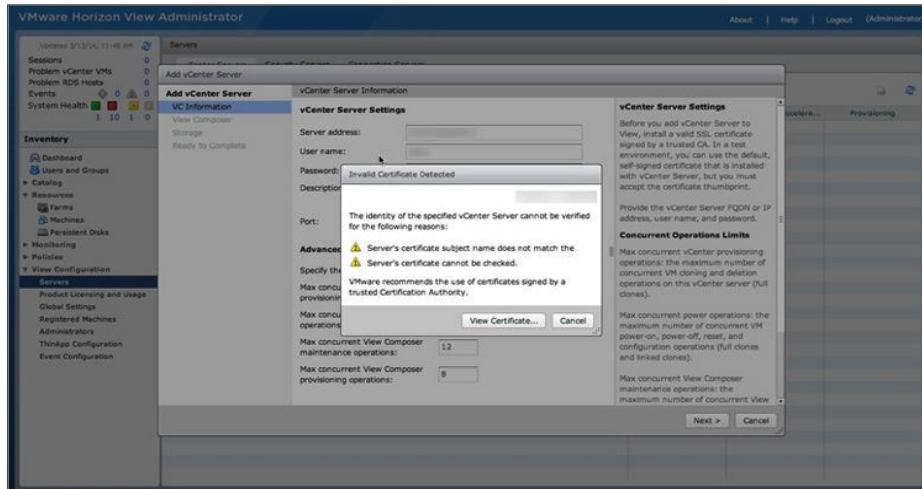
- In the **Servers** window, on the vCenter Servers tab, click **Add**.



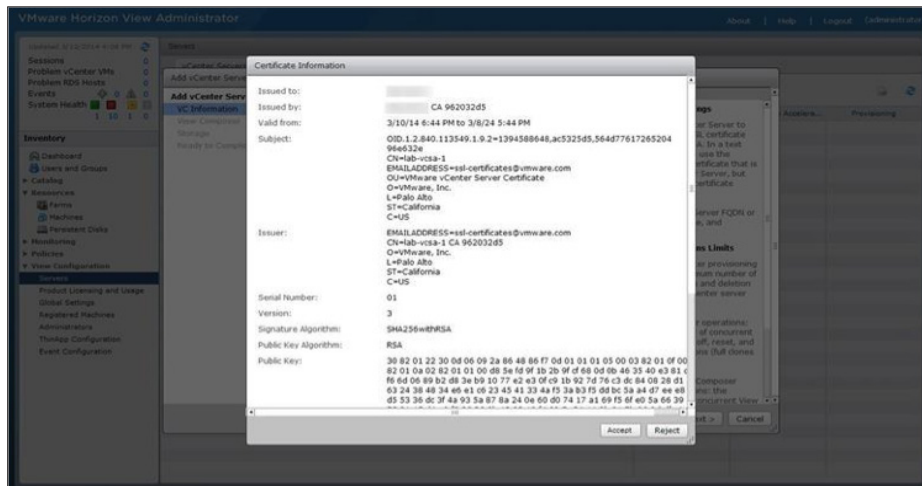
- In the Server address text box, type the fully qualified domain name or IP address of your vCenter Server. Accept or modify the default values for the other settings, and then click **Next**.



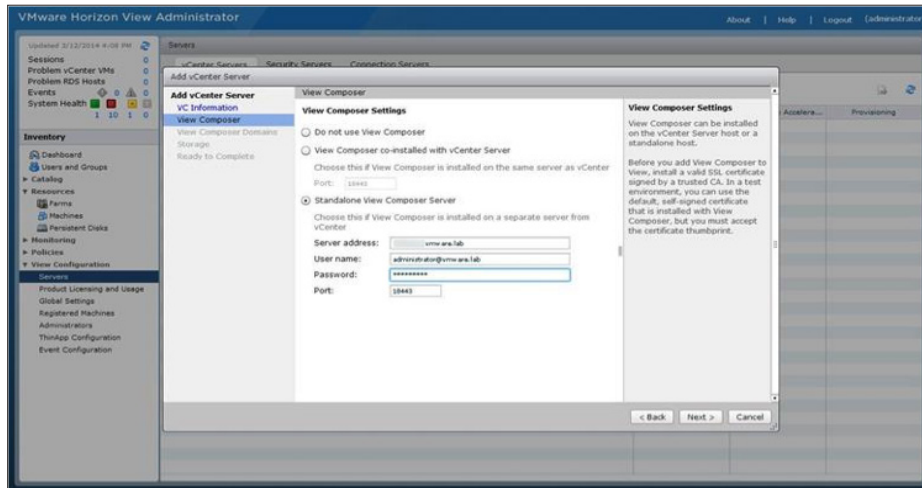
- In the Invalid Certificate Detected dialog box, click **View Certificate** to see the vCenter Server SSL certificate. In an evaluation environment, you can use a default self-signed certificate, but for a production environment, it is recommended that you replace the self-signed certificate with an approved certificate from a Certificate Authority.



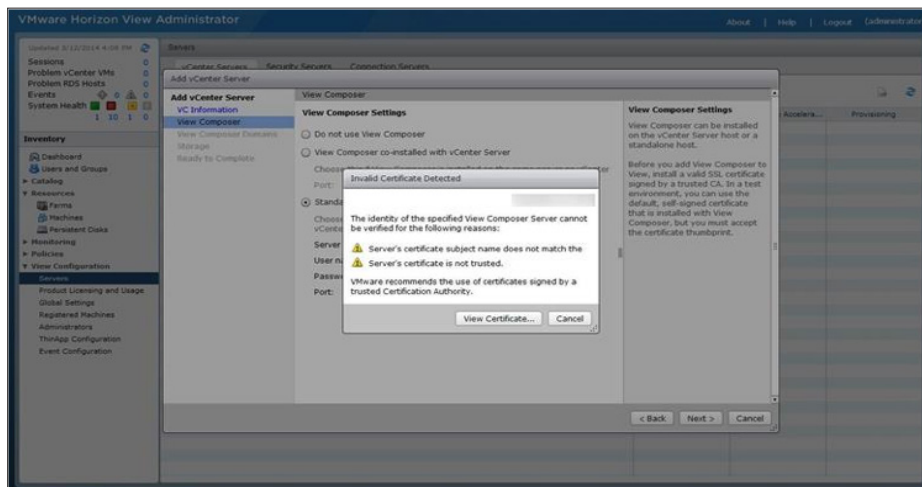
- Verify the self-signed certificate generated by the default installation of the vCenter Server Appliance, and click **Accept** to approve.



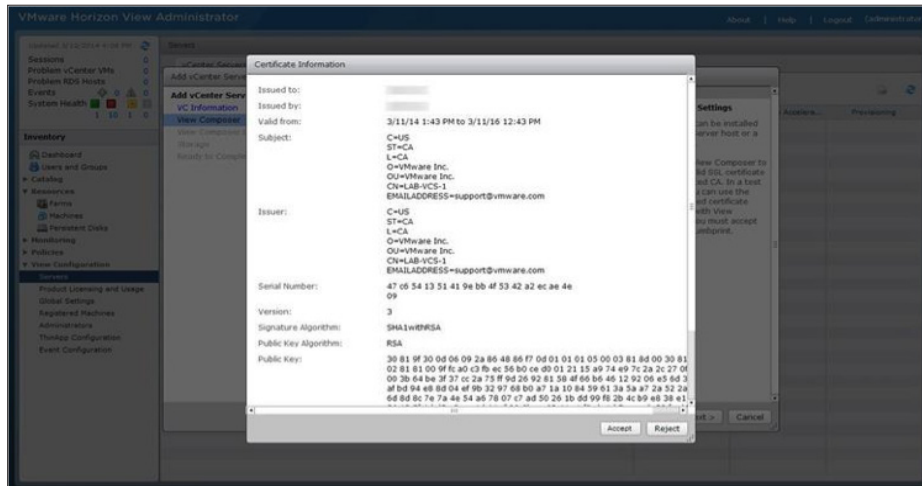
6. Configure the View Composer Server settings, and then click **Next**.
 - a. Select **Standalone View Composer Server** and type the required server address, either the FQDN or IP address of your View Composer Server virtual machine.
 - b. Enter the user name and password of the server.
 - c. Modify the port value only if you modified it during the View Composer Server installation. Otherwise, use the default.



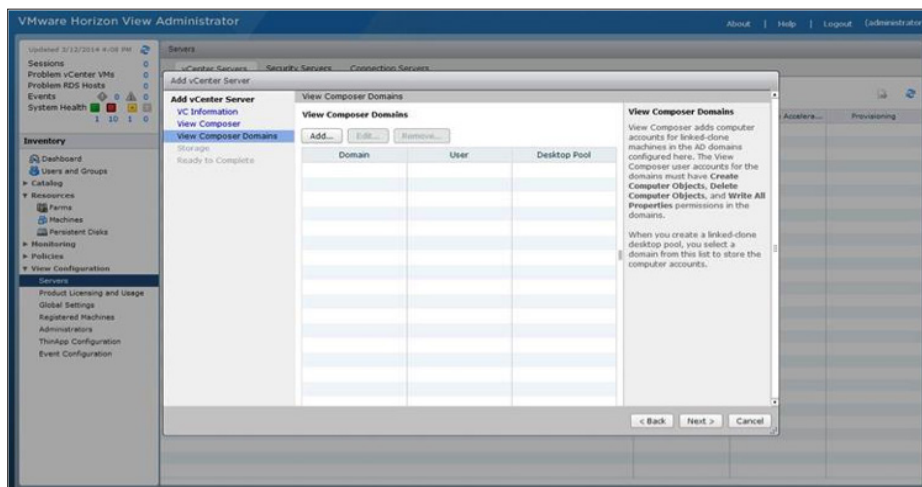
7. In the Invalid Certificate Detected dialog box, click **View Certificate** to see the View Composer SSL certificate. In an evaluation environment, you can use a default self-signed certificate, but for a production environment, it is recommended that you replace the self-signed certificate with an approved certificate from a Certificate Authority.



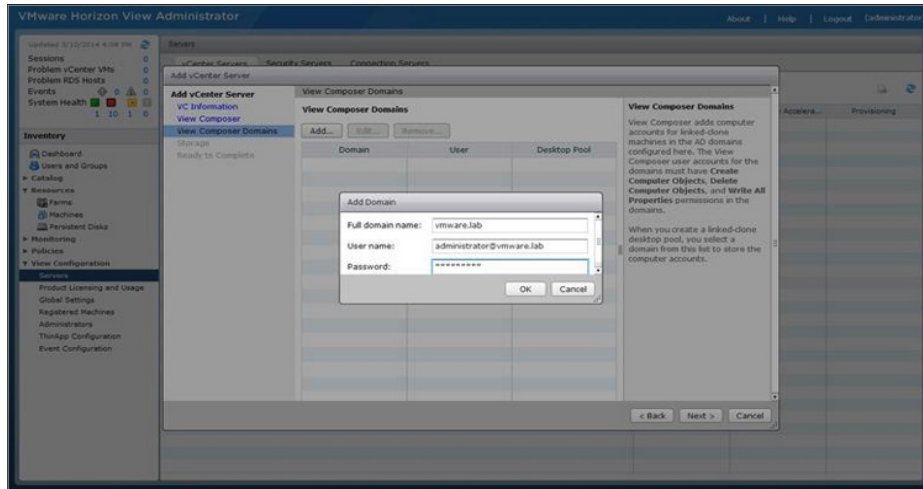
8. Verify the self-signed certificate generated by the default installation of the View Composer Server, and click **Accept** to approve.



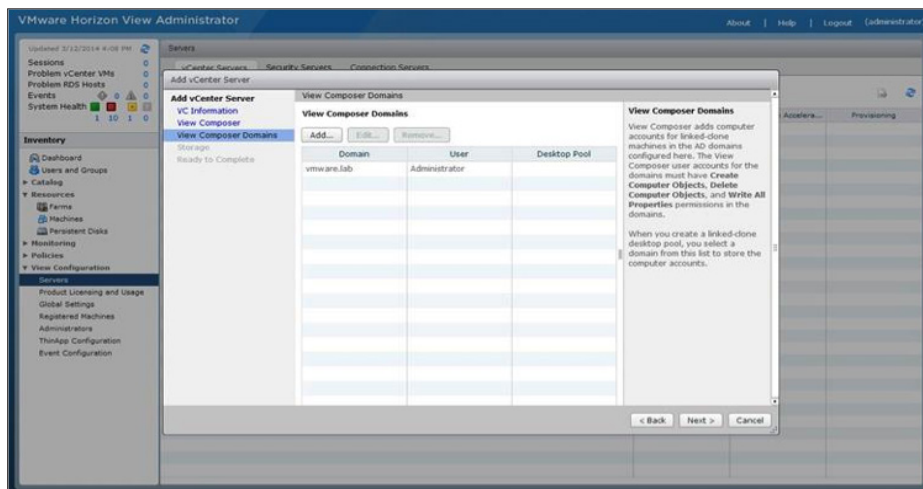
9. To add a View Composer domain, click **Add**.



10. In the Add Domain dialog box, enter the full domain name, user name, and password, and then 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.



11. Review the information and then click **Next**.



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

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

Add vCenter Server

VC Information
View Composer
View Composer Domains
Storage
Ready to Complete

Storage

Storage Settings

☒ Reclaim VM disk space

☒ Enable View Storage Accelerator

Default host cache size: 1024 MB

Cache must be between 100 MB and 2048 MB

Hosts

☐ Show all hosts

Edit cache size...

Host	Cache Size
demolab.	Default

Storage Settings

ESXi hosts can be configured to cache virtual machine disk data, which improves performance during I/O storms such as when many desktops power on and run anti-virus scans at once. Hosts read common data blocks from cache instead of reading the OS from disk.

By reducing IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array and uses less storage I/O bandwidth.

< Back Next > Cancel

13. Review the vCenter Server information, and then click **Finish** to accept these values and add the vCenter Server to your View environment. To modify any settings, click **Back**.

VMware Horizon View Administrator

Updated: 3/12/2014 4:09 PM

Sessions
Problem vCenter VMs
Problem RDS Hosts
Events
System Health

Inventory

Dashboard
Users and Groups
Catalog
Resources
Farms
Machines
Persistent Disks
Hosts
Policies
View Configuration
Servers
Product Licensing and Usage
Global Settings
Registered Machines
Administrators
ThinApp Configuration
Event Configuration

Servers

vCenter Services... Security Services... Connection Services...

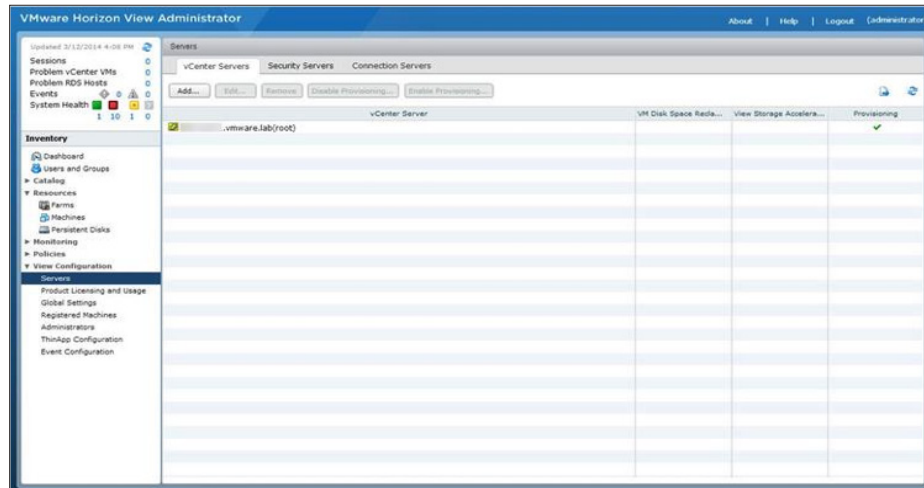
Add vCenter Server

Ready to Complete

Property	Value
vCenter Server	vmware.lab
User name	administrator@vmware.lab
Password	*****
Description	
Server Port	443
Max Provision	20
Max Power	50
Max View Composer Operations	12
Max View Composer Provision	8
View Composer State	Standalone View Composer Server
View Composer Address	vmware.lab
View Composer Password	*****
View Composer User Name	administrator@vmware.lab
View Composer Port	18443
Enable View Storage Accelerator	No
VM Disk Space Reclamation	No

< Back Finish Cancel

14. In the vCenter Servers tab, you can view the vCenter Server added to your View environment. To make changes to the connection information or settings, 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

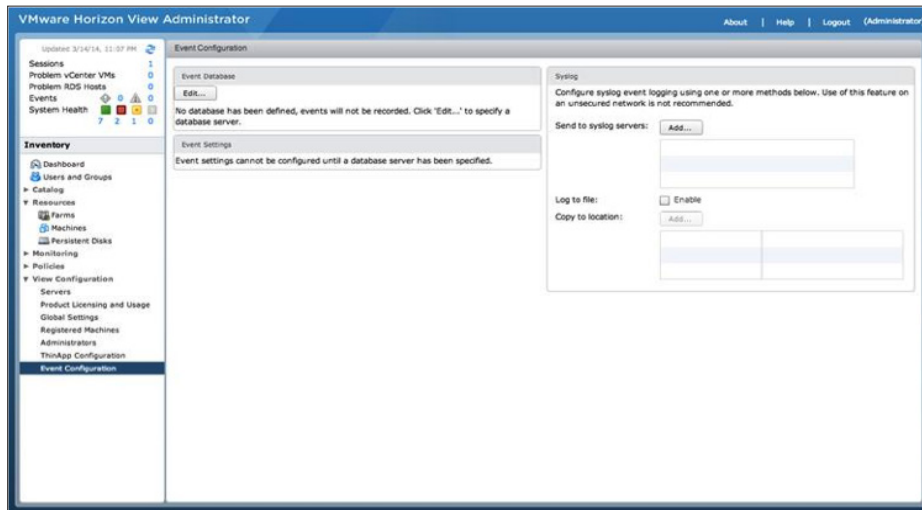
You can choose to skip this exercise and return to it after completing the rest of the exercises in this document.

It is recommended that you adjust the PCoIP settings to ensure the best user experience. For instructions on tuning PCoIP, see the [VMware View 5 with PCoIP Network Optimization Guide](#).

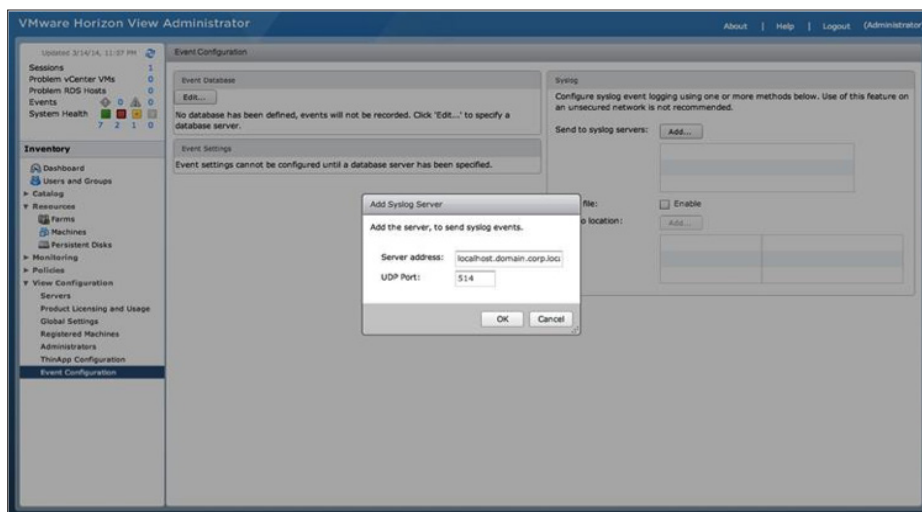
Configure Syslog Event Logging

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

1. In the View Administrator console, click **View Configuration > Event Configuration**, and then under Syslog on the right, click **Add**.



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

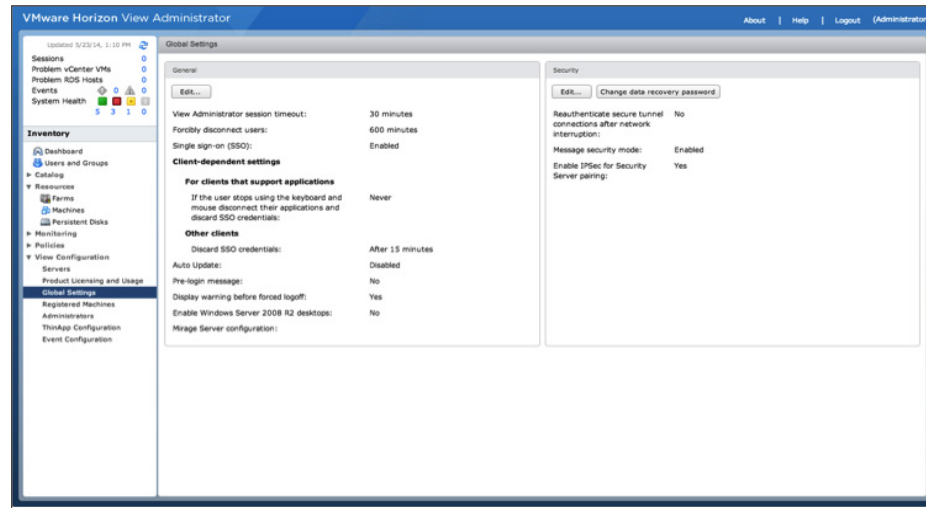


You have now set up Syslog collection for View events.

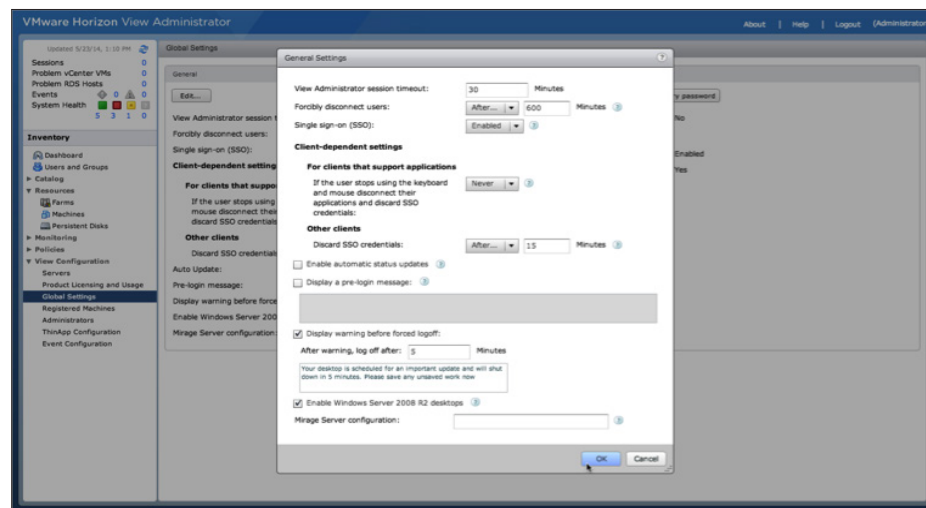
Enable Windows Server 2008 R2 SP1

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

1. In the View Administrator console, click **Global Settings** and in the General pane, click **Edit**.



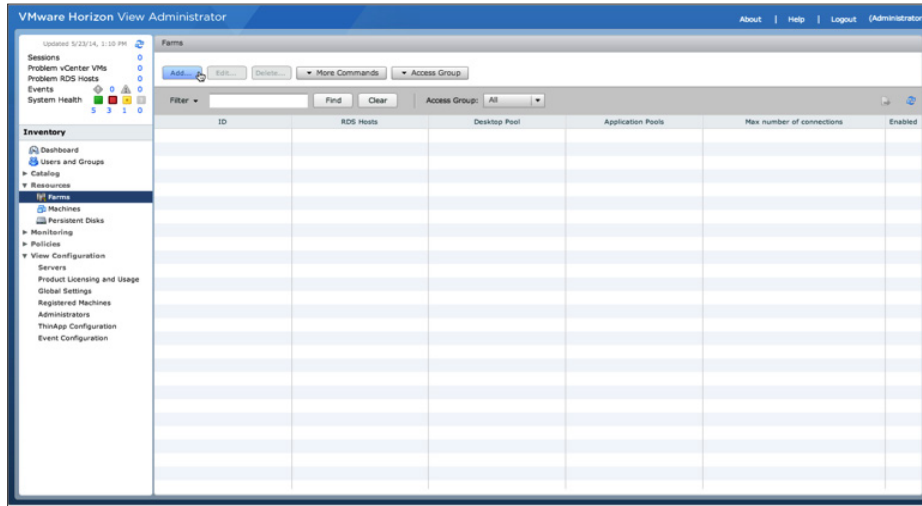
2. Select the check box **Enable Windows 2008 R2 desktops** and then click **OK**.



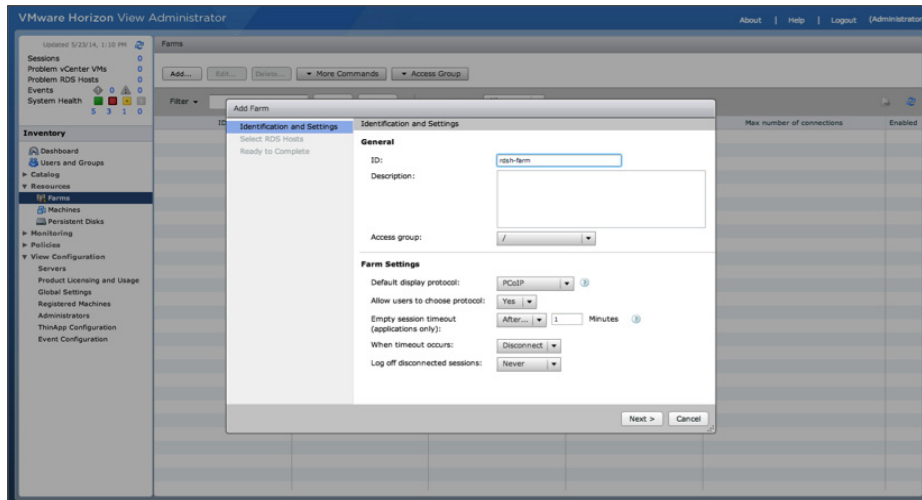
You have enabled Windows Server 2008 R2 SP1 View Desktop support. You are now ready to create a farm for Remote Desktop Session hosts.

Create a Farm for Remote Desktop Session Hosts

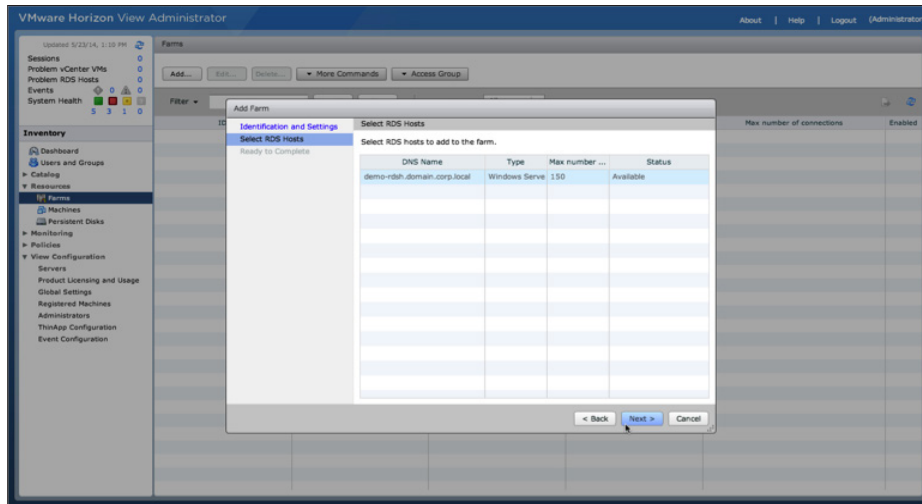
1. In the View Administrator console, select **Resources > Farms**.
2. Click **Add** to start the Add Farm wizard.



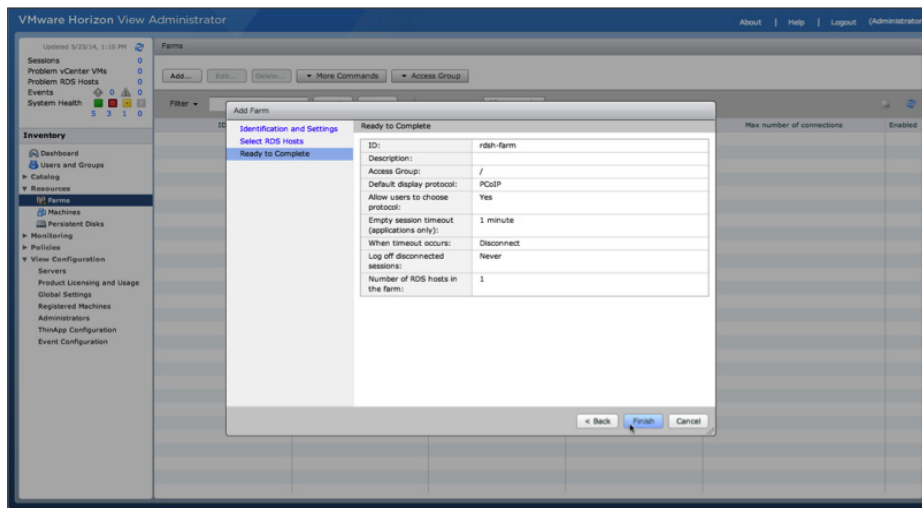
3. In the Add Farm wizard, enter a name for your farm in the **ID** text box.
4. For the other options, use the defaults settings or make changes, and then click **Next**.



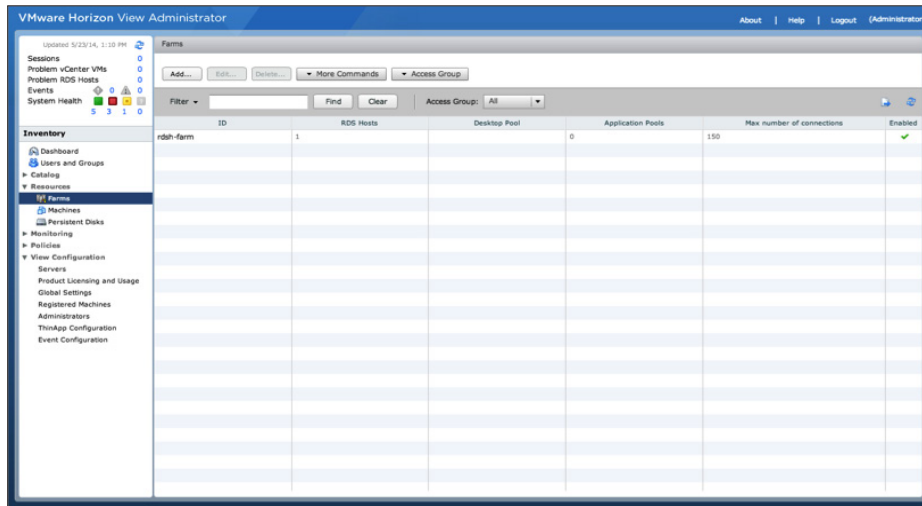
5. Select which RDS hosts to add to your farm, and click **Next**.



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



7. You are brought back to the Farms window, which now lists the new RDS host farm.



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

Preparing Desktop Images for Linked-Clone Desktop Pool Deployment

In this and the next series of exercises, you prepare two types of desktop images to use to deploy remote desktops. One desktop image is for linked-clone deployment, and the other is for full-clone deployment.

This section describes how to deploy Windows 7 32-bit View desktops configured in a stateless linked-clone pool. You install the required agents and optimize the desktop image for linked-clone deployment in the following exercises:

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

You can use virtual machines managed by vCenter Server to provision and deploy desktops as templates for automated full-clone pools, as parents for linked-clone pools, or as a desktop source in a manual pool. You must prepare virtual machines to deliver View desktop access.

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

Create the Parent Virtual Machine for Desktop Deployment

You start by creating a parent virtual machine for desktop deployment. A parent virtual machine is also referred to as a *golden image* or *master image*.

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

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

Table 10: Parent Virtual Machine Specifications for Nonproduction Deployment

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.

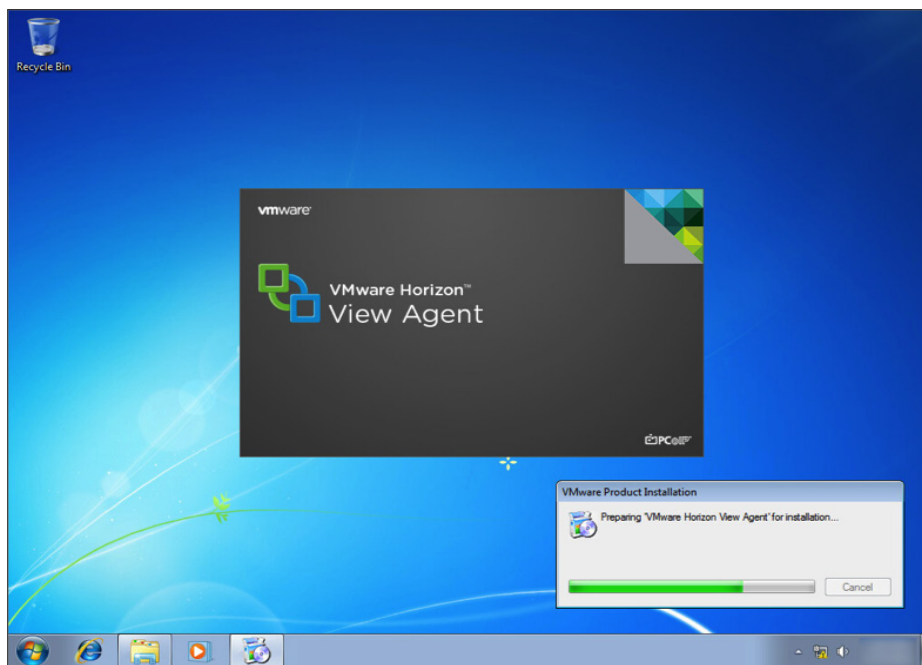
2. Install the Windows 7 32-bit guest operating system.
3. Activate your Windows operating system according to your organization's procedures.
4. After the installation is complete, log in to the virtual machine as a local administrator.

Proceed to the next exercise to install View Agent.

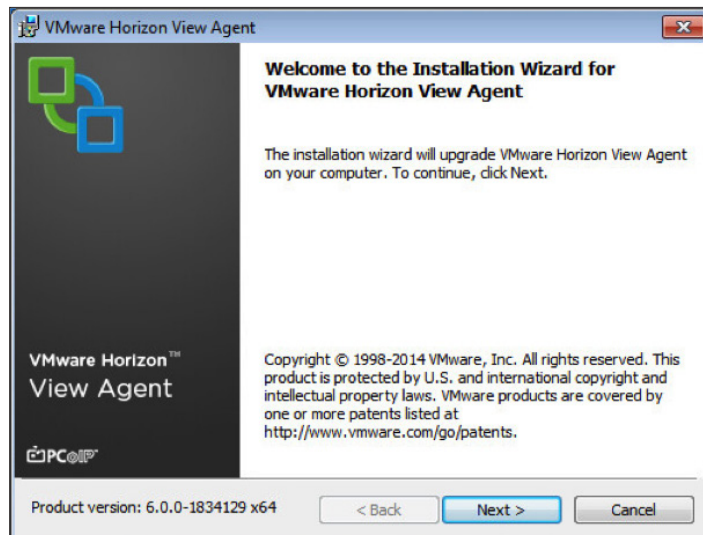
Install View Agent

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

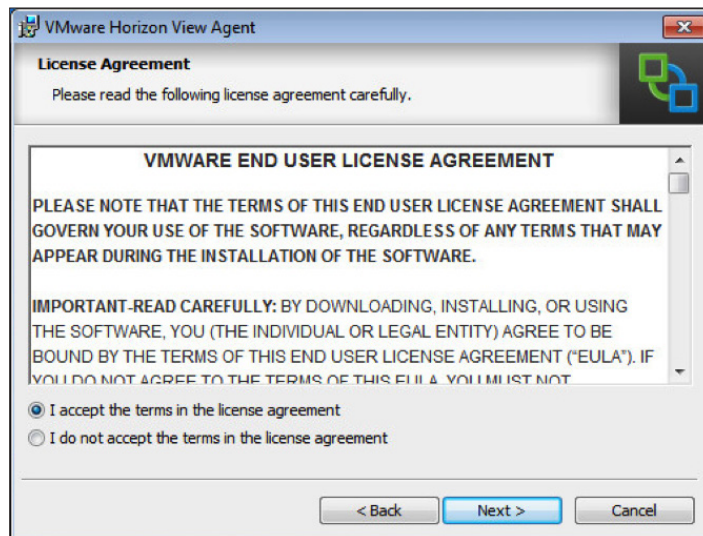
1. Launch the View Agent installer using the Run As Administrator option. Ensure that the installer is accessible from your virtual machine.



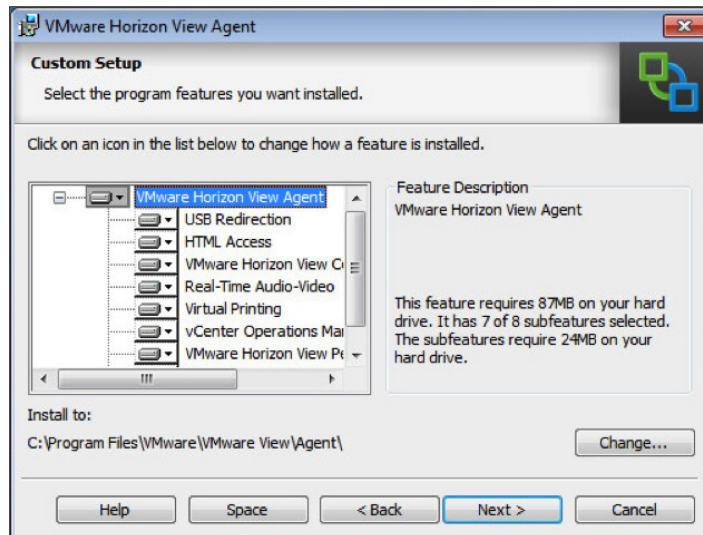
2. Wait for the installer to load, and then click **Next**.



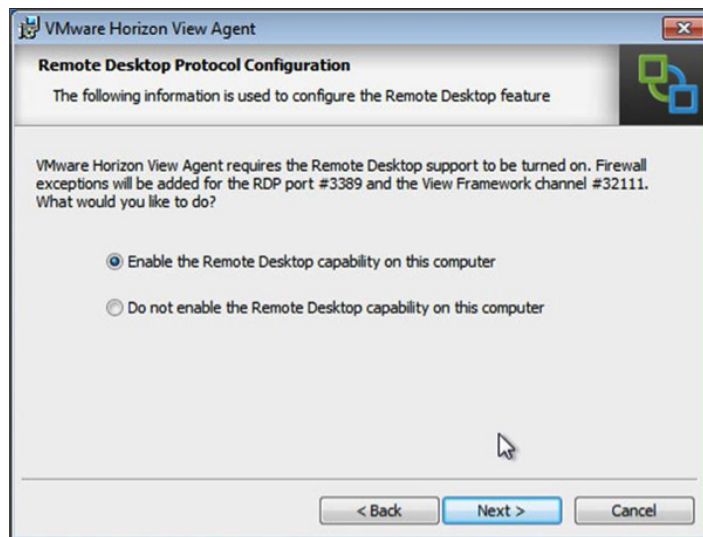
3. Review and accept the terms and conditions, and then click **Next**.



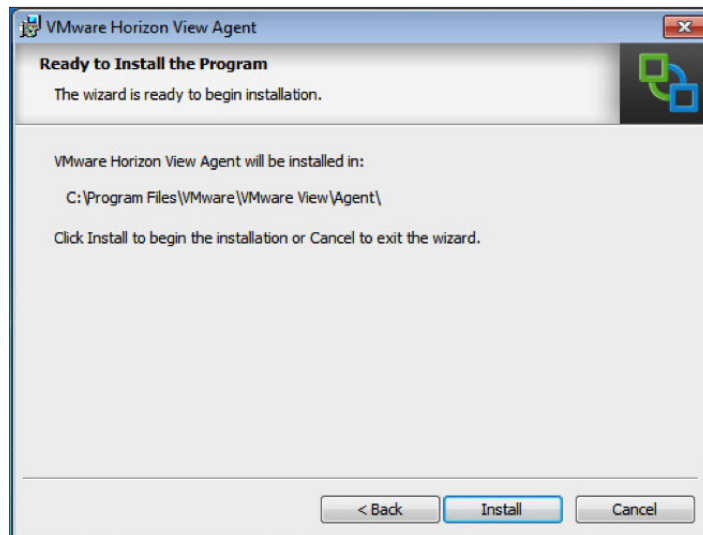
4. In the Custom Setup window, it is recommended that you enable all the features (the default) to take full advantage of View Agent and properly complete these exercises. Optionally, you can disable the features you do not want and change the default installation directory by clicking **Change**. Click **Next**.



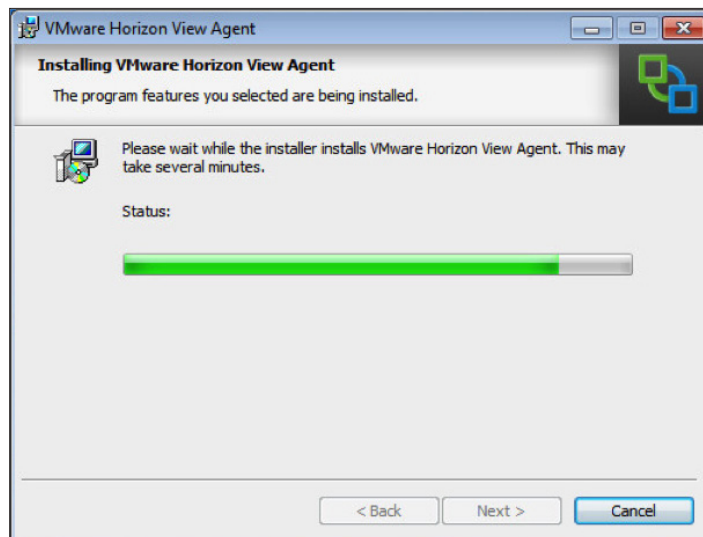
5. Select **Enable the Remote Desktop capability on this computer**. If you select **Do not enable...** you can also manually enable this feature later and configure the firewall exceptions. Click **Next**.



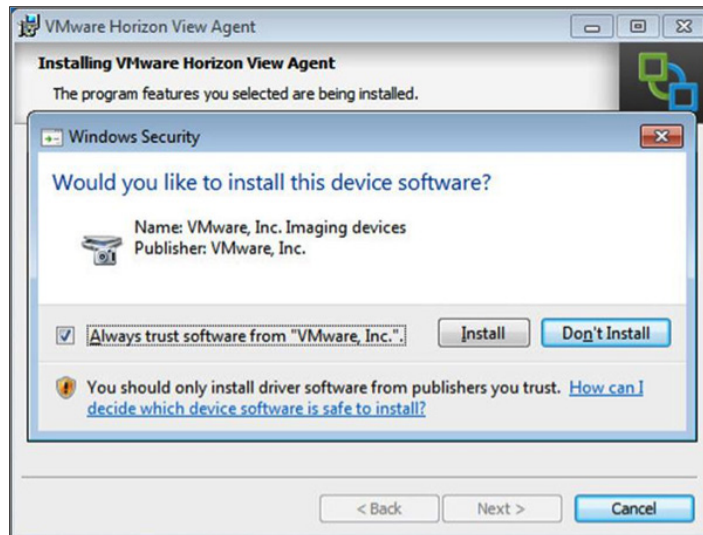
6. To install View Agent, click **Install**. To make changes, click **Back**.



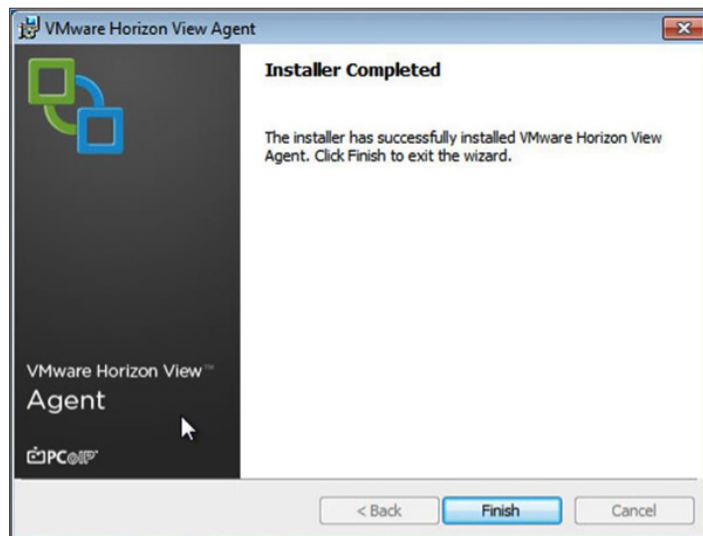
7. Monitor the installation status as it progresses.



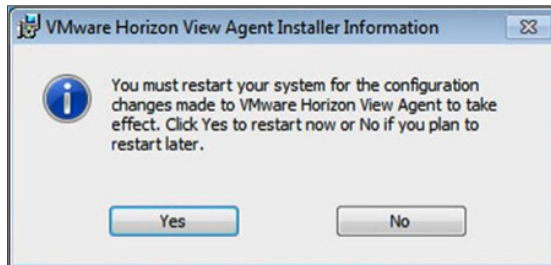
8. You might be prompted by Windows Security to allow installation of a device driver. These drivers are necessary to enable certain devices to work correctly with your View desktop. Select **Always trust software from "VMware, Inc."** and then click **Install**.



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



10. You must restart the operating system to complete the installation. In the VMware View Agent Installer Information dialog box, click **Yes**.



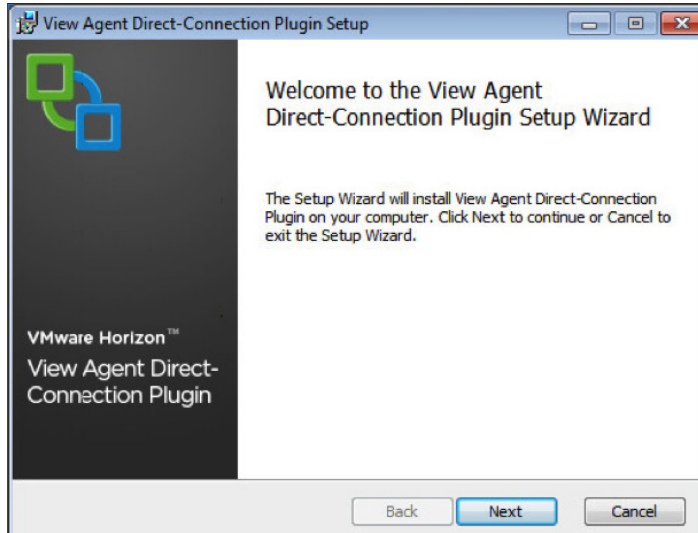
You have now installed View Agent and enabled Persona Management on desktop image virtual machines. Proceed to the next exercise to install the VMware View Agent Direct-Connection Plug-in.

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

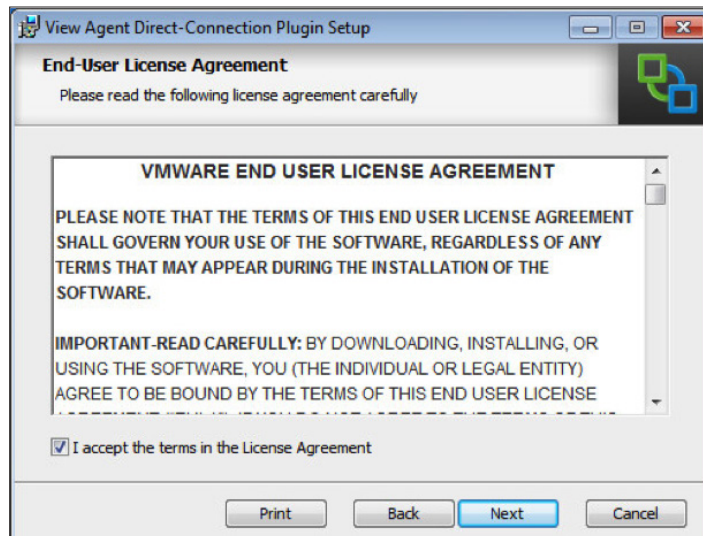
The View Agent Direct-Connection Plug-in enables any Horizon Client to connect directly to a View desktop without using View Connection Server.

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.

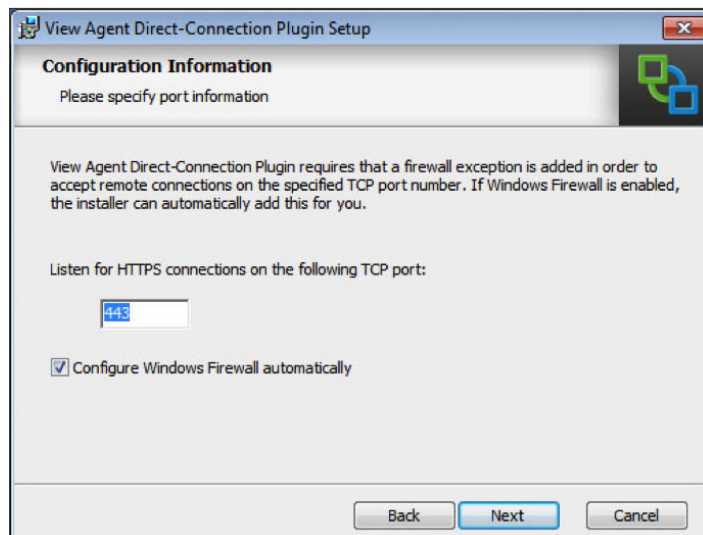
1. Launch the View Agent Direct-Connection Plug-in installer using the Run As Administrator option. Ensure that the installer is accessible from your virtual machine. When the launcher loads, click **Next**.



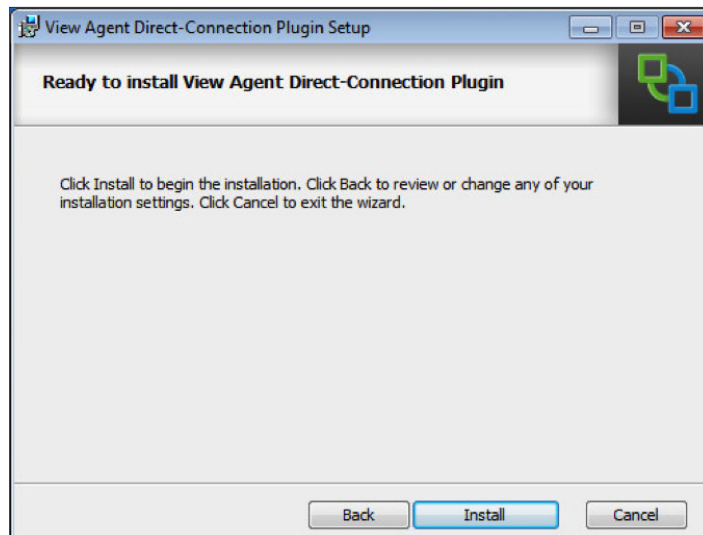
2. Review and accept the terms and conditions, and then click **Next**.



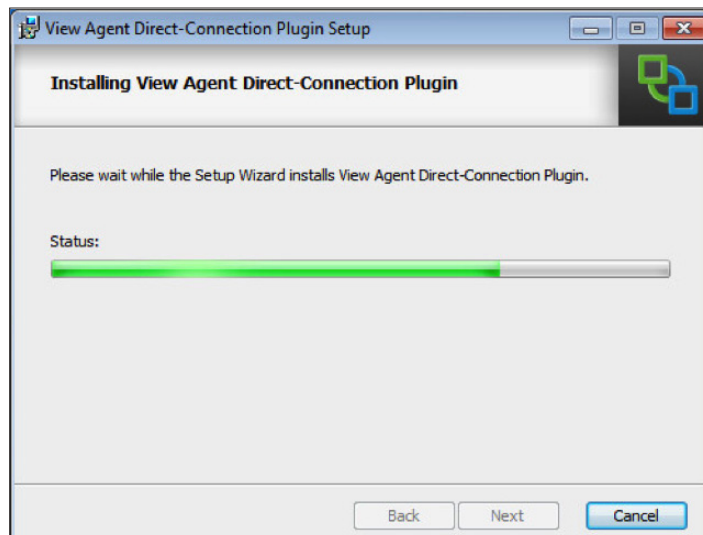
3. Confirm the default port required for HTTPS connections, select the **Configure the Windows Firewall automatically** option, and then click **Next**.



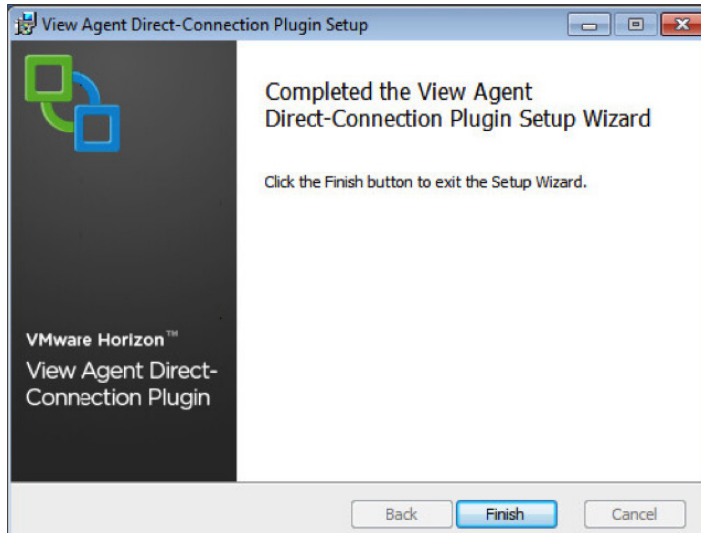
4. In the Ready to Install dialog box, click **Install** to proceed. If you want to make changes, click **Back**.



5. 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 proceed to the next exercise to optimize the parent virtual machine for desktop deployment.

Optimize the Parent Virtual Machine for Desktop Deployment

We recommend that you optimize Windows for View desktop deployment as described in *Windows 7 and Windows 8 OS Customizations* in the [Windows 7 Optimization Guide](#).

The guide includes the helper script, `CommandsPersonaManagementWin7_01062014.txt`, which you can use to apply all the recommended optimizations. Run the script on your parent virtual machine. This script optimizes the parent virtual machine to work with Persona Management.

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

Install Custom Applications and Configure the Parent Virtual Machine Operating System (Optional)

This exercise is optional but recommended. You can always come back to your parent virtual machine to install additional applications or modifications and then use the parent virtual machine to update the existing desktop pools or deploy new ones.

- Install the custom applications that you want preinstalled on your parent virtual machine for View desktop deployment.
- Make any modifications to the Windows operating system.
- 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 parent virtual machine for linked-clone deployment.

Prepare the Parent Virtual Machine for Linked-Clone Deployment

To prepare the parent virtual machine for linked-clone deployment:

1. Join the parent virtual machine to the domain.
2. Ensure that the parent 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 parent virtual machine.
5. Take a snapshot of the virtual machine from the vSphere Client. Give the snapshot a meaningful name and description so that you have a reference 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 parent virtual machine for linked-clone desktop deployment. Proceed to the next series of exercises to prepare a desktop image for full-clone desktop pool deployment.

Preparing a Desktop Image for Full-Clone Desktop Pool Deployment

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

- [Create a Virtual Machine Template 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 Parent Virtual Machine Operating System \(Optional\)](#)
- [Prepare the Parent Virtual Machine for Full-Clone Deployment](#)

You can use virtual machines managed by vCenter Server to provision and deploy desktops as templates for automated full-clone pools, as parents for linked-clone pools, or as a desktop source in a manual pool. You must prepare virtual machines to deliver View desktop access.

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

Create a Virtual Machine Template for Desktop Deployment

Full-clone desktop pools are usually deployed based on a virtual machine template.

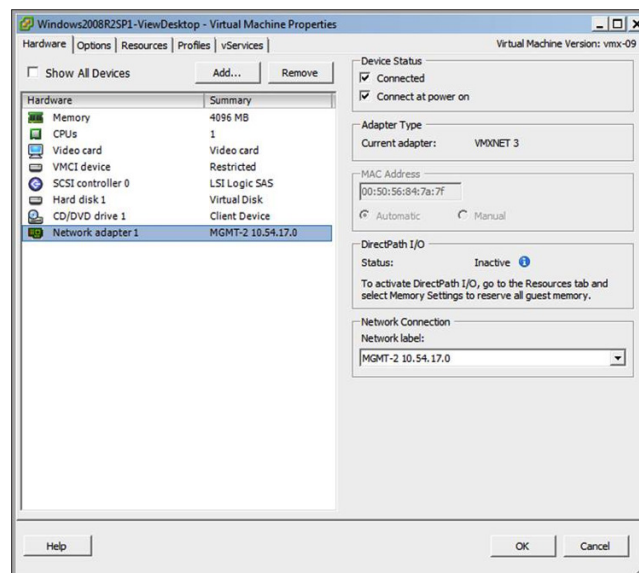
1. Log in to your host from the vSphere Client.
2. Create a new virtual machine using the following specifications as a guide.

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

Table 11: Virtual Machine Specifications for Nonproduction Deployment

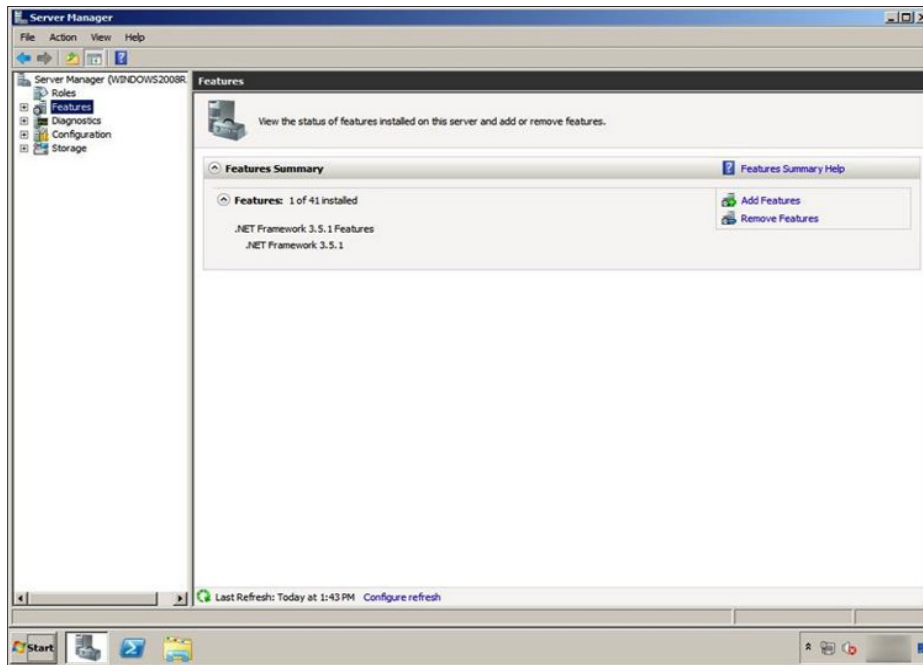
Note: These desktop specifications are recommended for evaluating a nonproduction deployment. For a production environment, where desktop sizing varies based on the types of user workloads, see the [View Architecture Planning guide](#) for best practices on resource planning.

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.

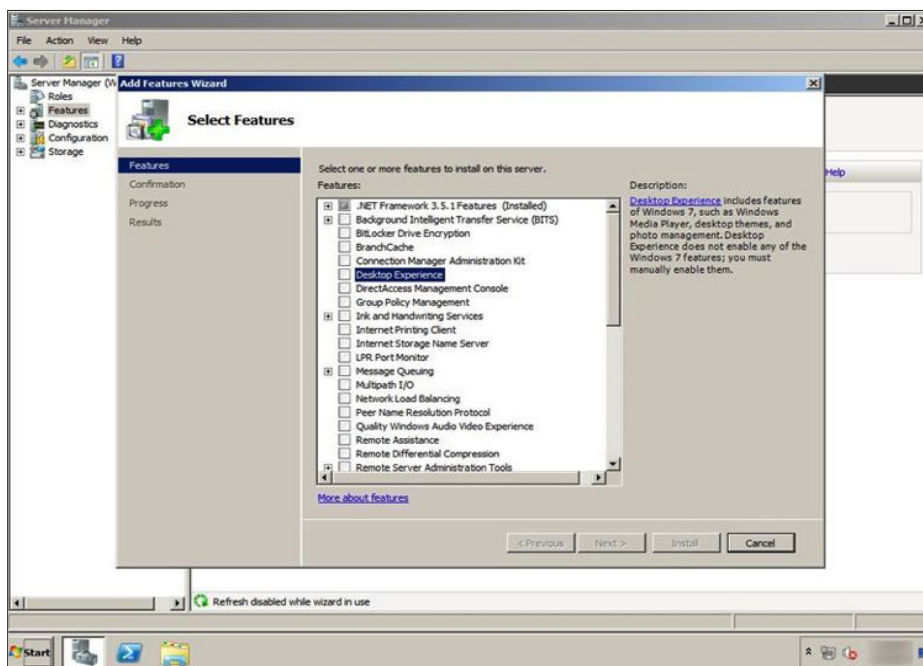


4. Install the Windows Server 2008 R2 with SP1 64-bit guest operating system, and ensure that Service Pack 1 has been applied to the OS if you used the base Windows Server 2008 R2 64-bit media. Activate your Windows operating system according to your organization's procedures.

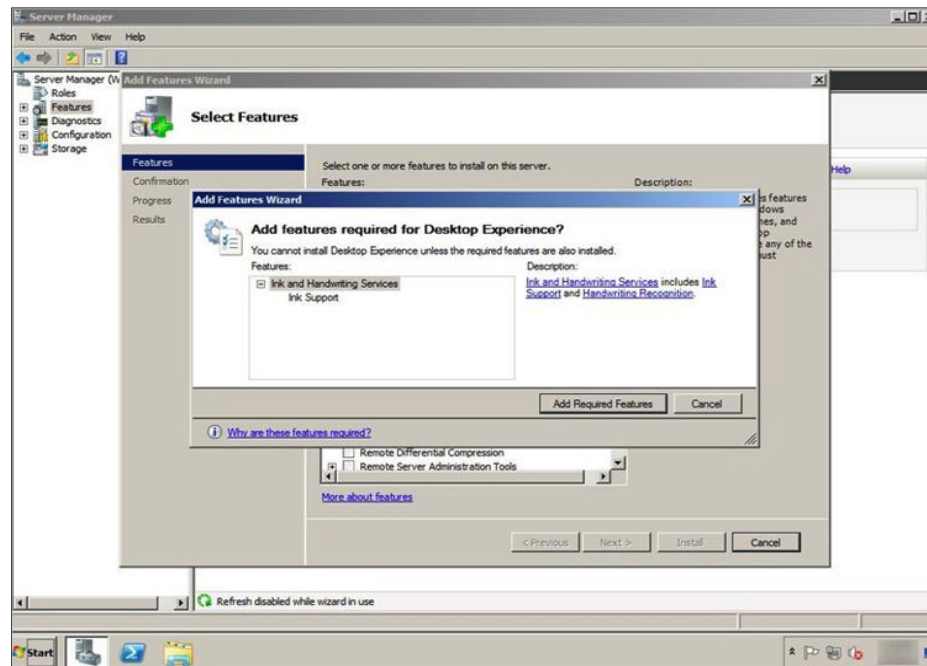
- Log in to the virtual machine as a local administrator and open the Server Manager utility to install the Desktop Experience feature, which is required for your image template to operate correctly with View.
- Click the **Features** menu, and then click **Add Features**.



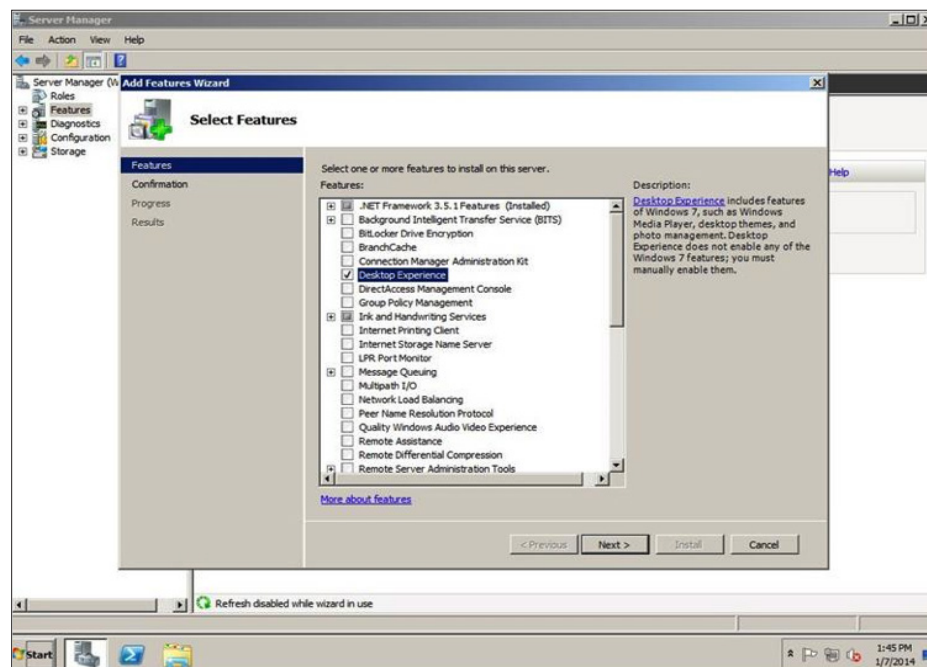
- In the Add Features Wizard window, select the **Desktop Experience** feature, and click **Next**.



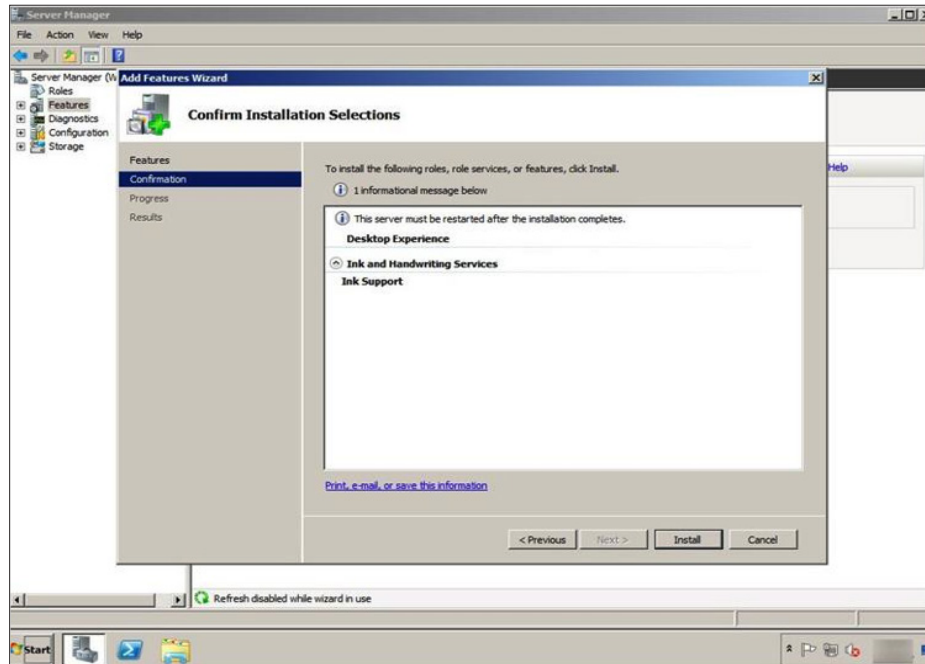
8. You might need to add feature prerequisites. Click **Add Required Features**.



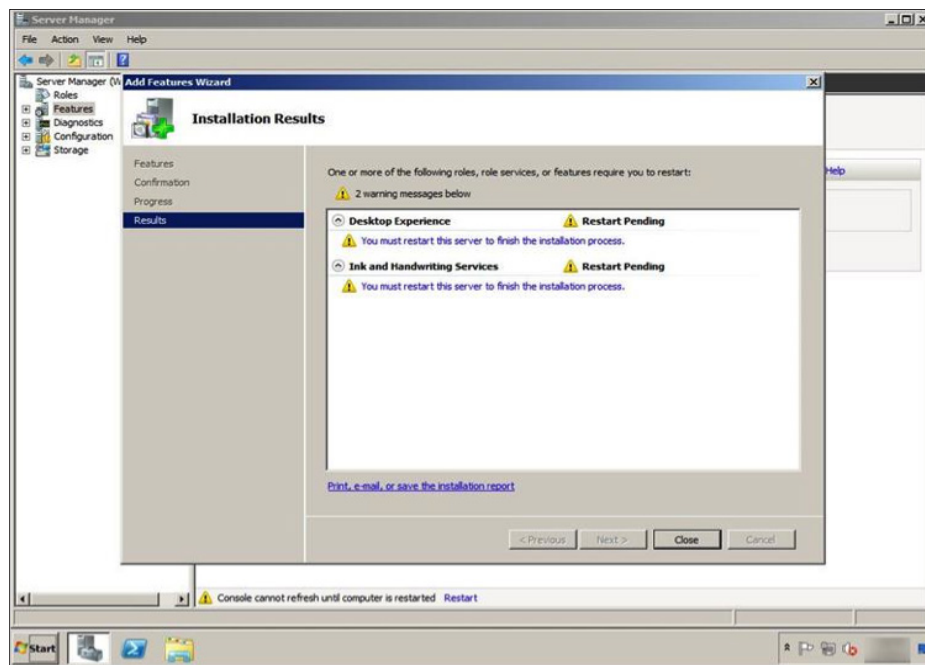
9. Confirm that Desktop Experience and the required prerequisites are selected, and click **Next**.



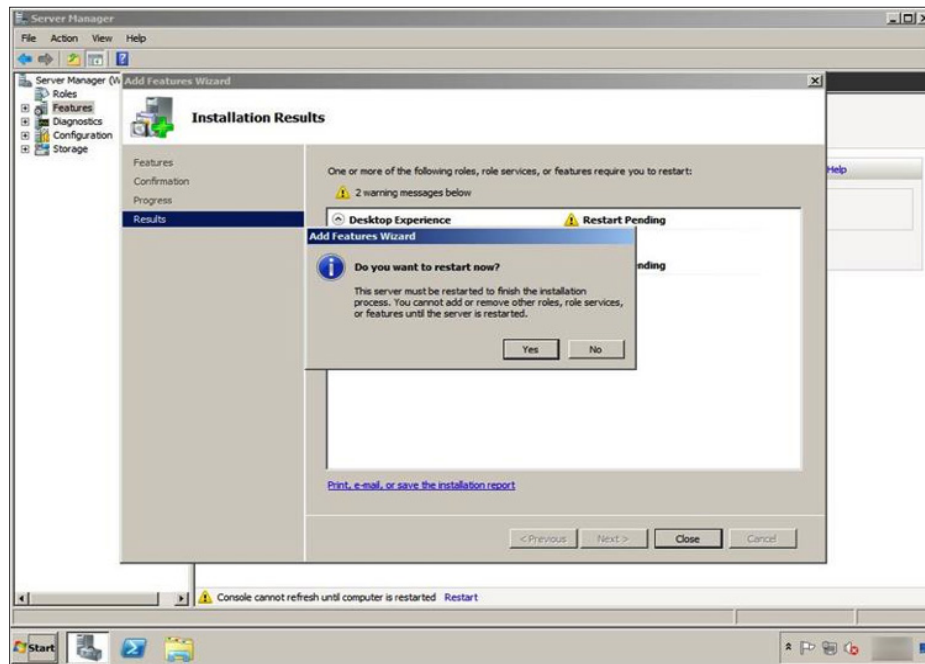
10. To all install the features, click **Install**.



11. A summary of the features and required actions appears. Click **Close** to continue.



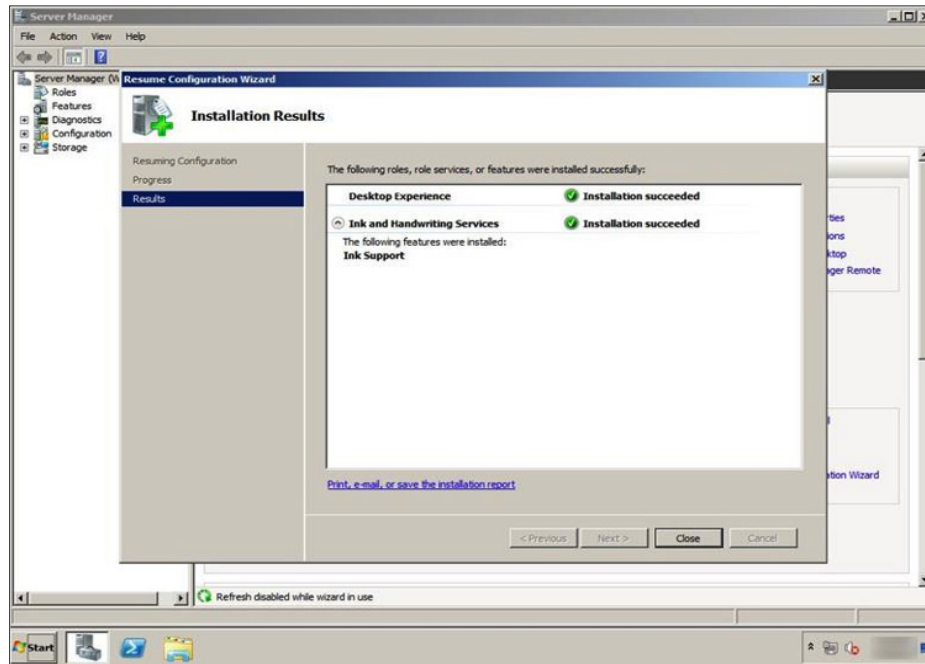
12. You are prompted to restart your computer. Click **Yes** to restart now and complete the installation.



13. Monitor the feature installation as it progresses.



14. When the installation is finished, log back in. A window verifying the installation of the Desktop Experience feature appears. Click **Close**.

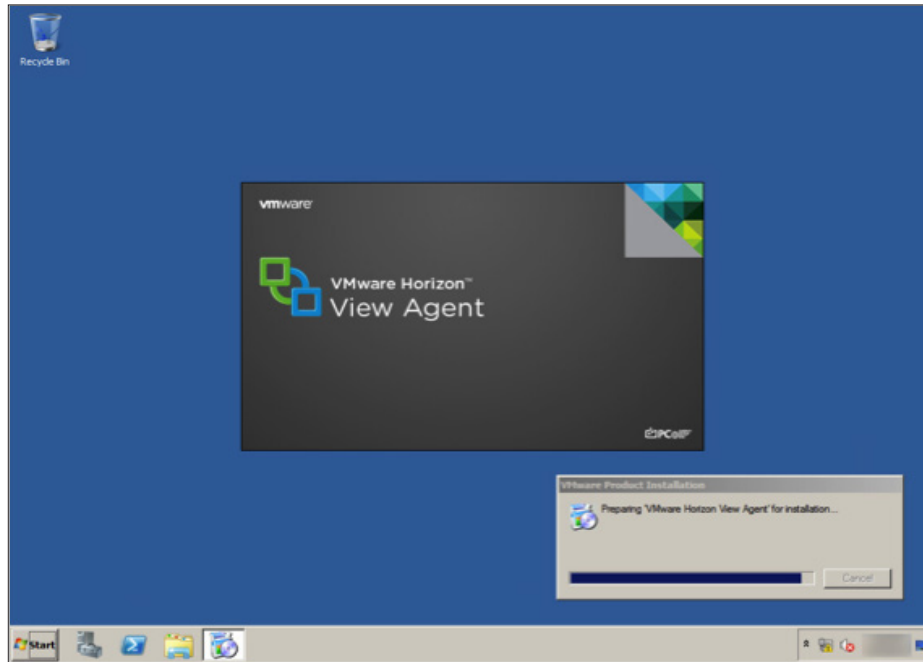


You have now finished all the operating system prerequisites for the Windows 2008 R2 SP1 View desktop template. Now you can install View Agent.

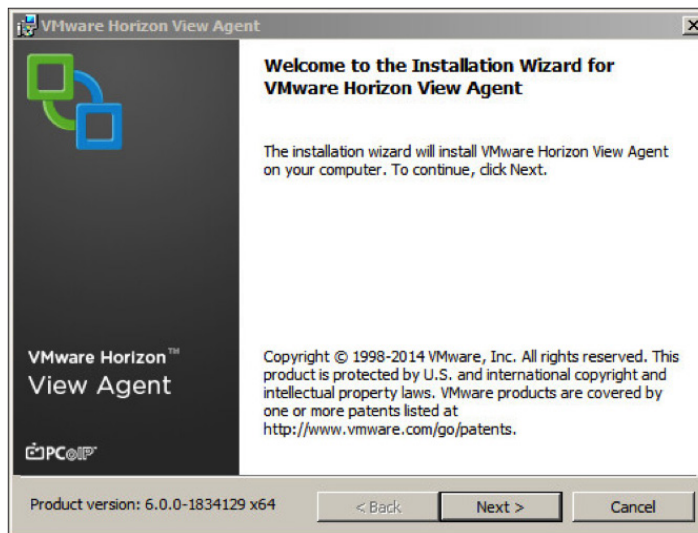
Install View Agent on the Desktop Image Virtual Machine

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

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



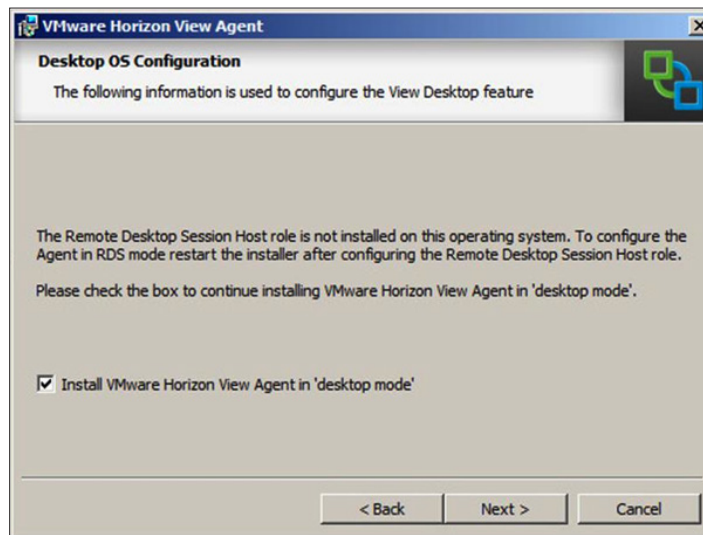
2. When the installer has loaded, click **Next**.



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



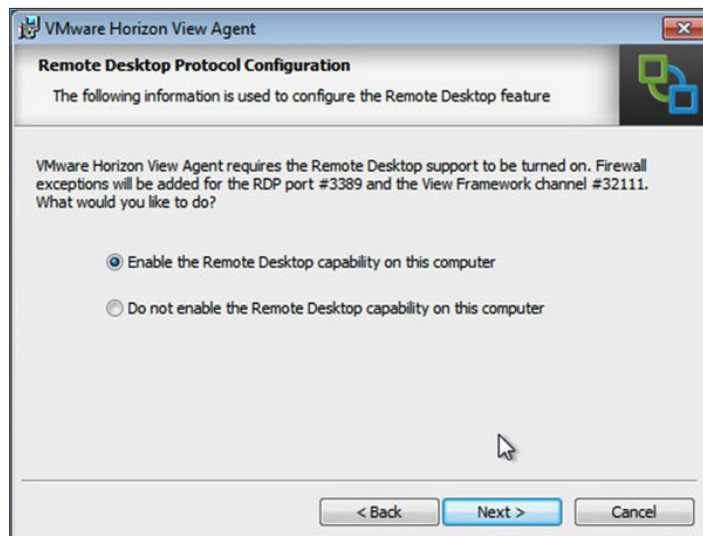
4. In the Desktop OS Configuration warning, select **Install VMware Horizon View Agent in 'desktop mode'** and then click **Next**.



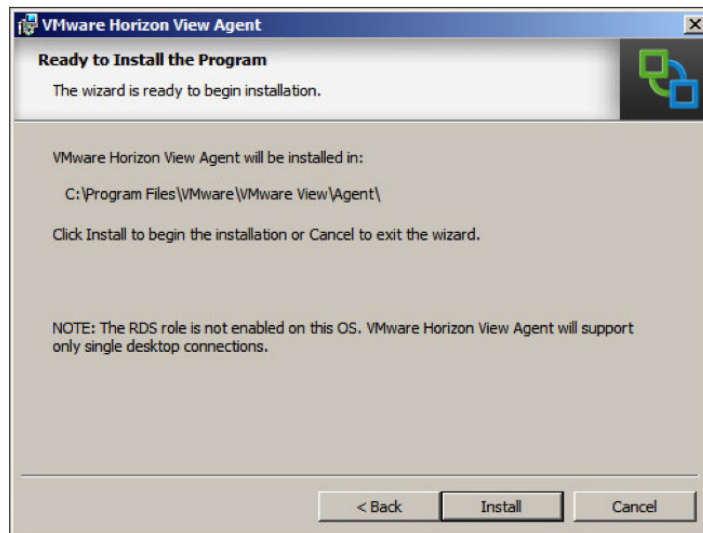
5. The available features that can be installed with View Agent are listed. It is recommended that you use the features selected to ensure that all View Agent features are available when you deploy your desktop pool. To change the default installation directory, click **Change**. When you are ready to proceed, click **Next**.



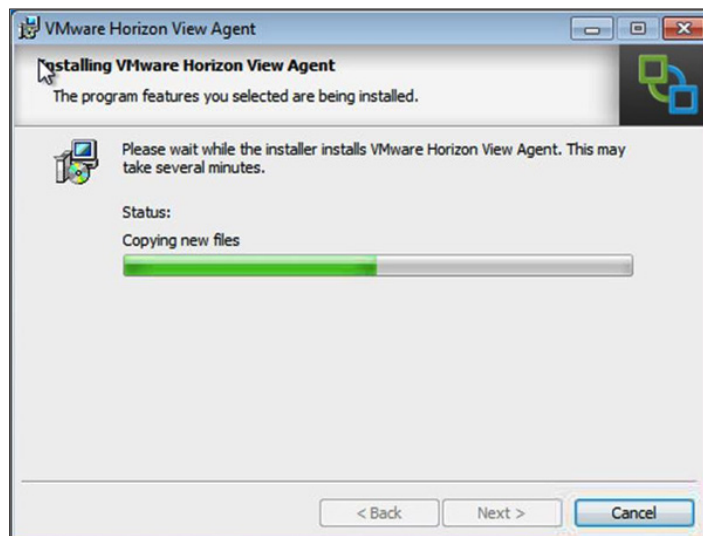
6. Select **Enable the Remote Desktop capability on this computer**. If you select **Do not enable...** you can also manually enable this feature later and configure the firewall exceptions. Click **Next**.



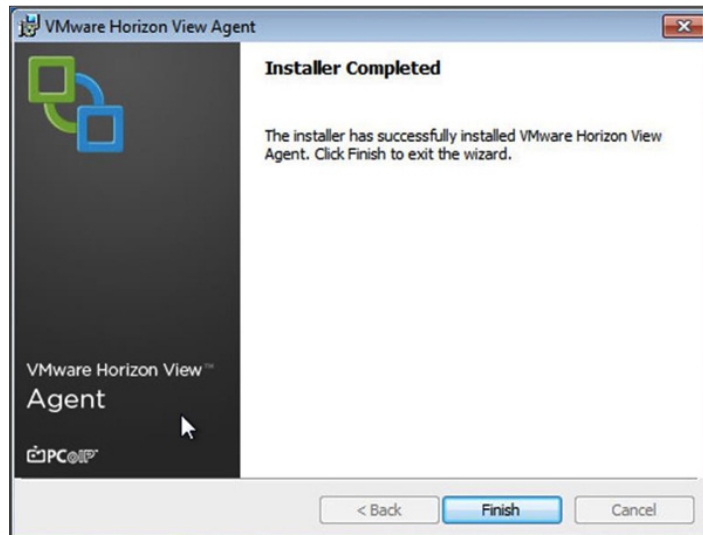
7. To install View Agent, click **Install**. To make changes, click **Back**.



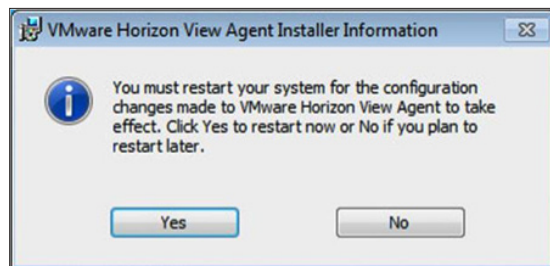
8. Monitor your installation status as it progresses.



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



10. You must restart the operating system to complete the installation. In the VMware View Agent Installer Information dialog box, click **Yes**.



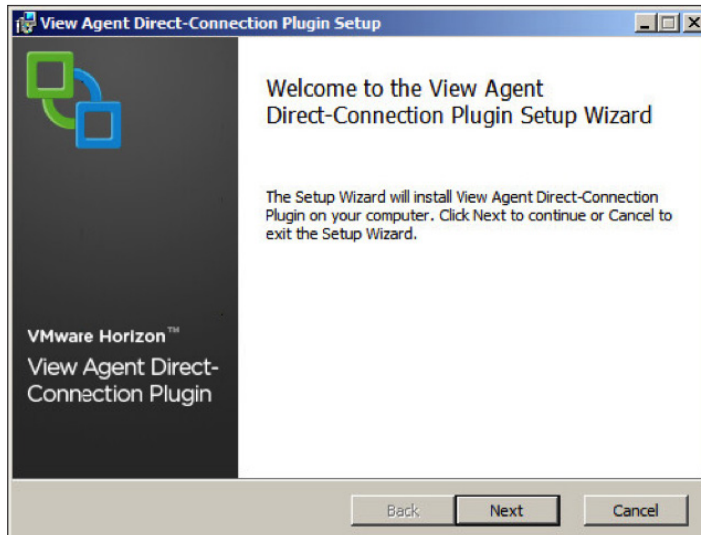
You have now installed View Agent. Proceed to the next exercise to install the VMware View Agent Direct-Connection Plug-in.

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

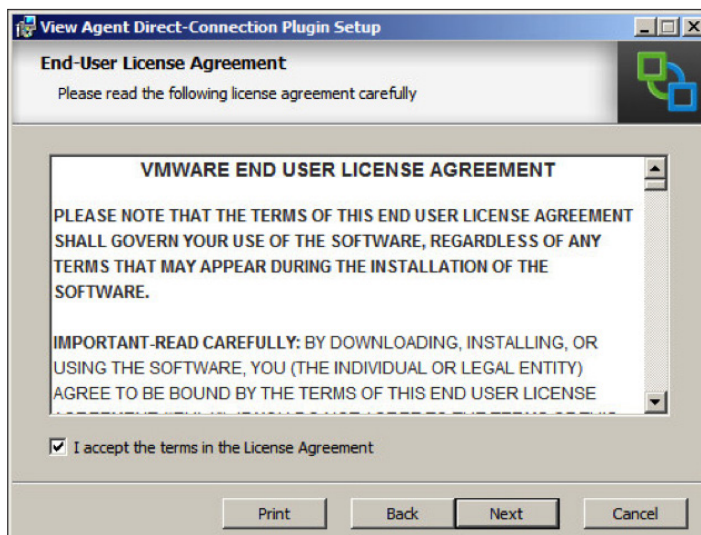
The View Agent Direct-Connection Plug-in enables any Horizon Client to connect directly to a View desktop without using View Connection Server.

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.

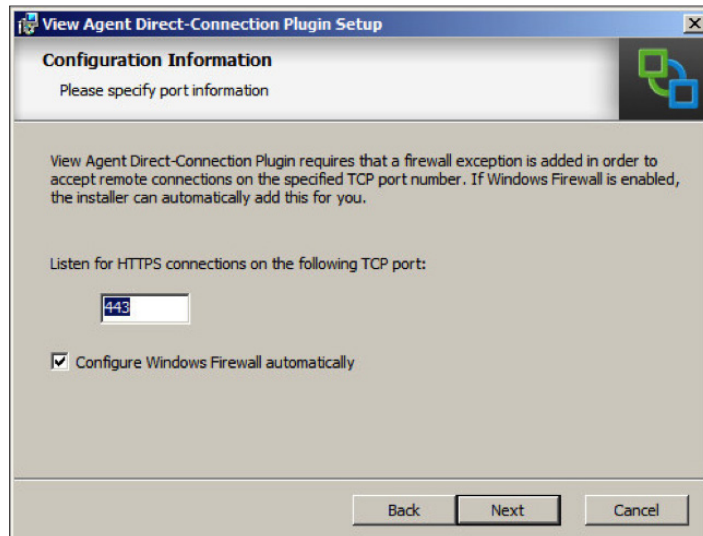
1. Launch the View Agent Direct-Connection Plug-in installer using the Run As Administrator option. Ensure that the installer is accessible from your virtual machine. When the launcher loads, click **Next**.



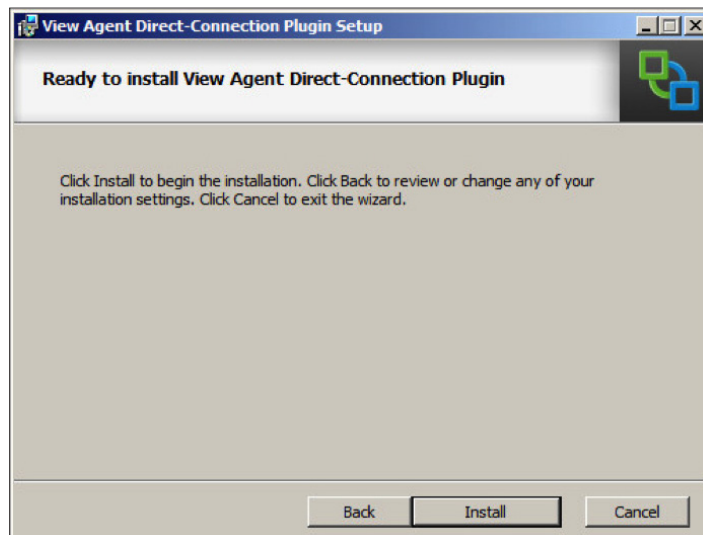
2. Read the license agreement, accept the terms and conditions, and click **Next**.



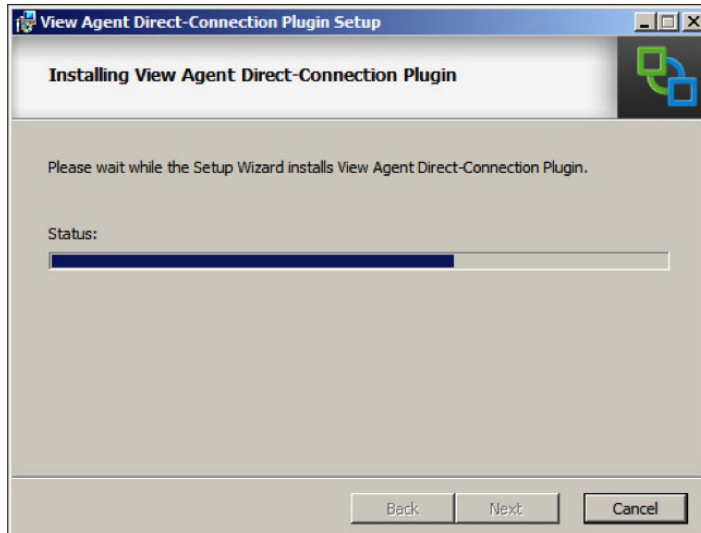
3. Confirm the default port required for HTTPS connections, select the **Configure the Windows Firewall automatically** option, and then click **Next**.



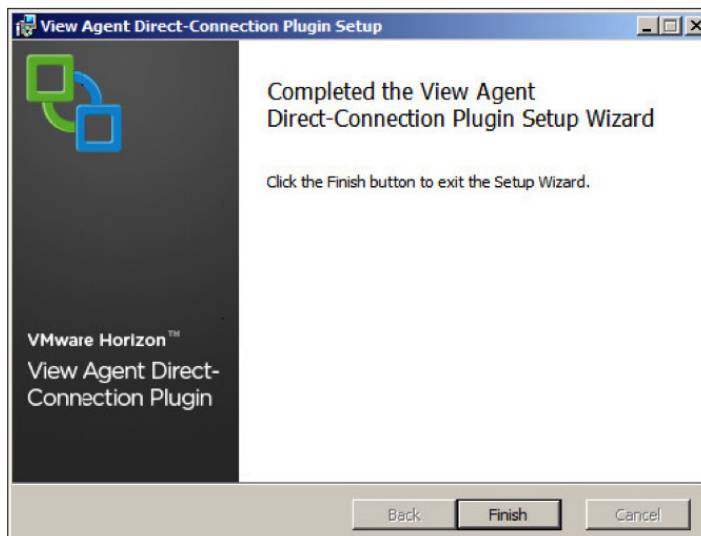
4. In the Ready to Install dialog box, click **Install** to proceed. If you want to make changes, click **Back**.



5. Monitor your installation status as it progresses.



6. 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 Parent Virtual Machine Operating System (Optional)

This exercise is optional but recommended. You can always come back to your Windows 2008 R2 SP1 View Template to install additional applications or modifications and then use the View Administrator console to update existing desktop pools or deploy new ones.

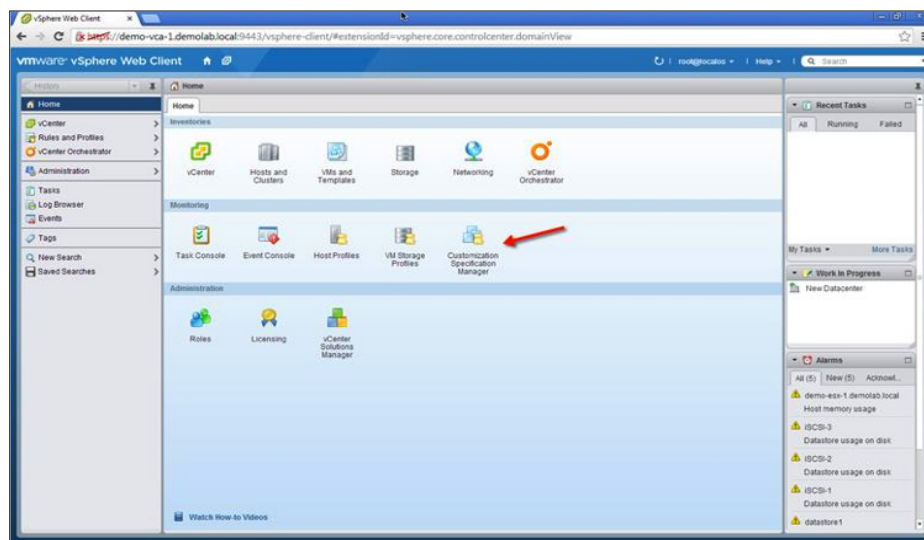
1. Install the custom applications that you want preinstalled on your Windows 2008 R2 SP1 View Template for View desktop deployment.
2. Make any modifications to the Windows operating system.
3. Verify that Windows Activation has been completed to ensure that your operating system is activated.

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

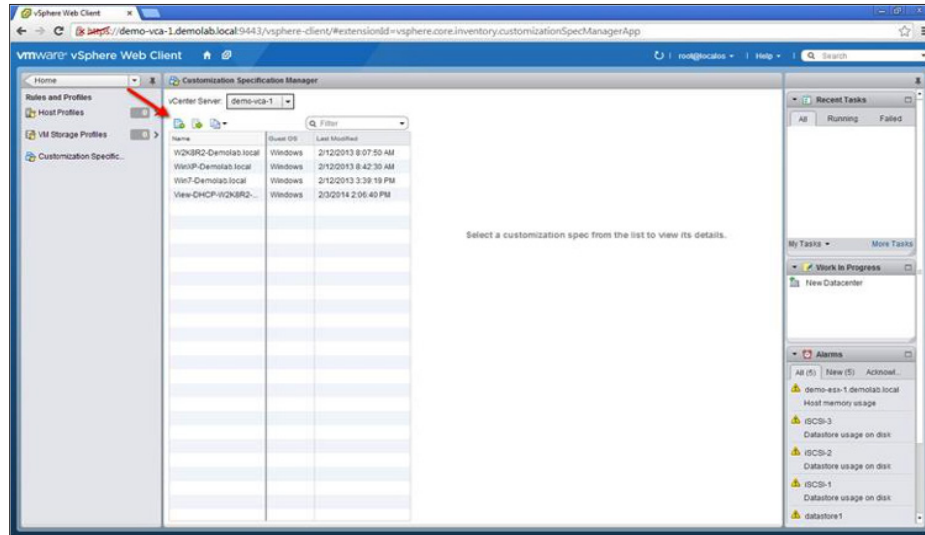
Prepare the Parent Virtual Machine for Full-Clone Deployment

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](#).

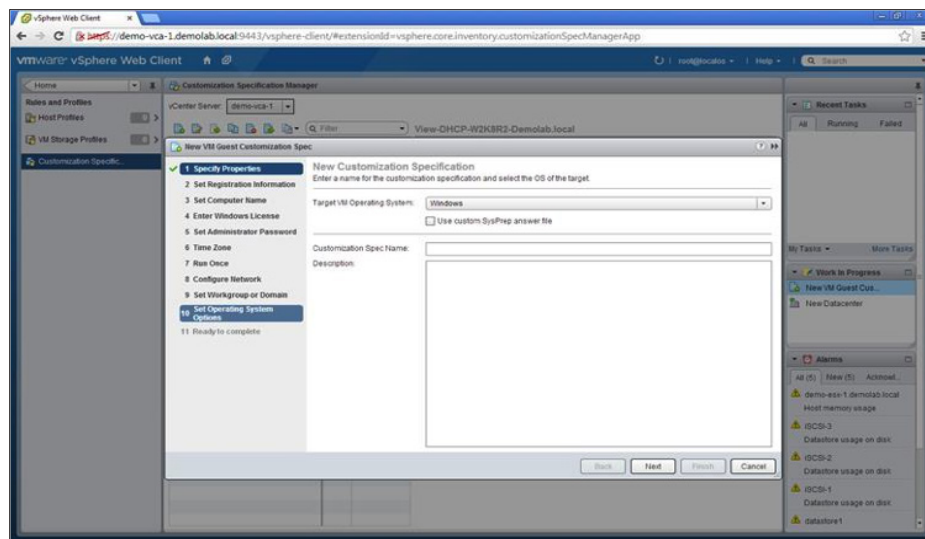
1. Navigate to the URL that connects you to your vSphere environment (vCenter Server) through the vSphere Web Client.
2. On the home page, click **Customization Specification Manager**.



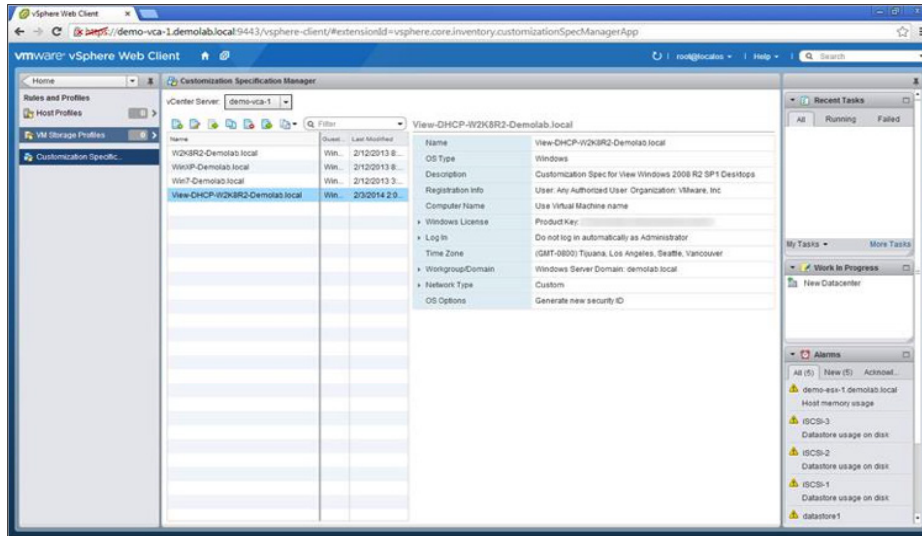
- Click the **Add** icon to create a customization specification to correspond to the Windows 2008 R2 SP1 View Template that you created.



- 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 its name because you need it when deploying the automated full-clone pool.



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

Deploying View Desktops and Applications

After you have finished preparing desktop images, you are ready to deploy View desktops and applications. In this series of exercises, you create and deploy linked-clone and full-clone desktop pools as well as RDS desktop and application pools.

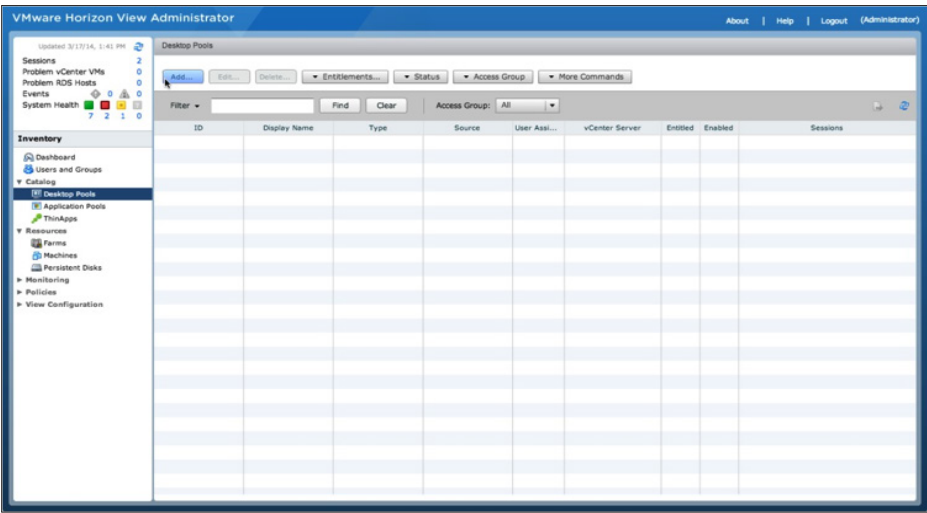
- [Deploy a Linked-Clone Desktop Pool](#)
- [Deploy a Full-Clone Desktop Pool](#)
- [Deploy an RDS Desktop Pool](#)
- [Deploy an Application Pool](#)

Deploy a Linked-Clone Desktop Pool

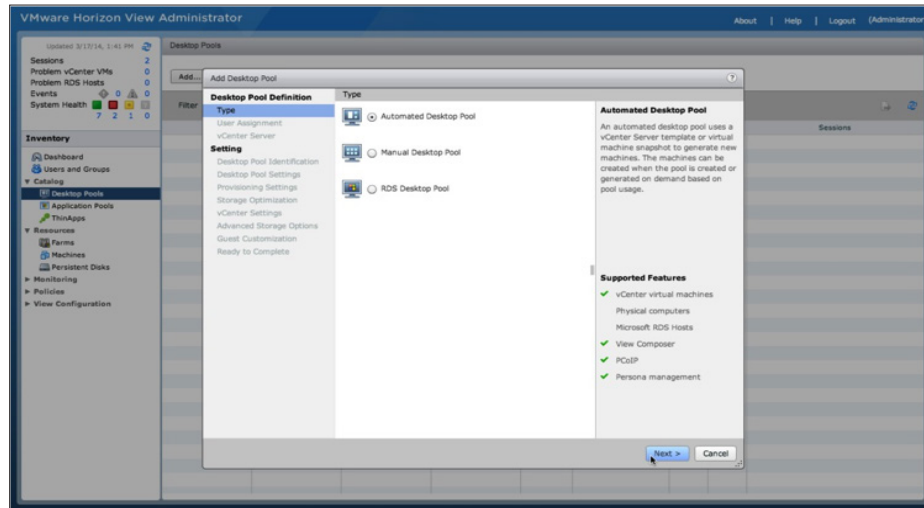
You deploy a linked-clone desktop pool based on the linked-clone desktop image that you prepared in earlier exercises.

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

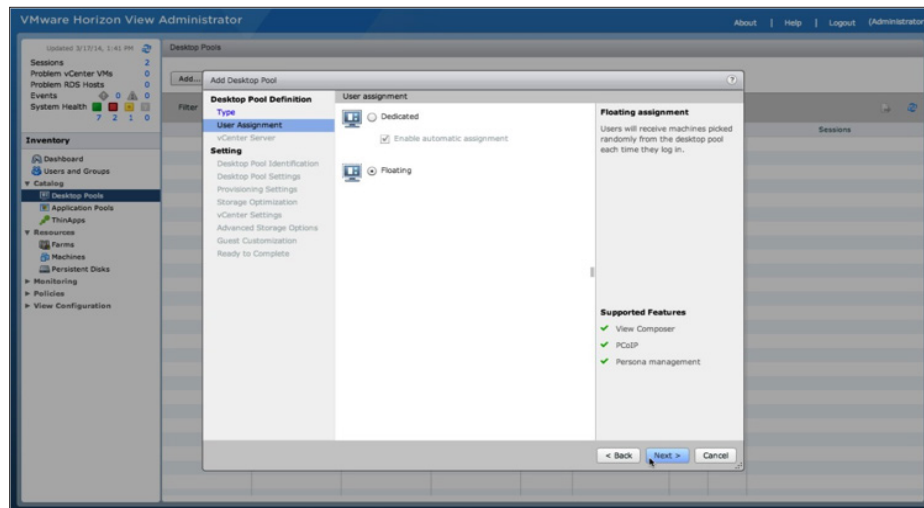
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To deploy a new pool, click **Add**.



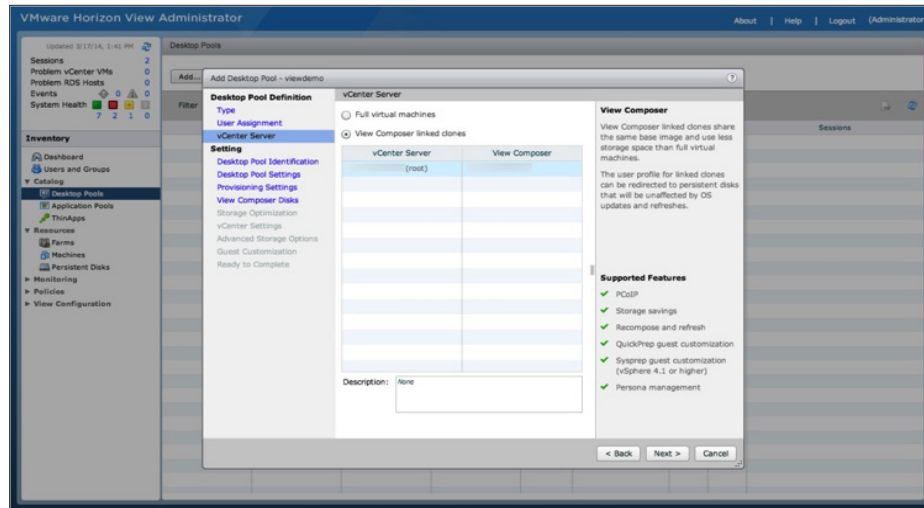
3. In the Add Desktop Pool window, select **Automated Desktop Pool**, and then click **Next**.



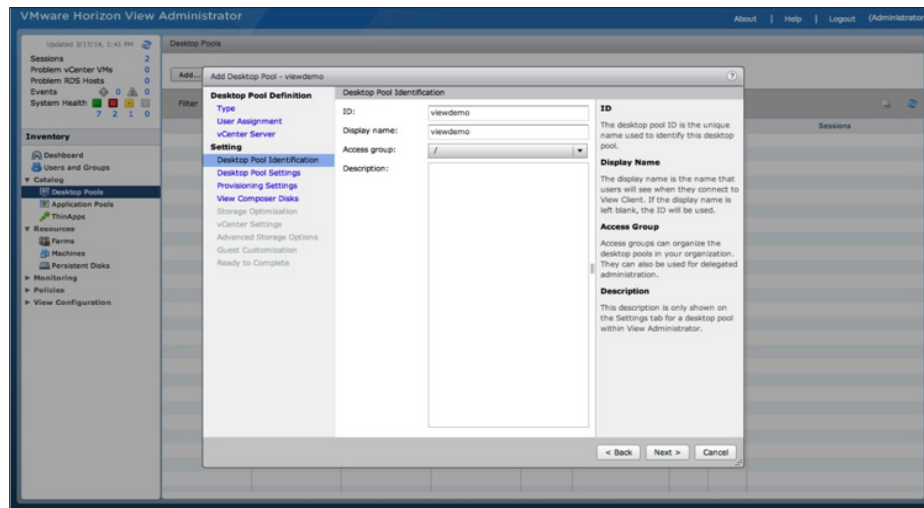
4. Specify the type of user assignment for the pool. You can select either dedicated or floating, but for this exercise, select **Floating** and then click **Next**.



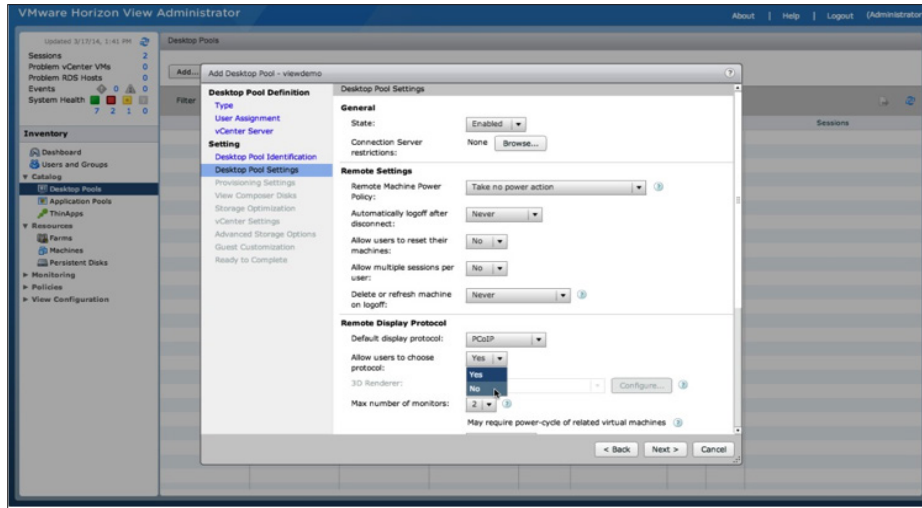
5. Select the type of virtual desktop to deploy. Select **View Composer linked clones** and click **Next**.



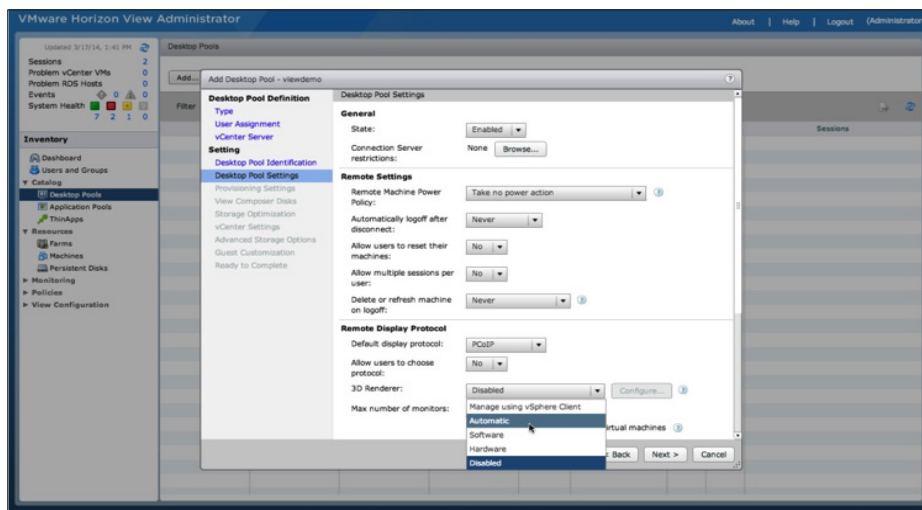
6. Add a pool ID and display name. Optionally, select a folder to organize your pools. Click **Next**.



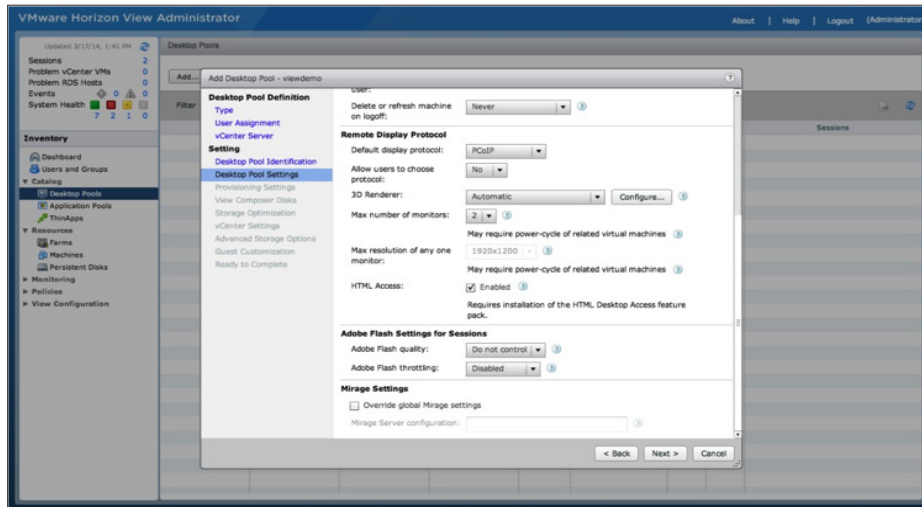
7. Adjust the pool settings to enable certain features. For this example, enable vSGA - 3D Virtual Shared Graphics for the desktop pool. Under Remote Display Protocol, set **Allow users to choose protocol setting** to **No**.



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

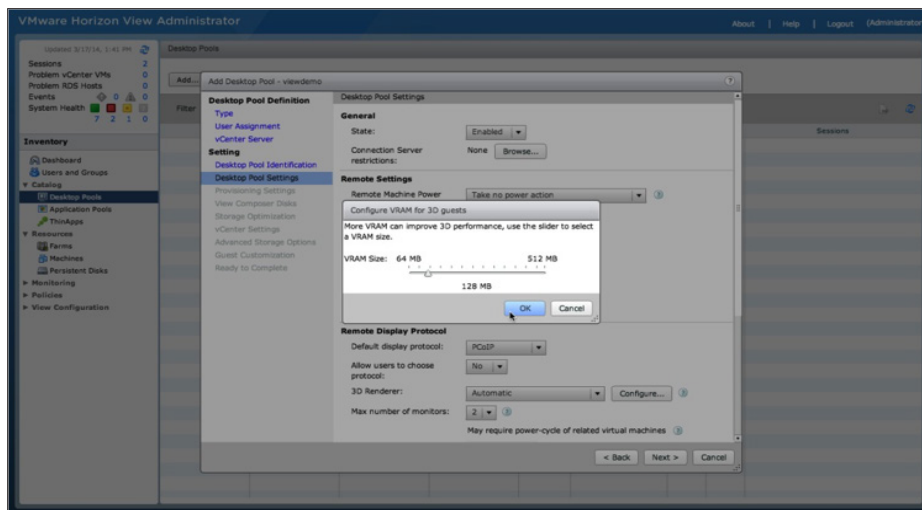


9. Scroll down the Pool Settings window to view the other available options. Enable **HTML Access**. Next to 3D Renderer, click **Configure**.



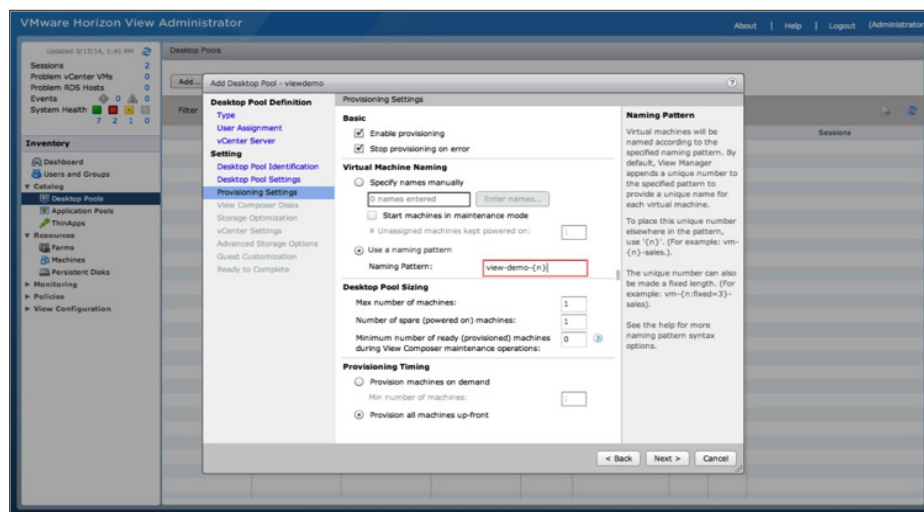
10. Use the slider to configure the amount of VRAM available to each virtual desktop guest and click **OK**.

11. Click **Next** to configure the provisioning settings.

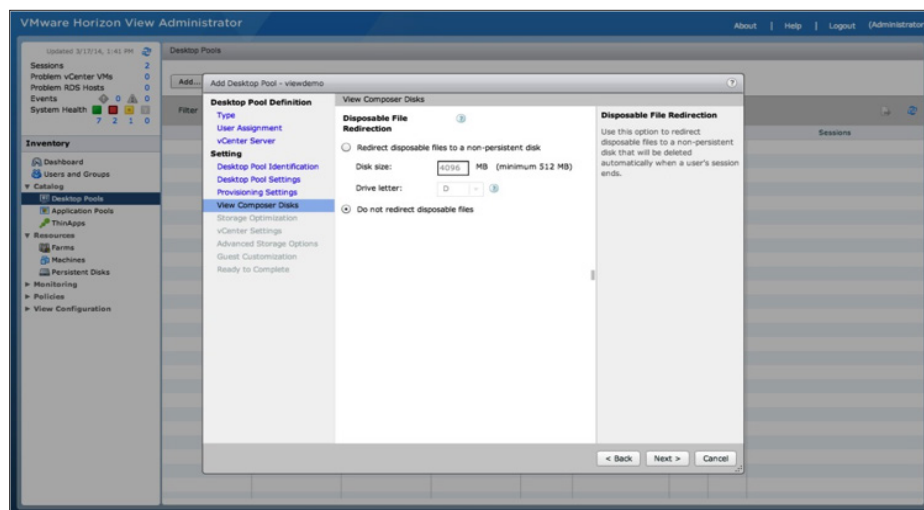


12. Adjust the provision settings and then click **Next**.

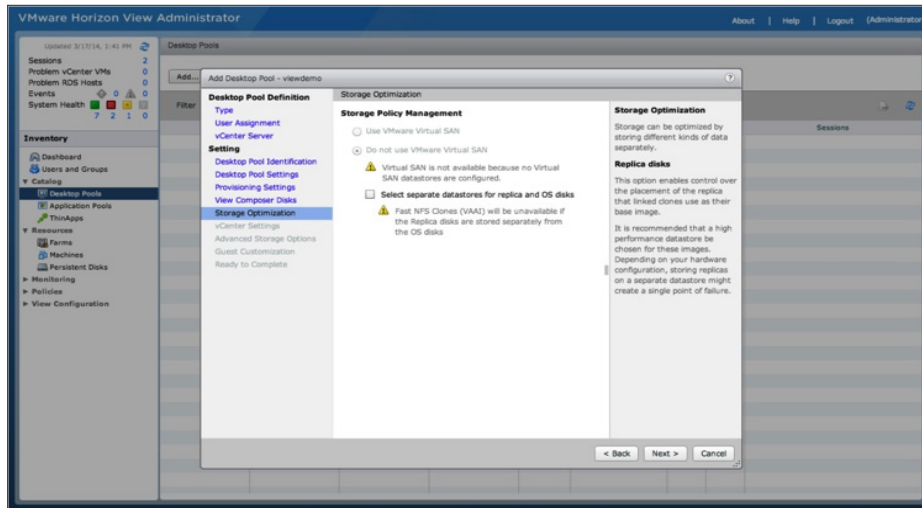
- Select **Use a naming pattern** and enter a naming pattern in the text box. A common pattern is `<poolname>-{n}`, which displays the poolname with an incremented desktop number as desktops in the pool are provisioned.
- Specify the maximum pool size. First deploy a small number of desktops to test your pool, and then increase the number of desktops after you have confirmed that your deployment is successful.
- Under Provision Timing, select **Provision all desktops 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 any additional desktops are provisioned as required, up to the maximum number of desktops. You can try these different pool features during subsequent pool deployments.



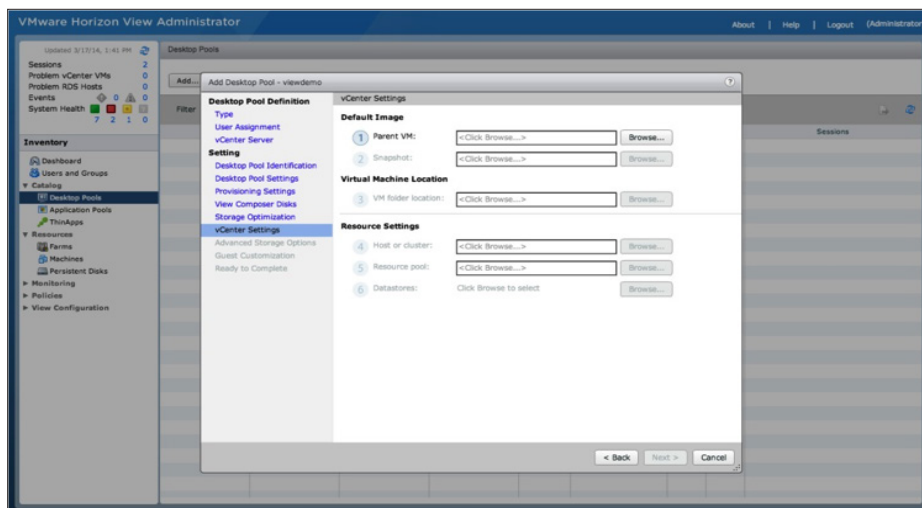
13. You can specify the type of disposable disks to deploy with the pool. For this exercise, select **Do not redirect disposable files** and click **Next**.



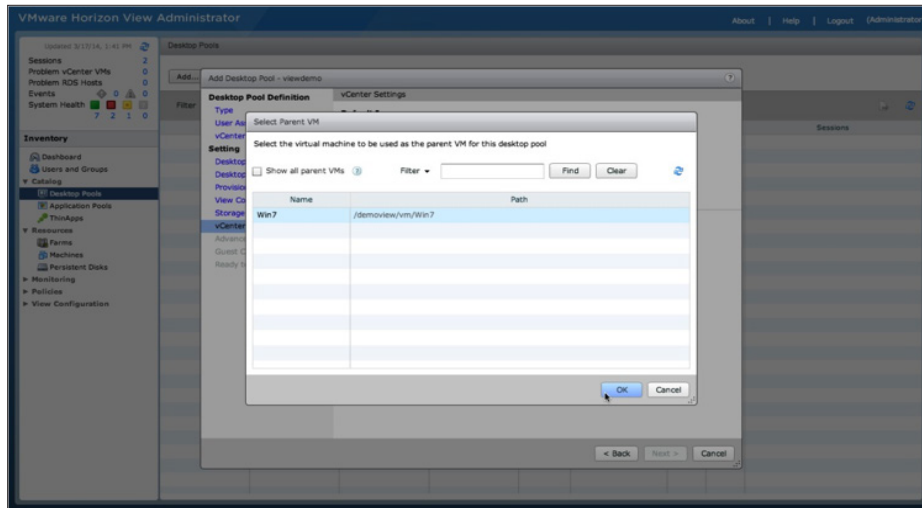
14. Do not make any modifications to the Storage Optimization options. Click **Next**.



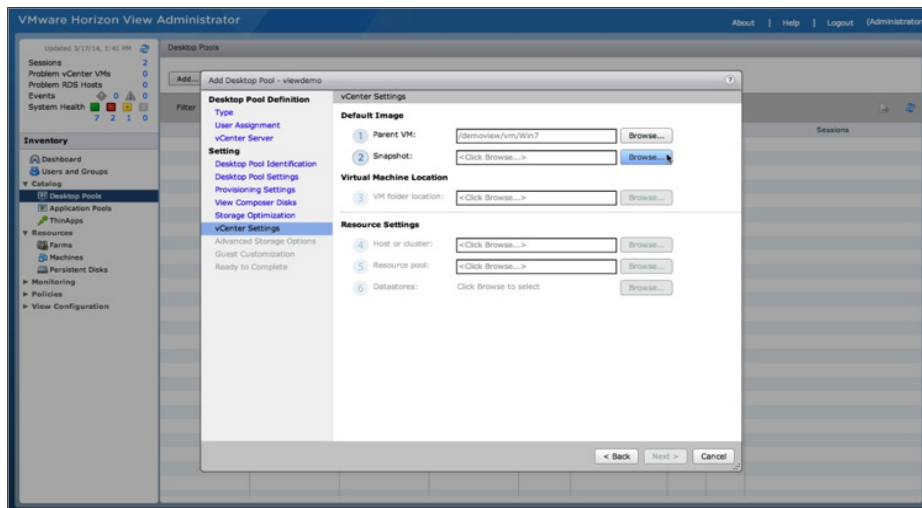
15. For the vCenter settings, select your Windows 7 template and associated options. Next to the Parent VM text box, click **Browse**.



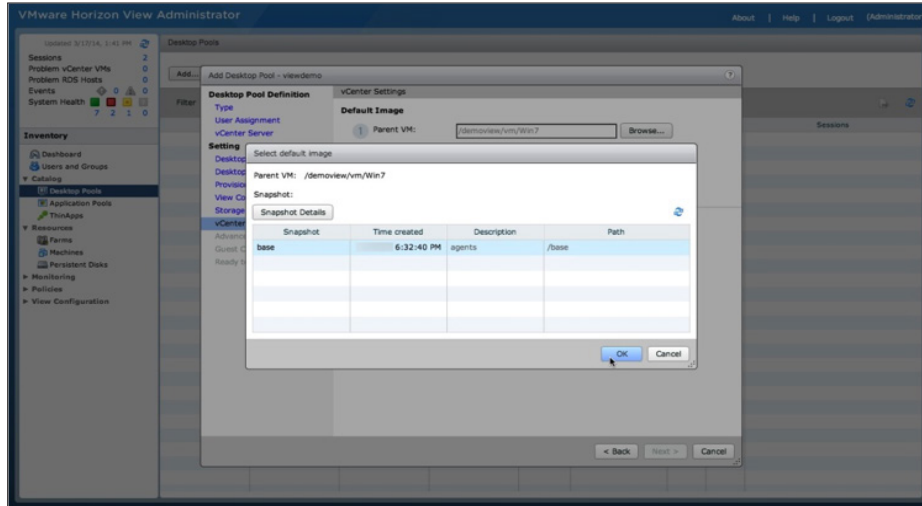
16. Click the Windows 7 parent virtual machine to use for the pool deployment and click **OK**.



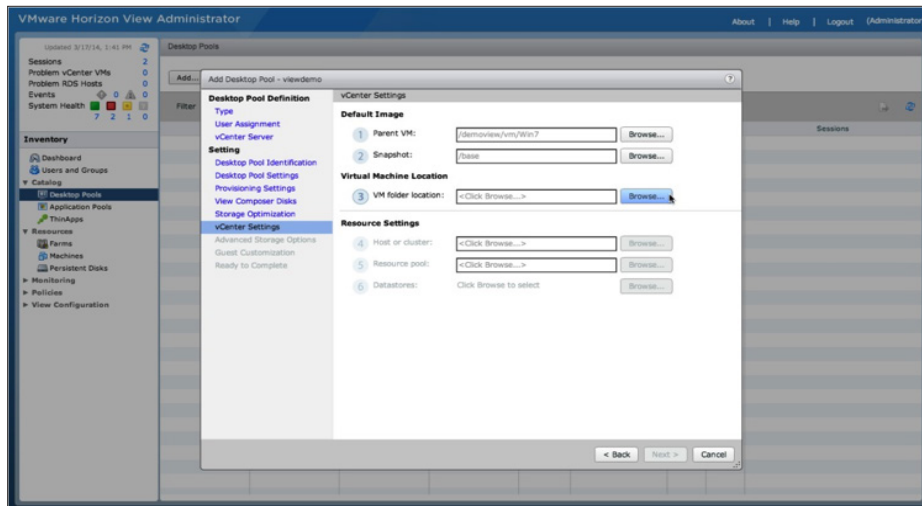
17. Next to the Snapshot text box, click **Browse**.



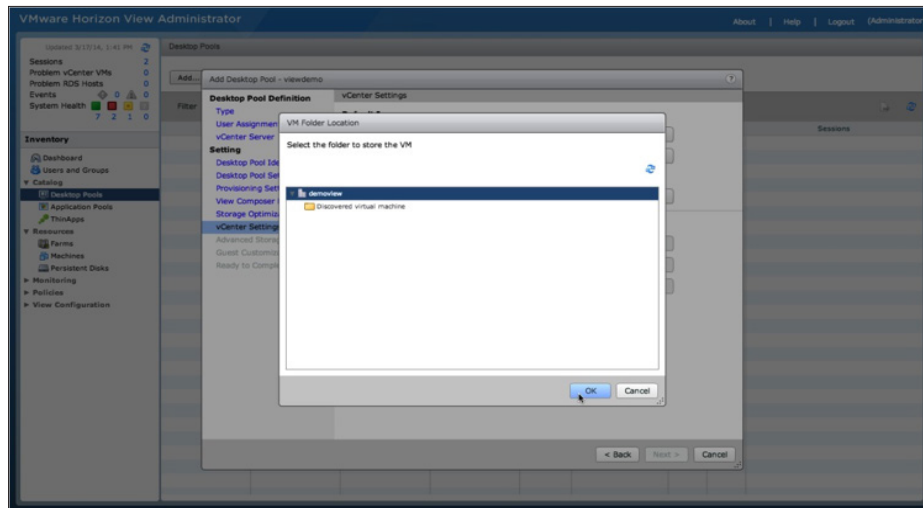
18. Click the snapshot to use for the pool deployment and click **OK**.



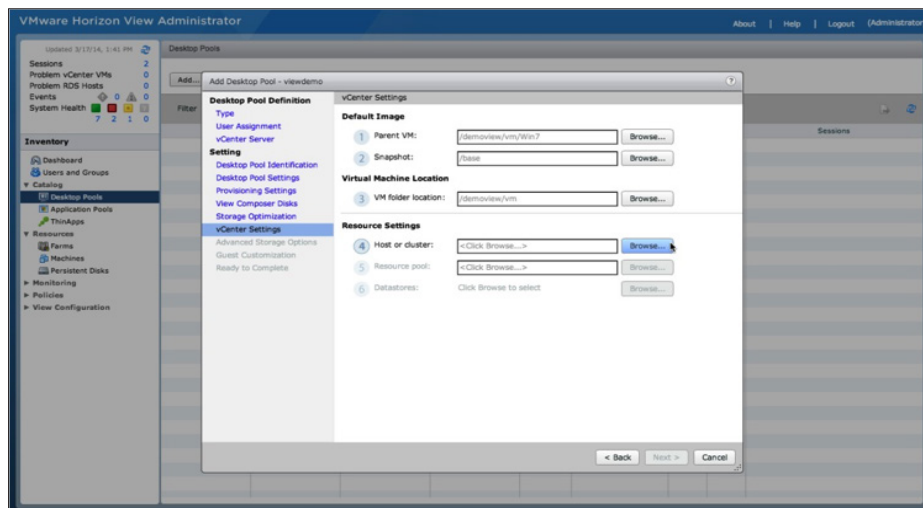
19. Next to the VM folder location text box, click **Browse**.



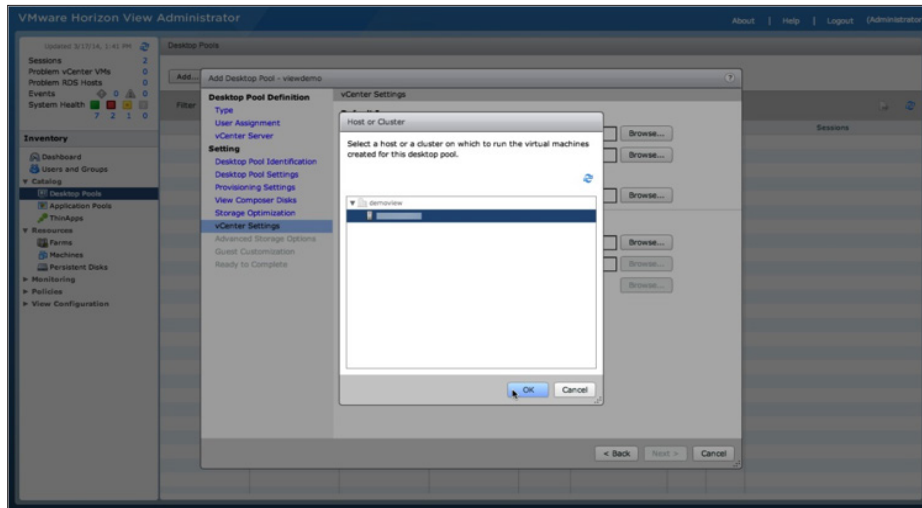
20. Click the folder location. If you do not have a folder created, select the data center and click **OK**.



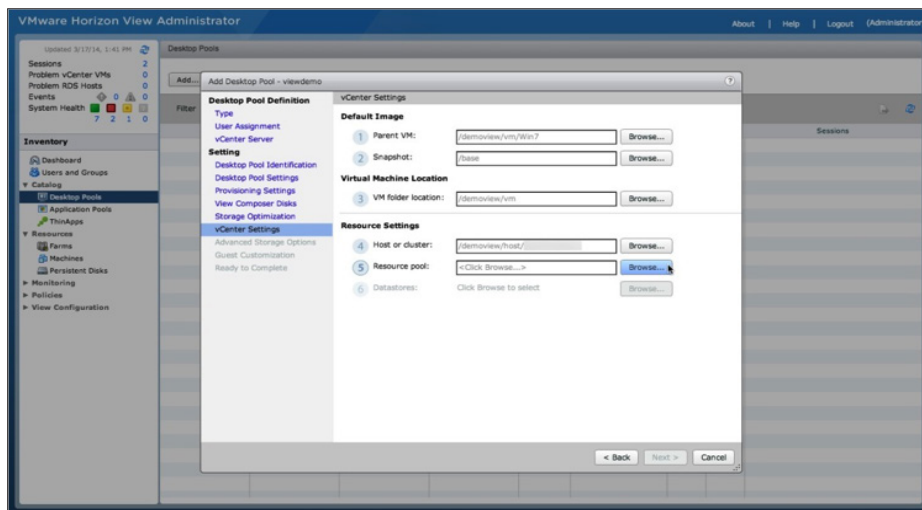
21. Next to the Host or cluster text box, click **Browse**.



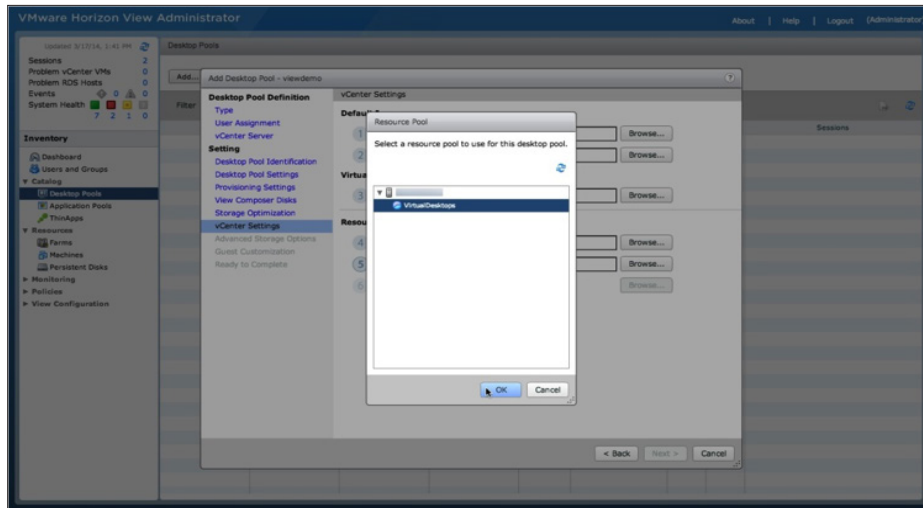
22. Click the target host or cluster for your pool desktop deployment and click **OK**.



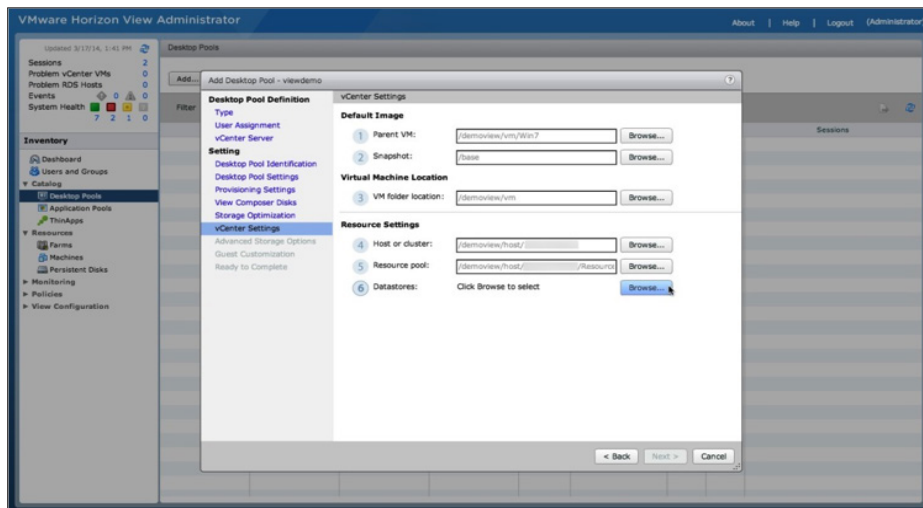
23. Next to the Resource pool text box, click **Browse**.



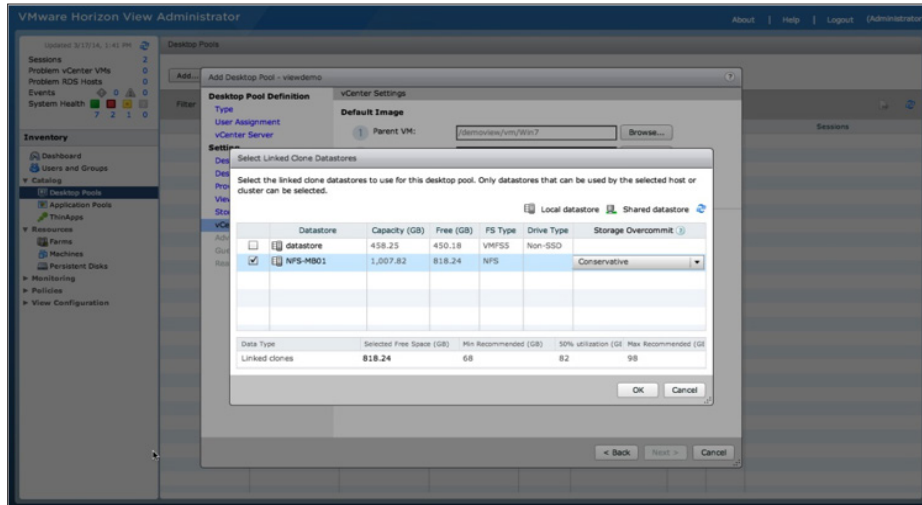
24. Click the resource pool to use, or select the host if you have not set up a resource pool, and click **OK**.



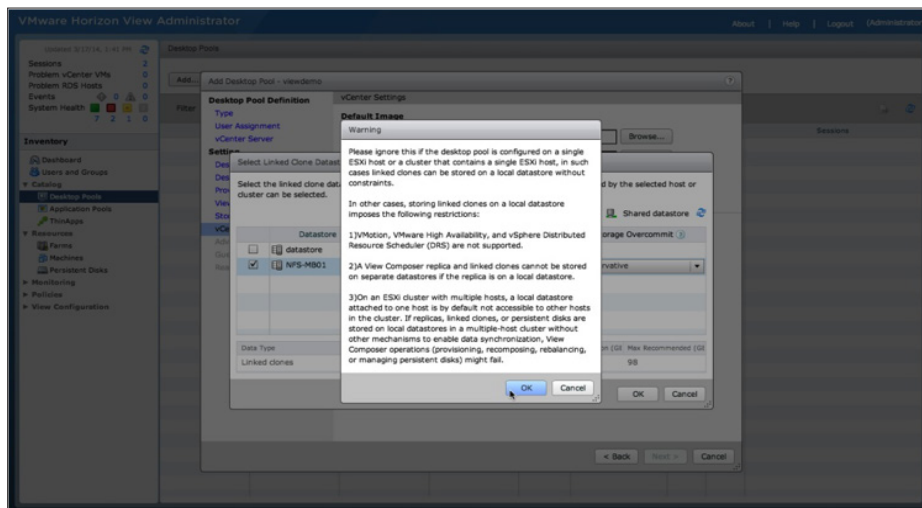
25. Next to the Datastores text box, click **Browse**.



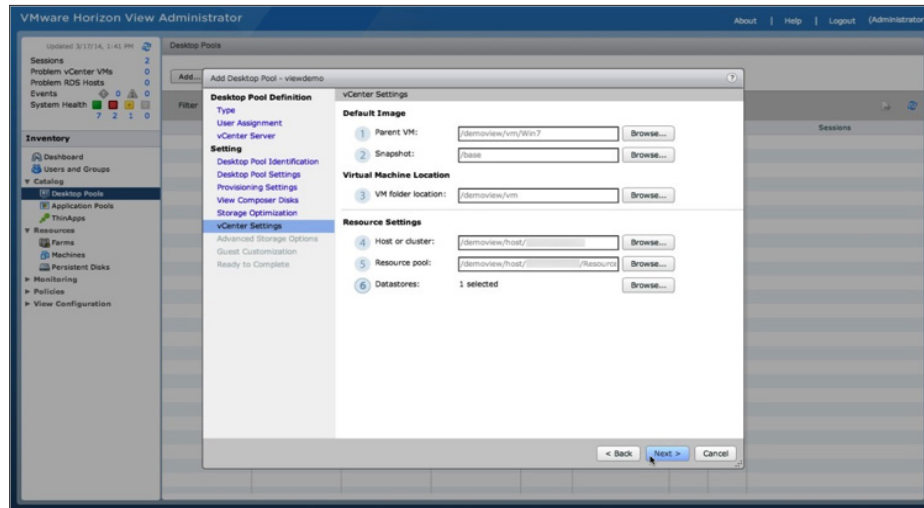
26. Click the target datastore to store your virtual desktops. You can leave the Storage Overcommit settings as the default Conservative. Click **OK**.



27. You receive a warning if you are storing your virtual desktops on a local datastore or are only using a single host. Because you are using a single host, you can ignore this warning. Click **OK** to continue.

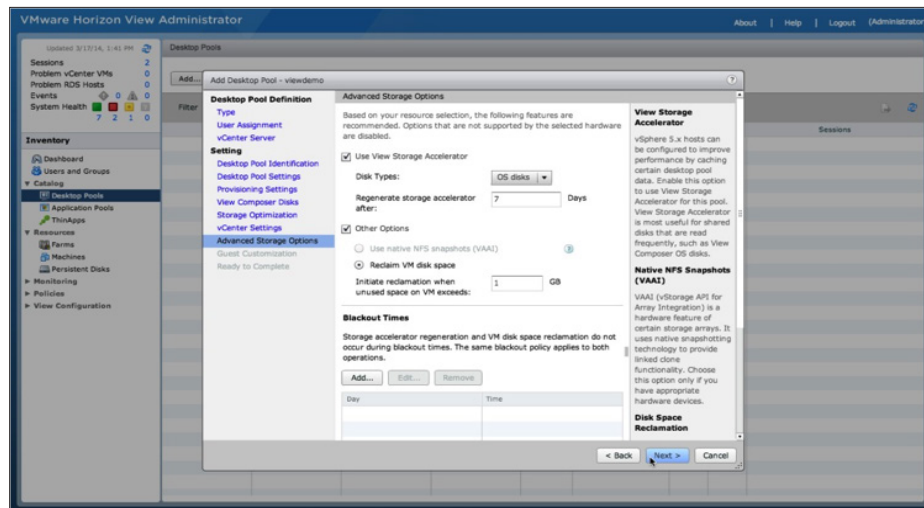


28. Review your vCenter settings and click **Next**. To make changes, click **Back**.

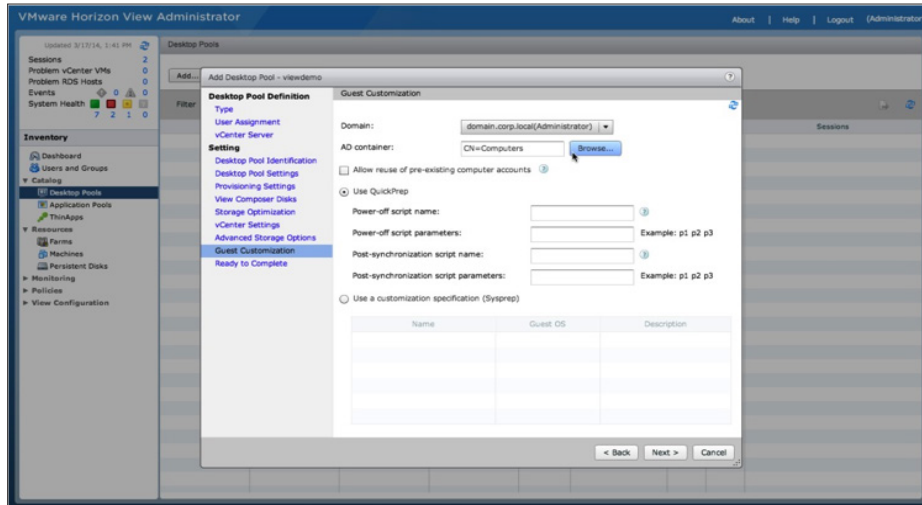


29. Adjust the Advanced Storage Options and then click **Next**.

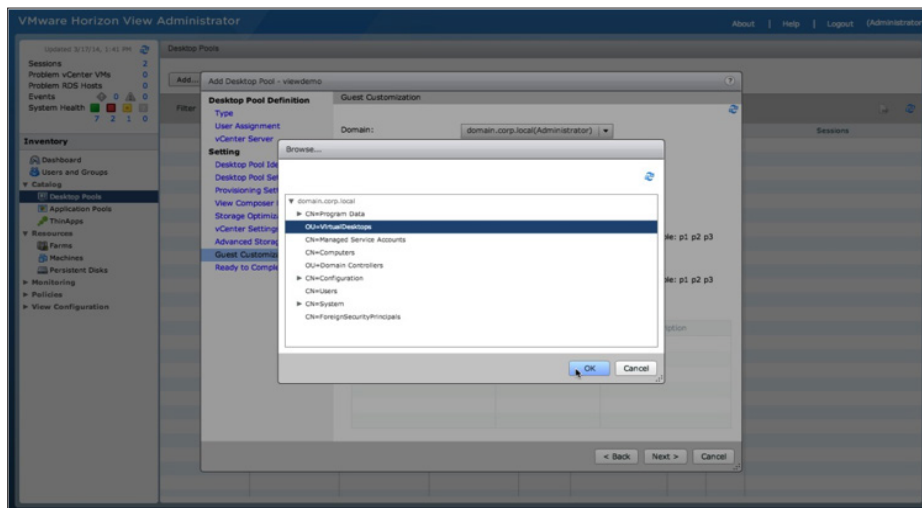
- Optionally select **Use View Storage Accelerator**.
- Select **Other Options** and then select **Reclaim VM disk space**.
- Specify the value for **Initiate reclamation when unused space on VM exceeds**. The recommended value is 1GB.



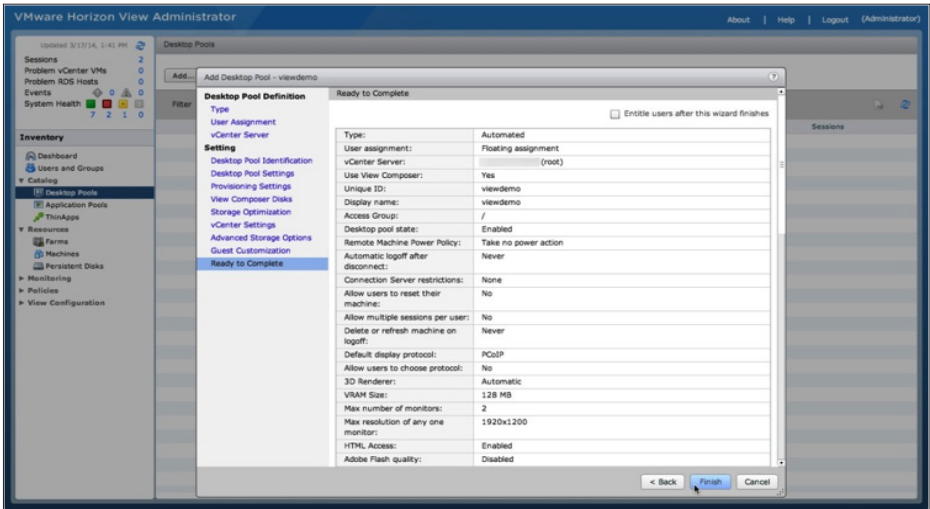
30. Adjust the AD container. Click **Browse** next to the text box to view the available AD containers for the domain.



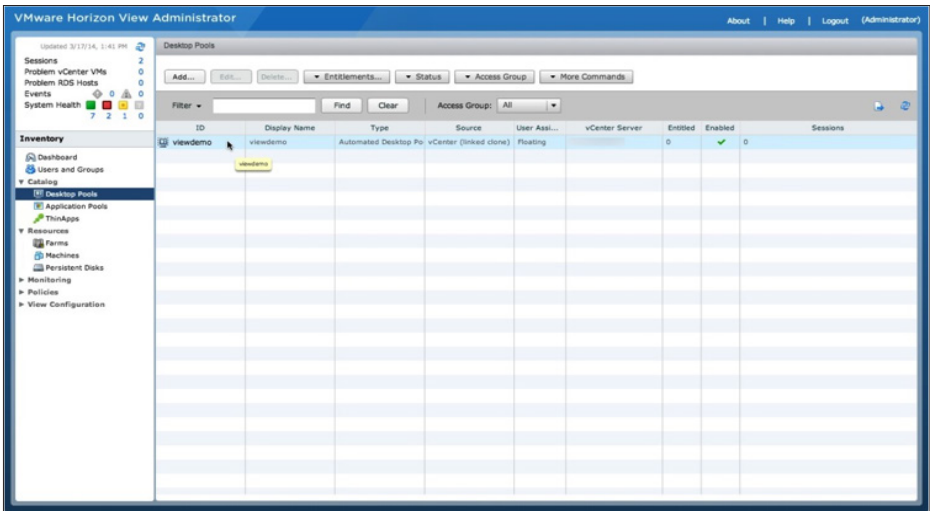
31. Select a valid OU or the default CN to store your View desktop computer account names and click **OK**. In the Guest Customization window, click **Next**.



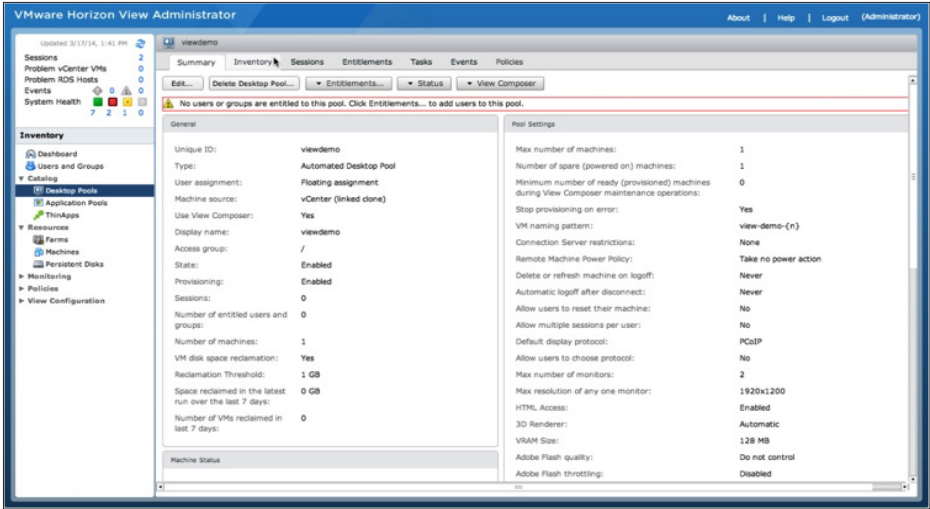
32. Review the summary of all your pool settings and click **Finish** to deploy the pool. Or to make changes, click **Back**.



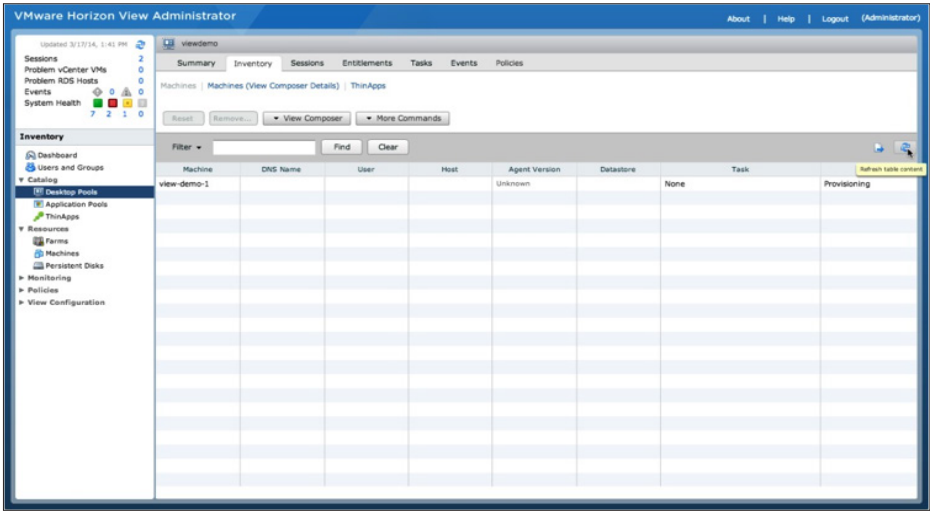
33. You return to the pool inventory list. Double-click your desktop pool to check the deployment status.



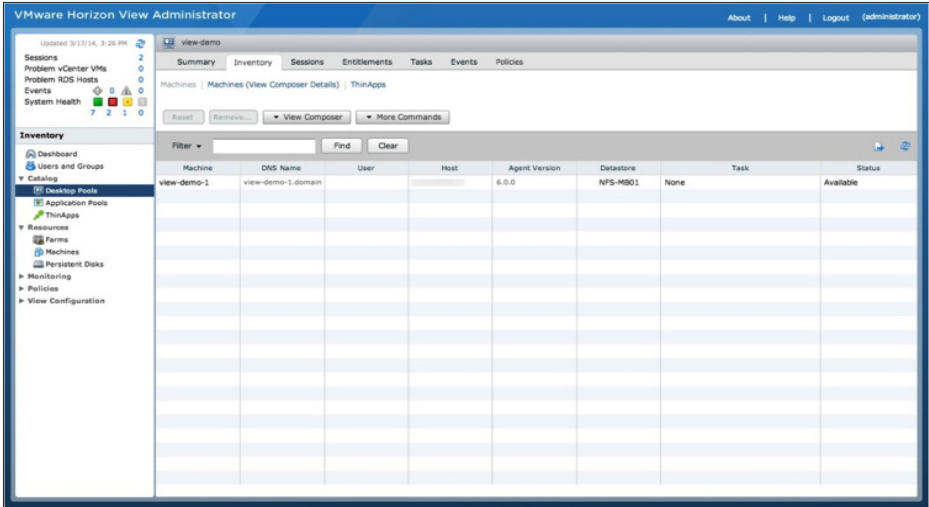
34. You return to the pool settings overview. Click the **Inventory** tab to check the individual desktop deployment status.



35. You can now monitor the deployment status for each desktop. Click the **Refresh** icon to update the status.



36. 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.

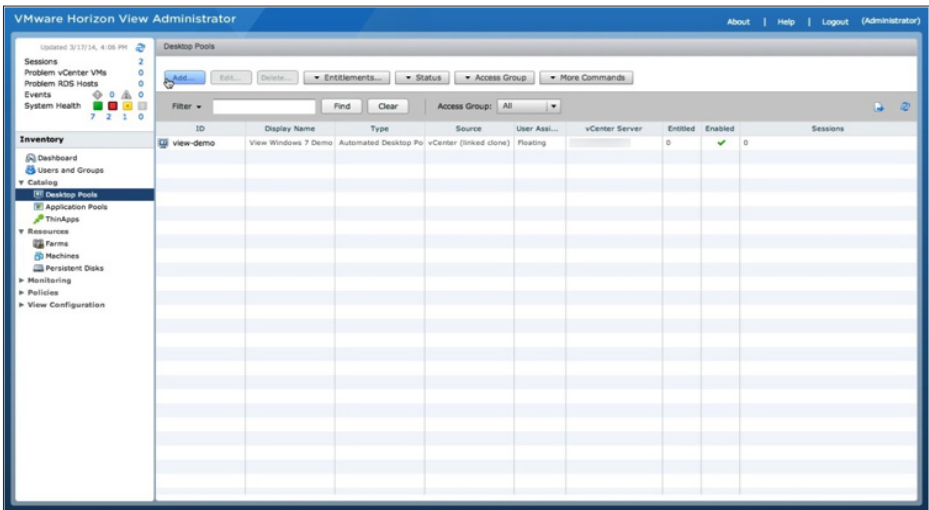


You have now created a linked-clone desktop pool. You can now proceed to creating a full-clone desktop pool.

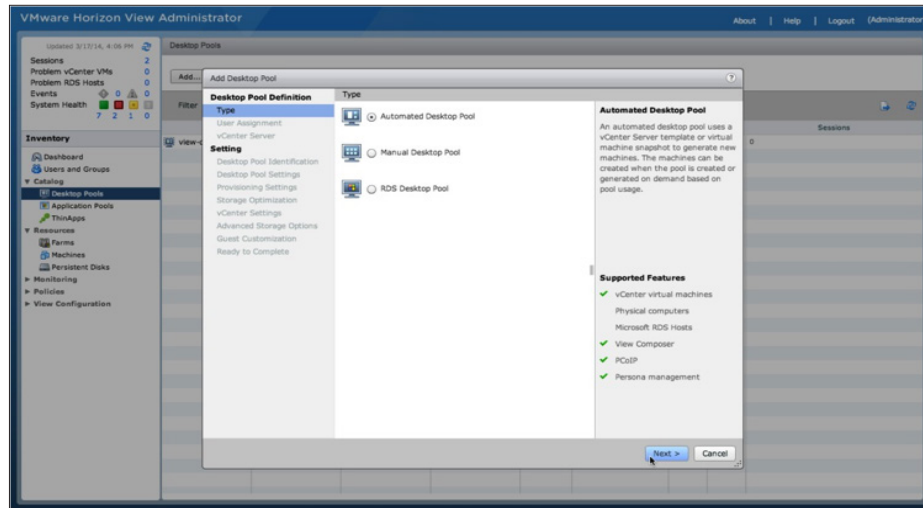
Deploy a Full-Clone Desktop Pool

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

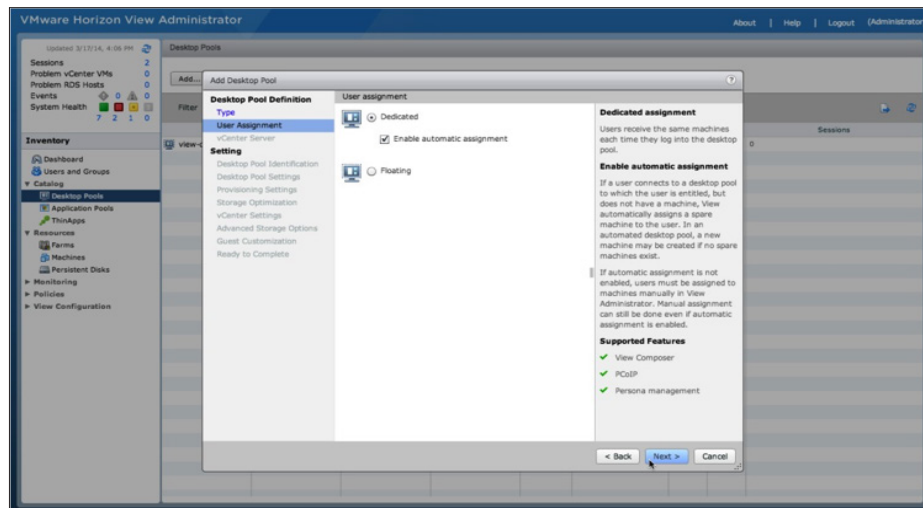
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To deploy a new pool, click **Add**.



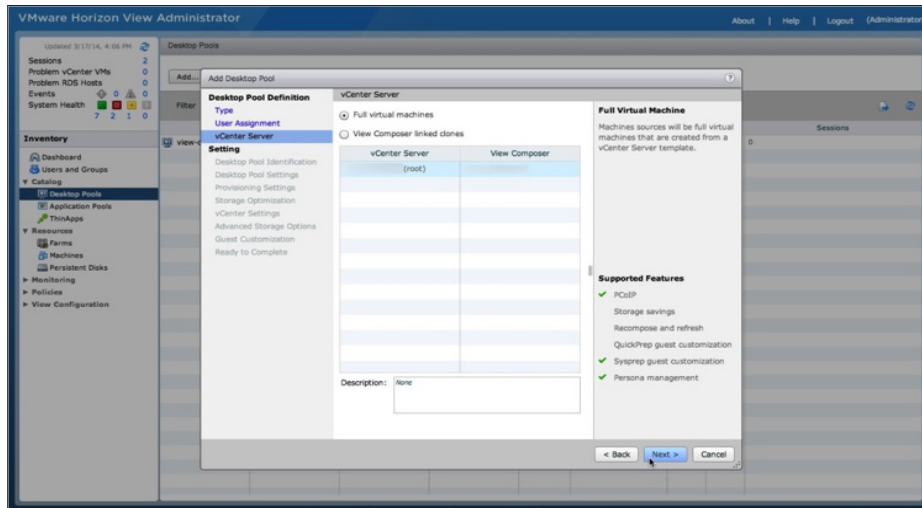
3. In the Add Desktop Pool window, select **Automated Desktop Pool**, and then click **Next**.



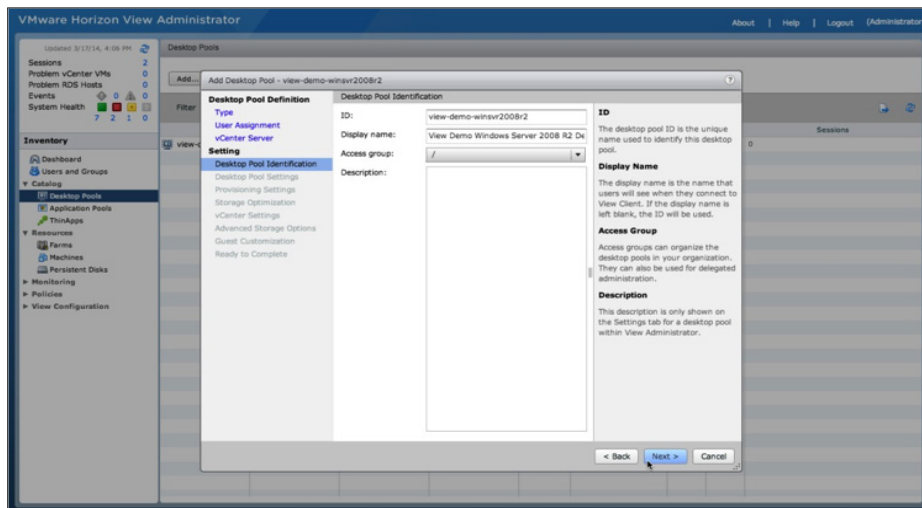
4. Specify the type of user assignment for the pool. You can select either dedicated or floating, but for this exercise, select **Dedicated**. You can optionally select **Enable automatic assignment**. Click **Next**.



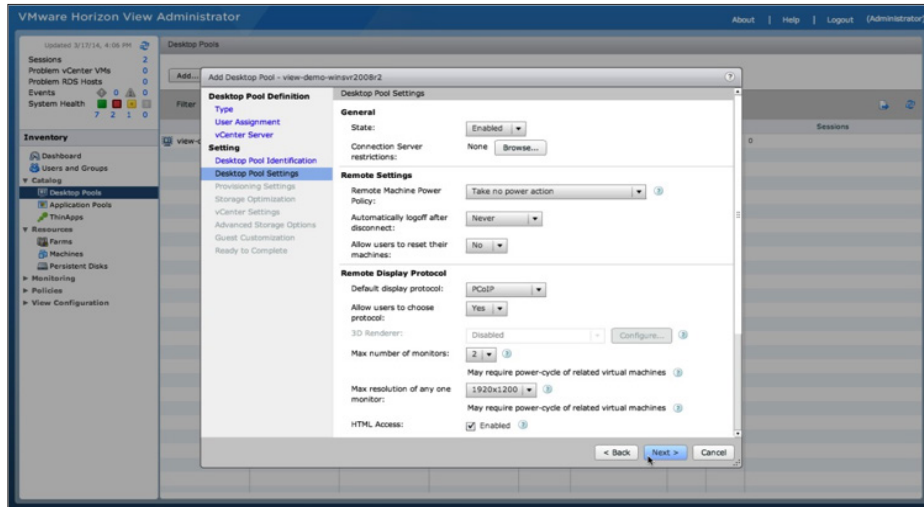
5. Select the type of virtual desktop to deploy. Select **Full virtual machines** and click **Next**.



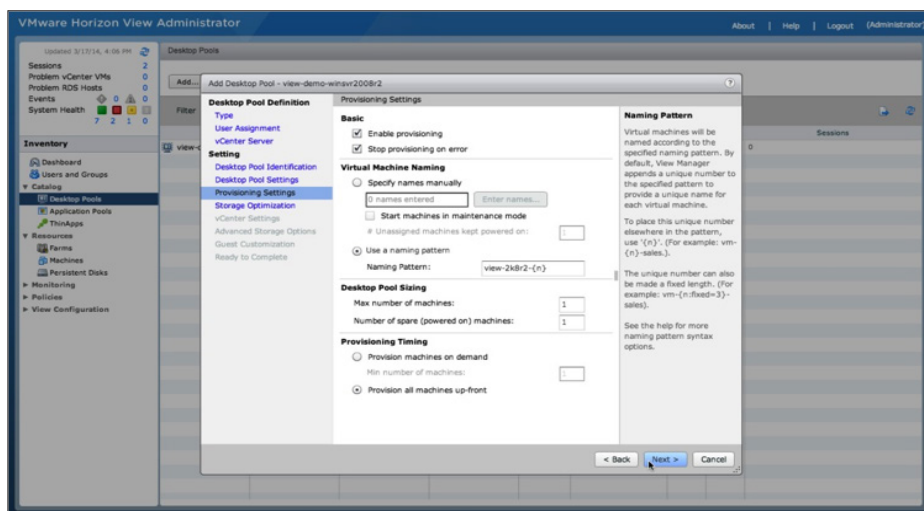
6. Add a pool ID and display name. Optionally, select a folder to organize your pools. Click **Next**.



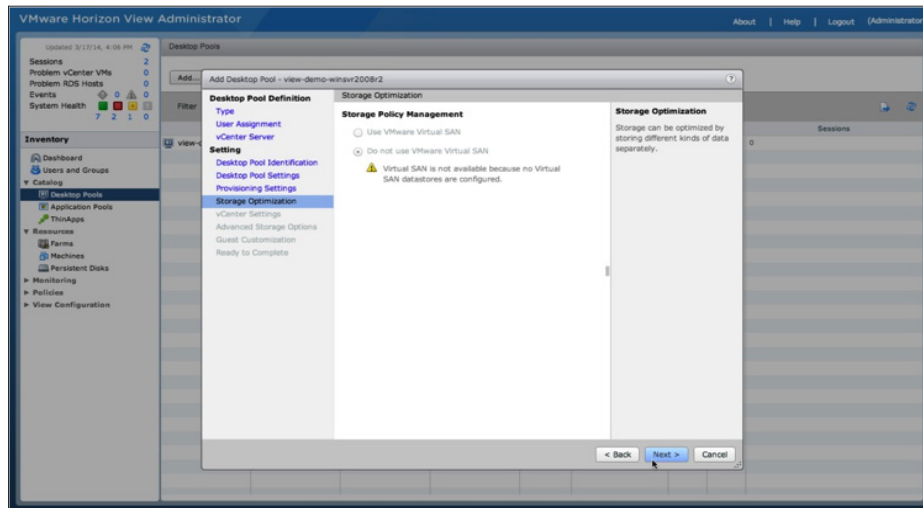
7. Scroll down the Pool Settings window to see the available options. Make sure that **HTML Access** is enabled. Click **Next**.



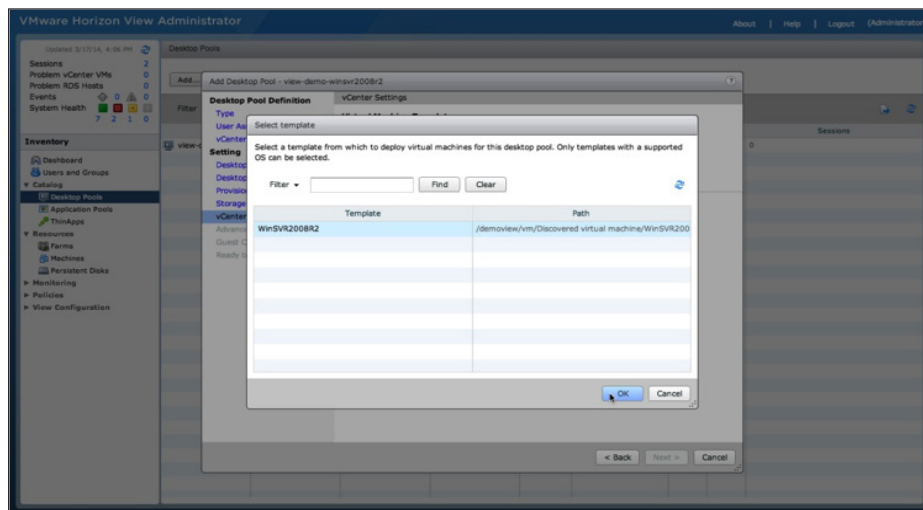
8. Adjust the provision settings and then click **Next**.
 - a. Select **Use a naming pattern** and enter a naming pattern in the text box. A common pattern is `<poolname>-{n}`, which displays the poolname with an incremented desktop number as desktops in the pool are provisioned.
 - b. Specify the maximum pool size. First deploy a small number of desktops to test your pool, and then increase the number of desktops after you have confirmed that your deployment is successful.
 - c. Under Provision Timing, select **Provision all desktops 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 any additional desktops are provisioned as required, up to the maximum number of desktops. You can try these different pool features during subsequent pool deployments.



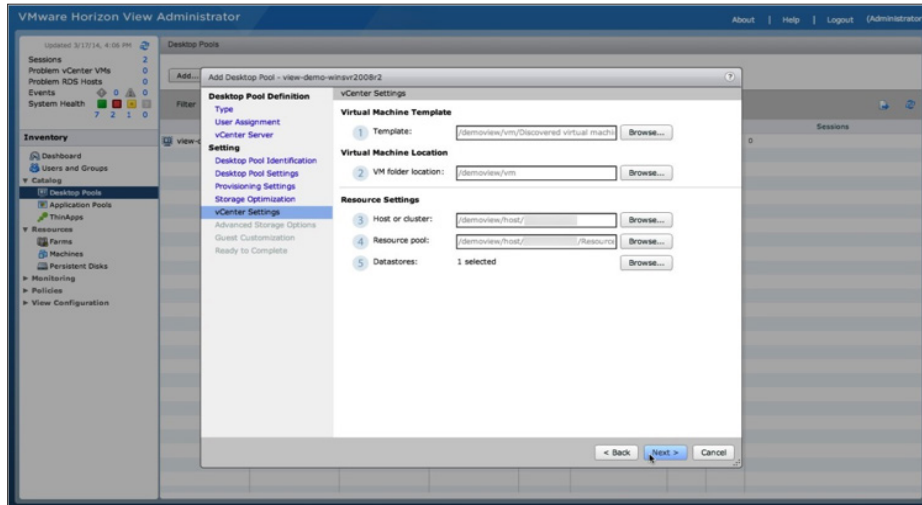
9. For the Storage Optimization settings, you can accept the defaults and click **Next**.



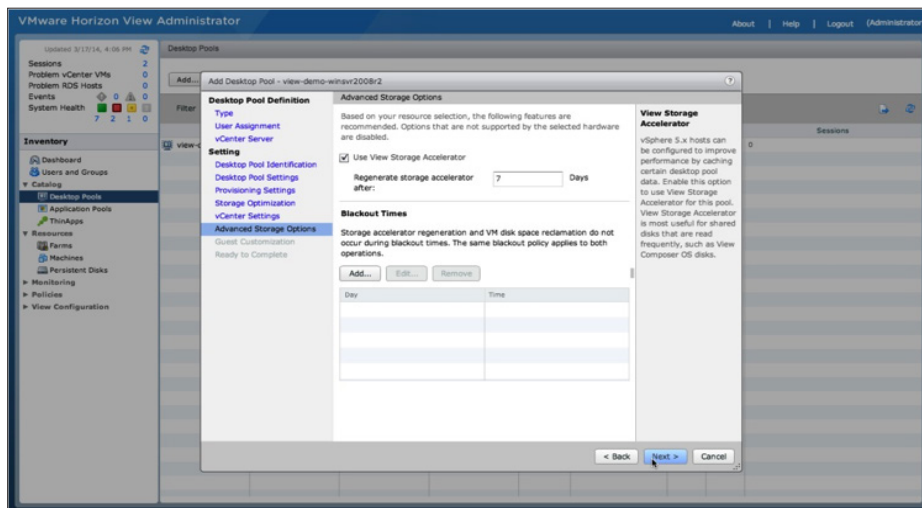
10. For the vCenter Settings, select the Virtual Machine Template to use by clicking **Browse** next to the Template text box. Select the Windows Server 2008 R2 SP1 View desktop template you set up earlier and click **OK**.



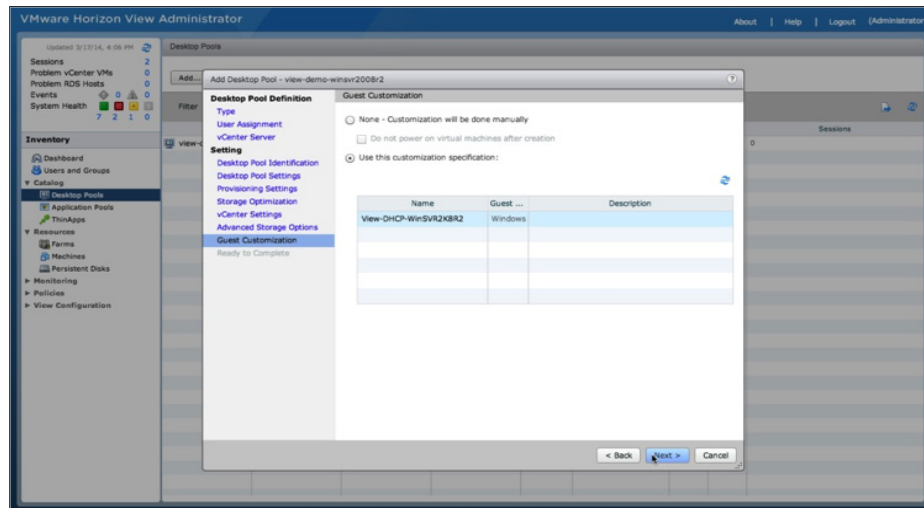
11. Continue through the other vCenter settings, selecting values for virtual machine folder location, host or cluster, resource pool, and datastore, and then click **Next**.



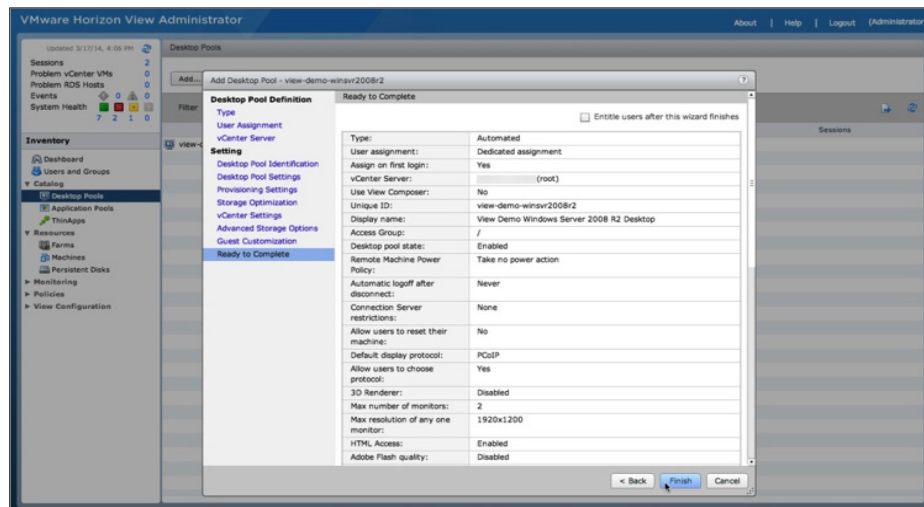
12. Adjust the Advanced Storage Options. Optionally select **Use View Storage Accelerator**. Click **Next** to continue.



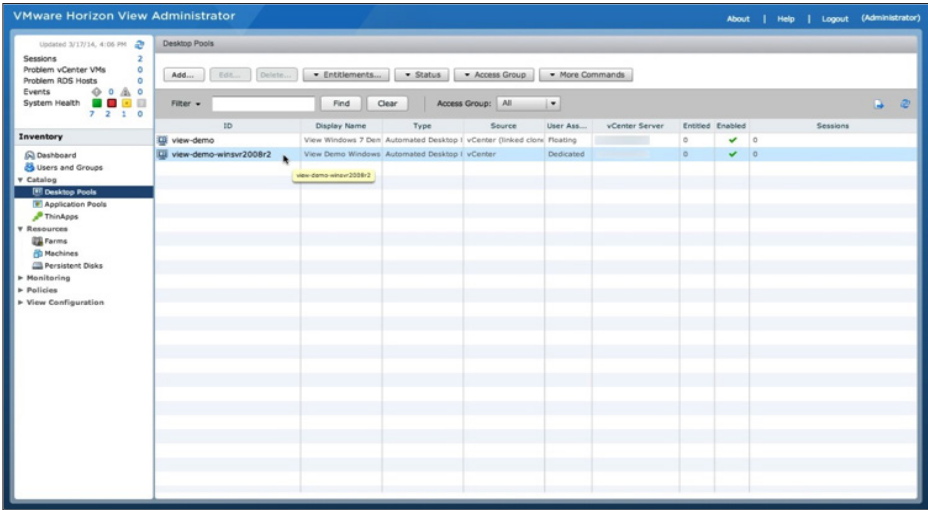
13. For the Guest Customization options, select **Use this customization specification**. Select the customization specification you created to customize your Windows Server 2008 R2 SP1 View desktop template. Click **Next**.



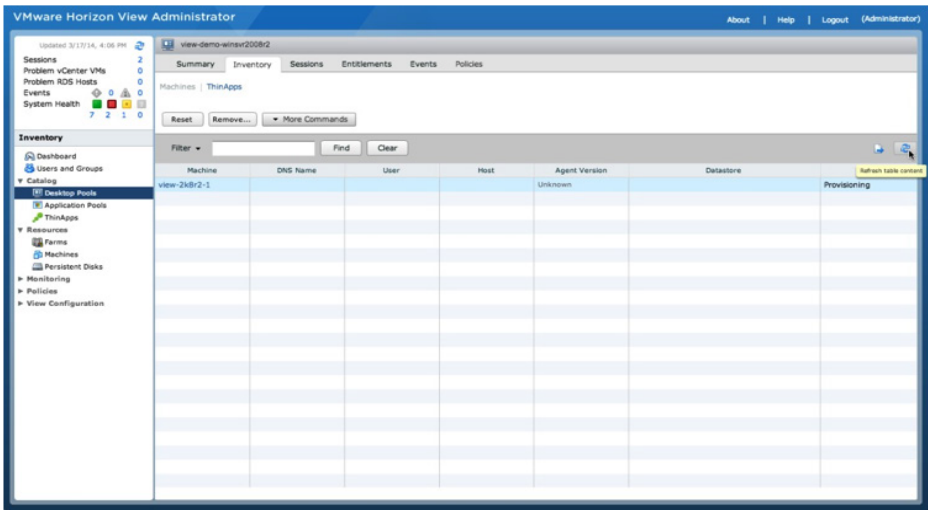
14. Review the summary of all your pool settings and click **Finish**. Or to make changes, click **Back**.



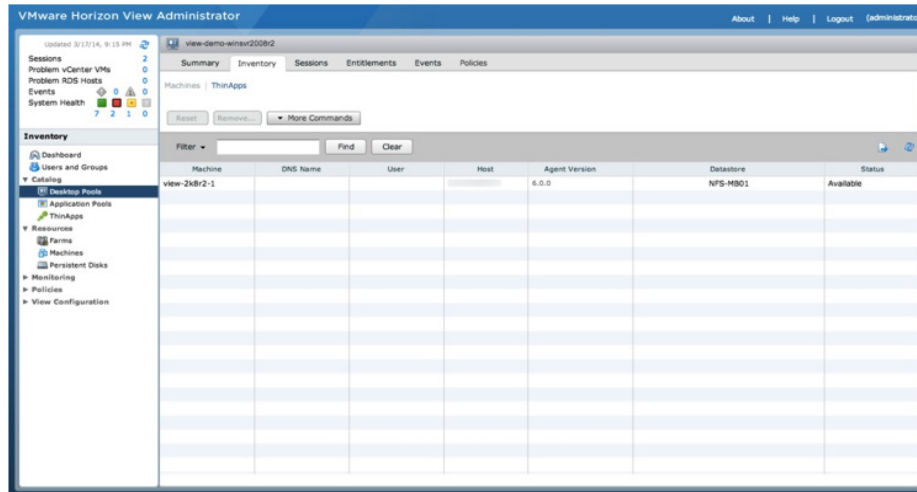
15. You return to the pool inventory list. Double-click your desktop pool to check the deployment status.



16. You return to the pool settings overview. Click the **Inventory** tab to check the individual desktop deployment status. You can monitor the deployment status for each desktop. Click the **Refresh** icon to update the status.



17. 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.



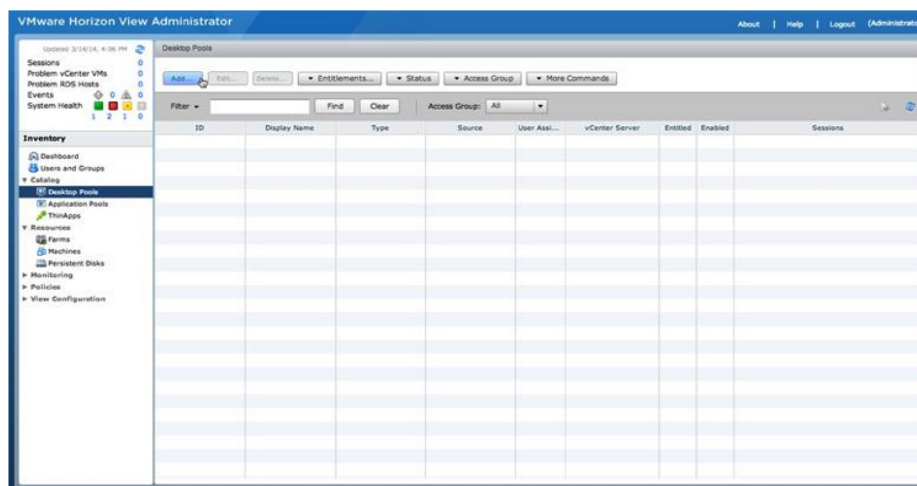
You have now deployed a full-clone desktop pool.

Deploy an RDS Desktop Pool

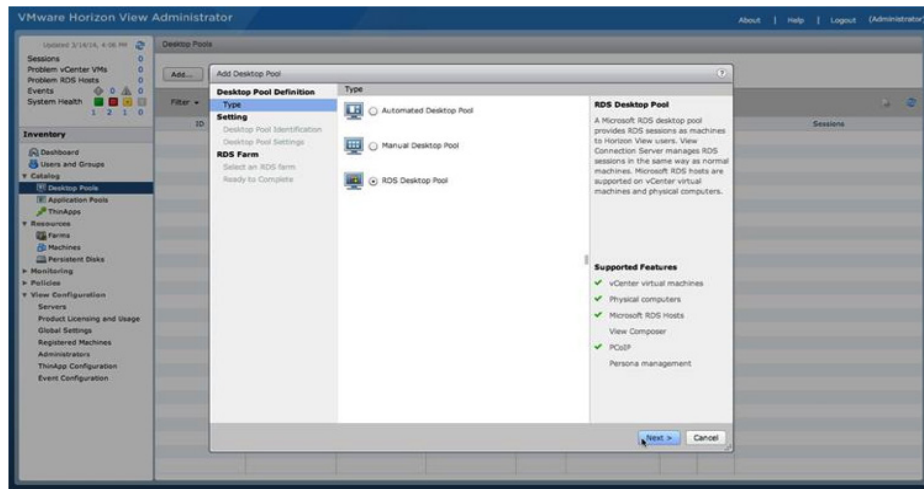
You will now deploy an RDS desktop pool. In previous View releases, this was known as a Microsoft Terminal Services pool. An RDS desktop pool has different characteristics compared to full-clone-based or linked-clone-based automated desktop pools. An RDS desktop pool is based on a session to an RDS host.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

You will use the RDS host that you set up and configured in previous exercises to deploy an RDS desktop pool.

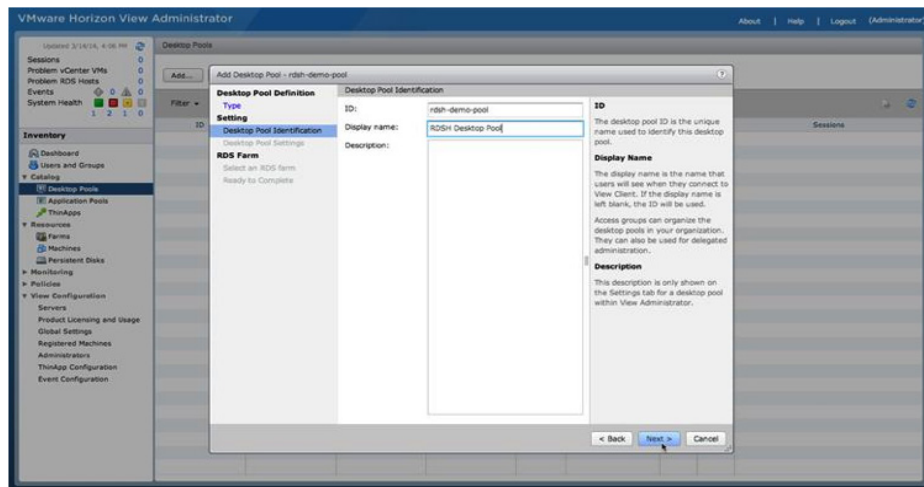
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To create a new pool, click **Add**.



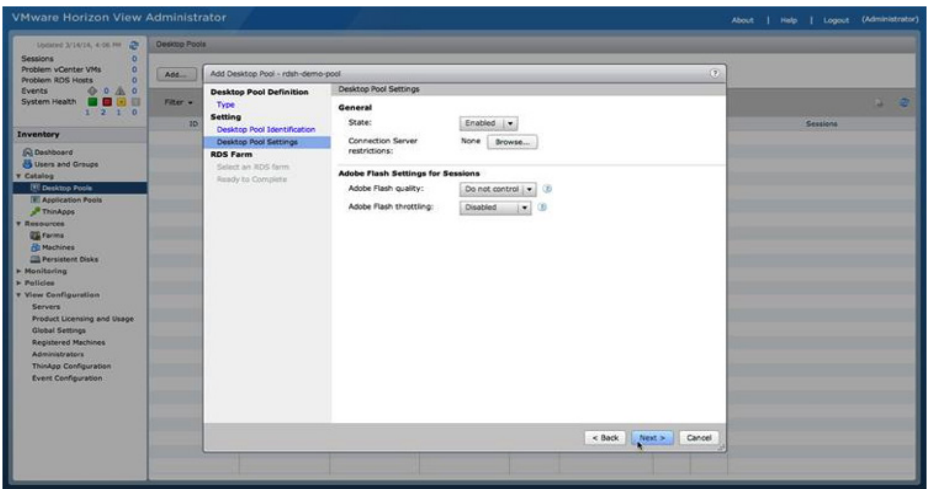
3. In the Add Desktop Pool window, select **RDS Desktop Pool**, and then click **Next**.



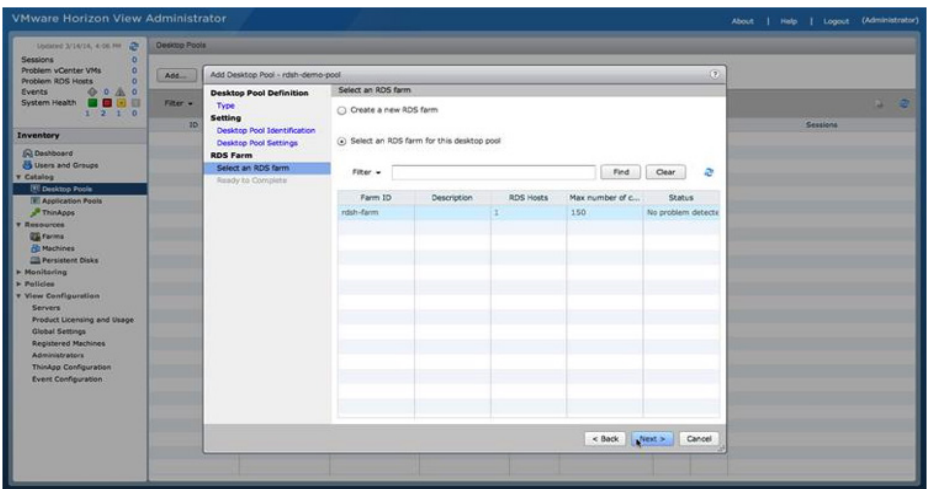
4. Give your desktop pool an ID and display name. The ID is a unique name used to identify the desktop pool. The display name is the name end users see when connecting to the desktop pool. Click **Next**.



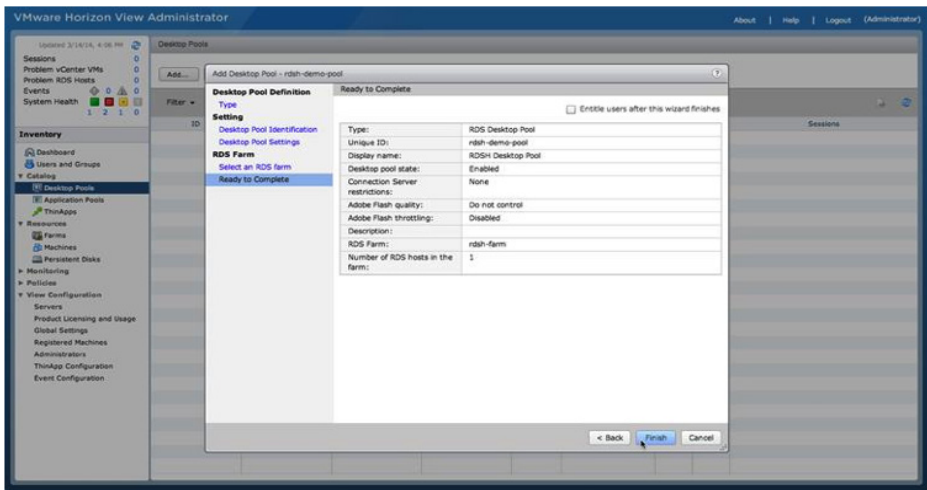
5. Adjust the desktop pool settings or keep the default settings, and then click **Next**.



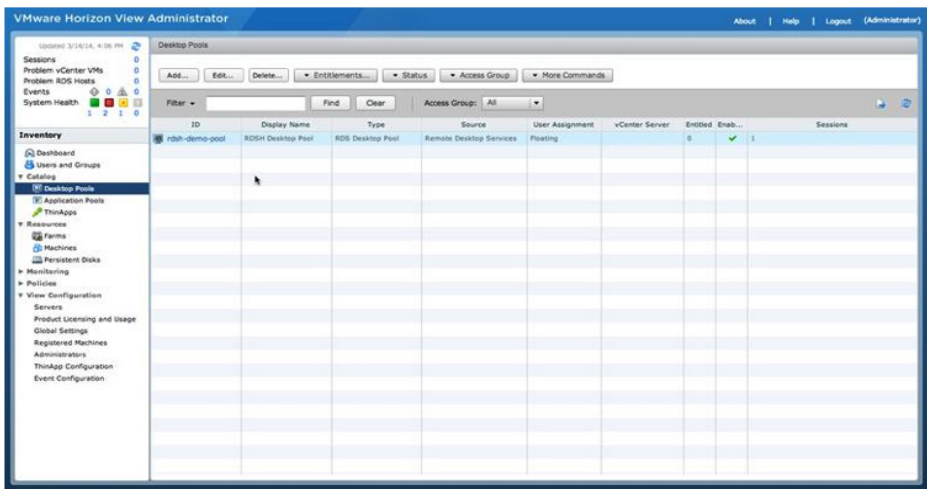
6. Select the RDS farm for the desktop pool and click **Next**.



7. Review the RDSH Desktop Pool settings and click **Finish**. Or to make changes, click **Back**.



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

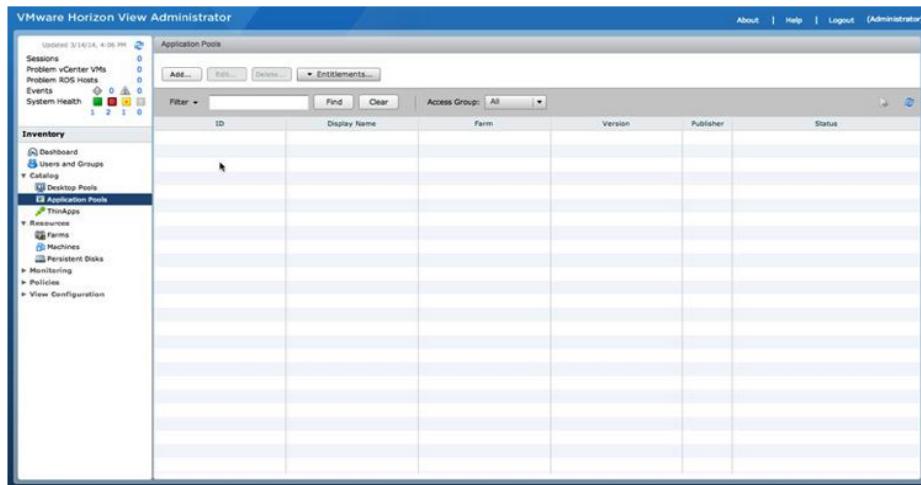


You have now deployed a RDSH desktop pool. In the next exercise, you deploy an RDS-based application pool.

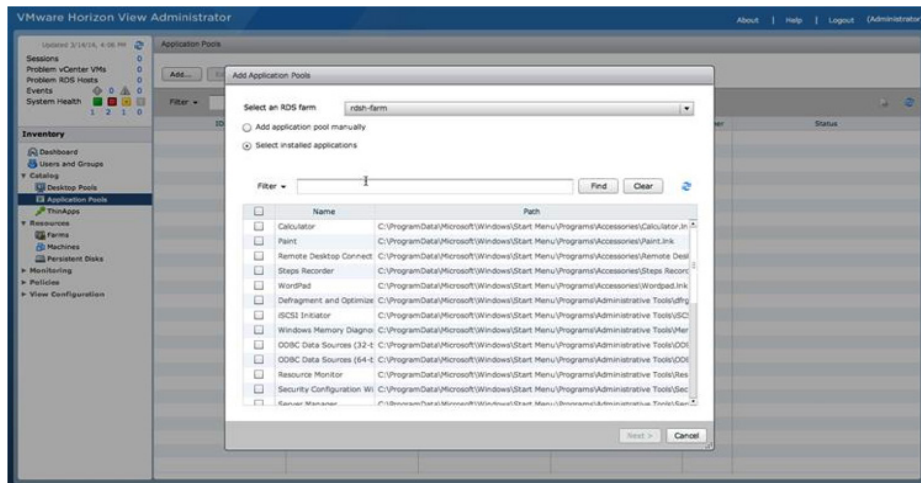
Deploy an Application Pool

An application pool lets you deliver a single application to many users. The application runs on a farm of RDS hosts.

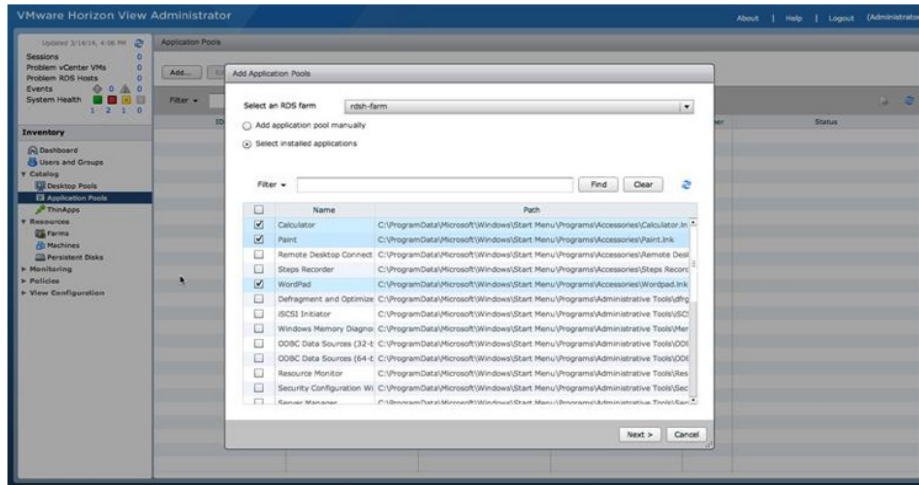
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools.
2. To create a new application pool, click **Add**.



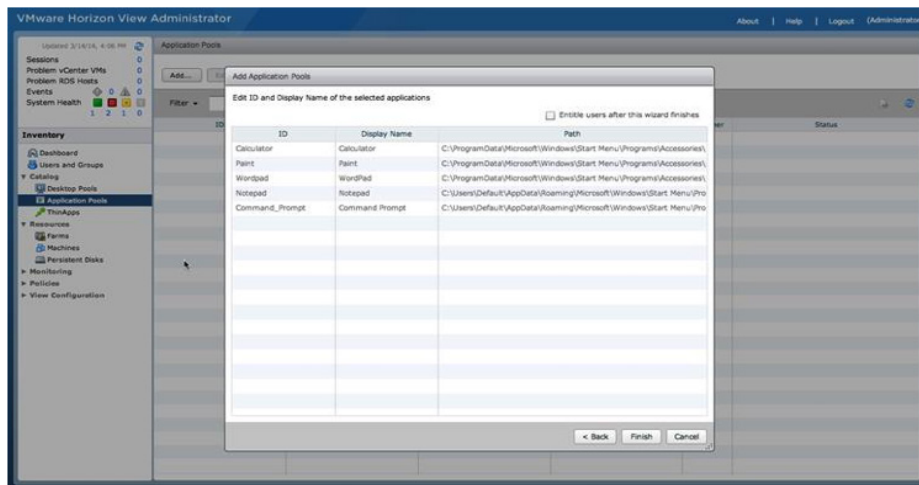
3. In the Add Application Pools wizard, you see a list of all the available applications that can be used to create an application pool.



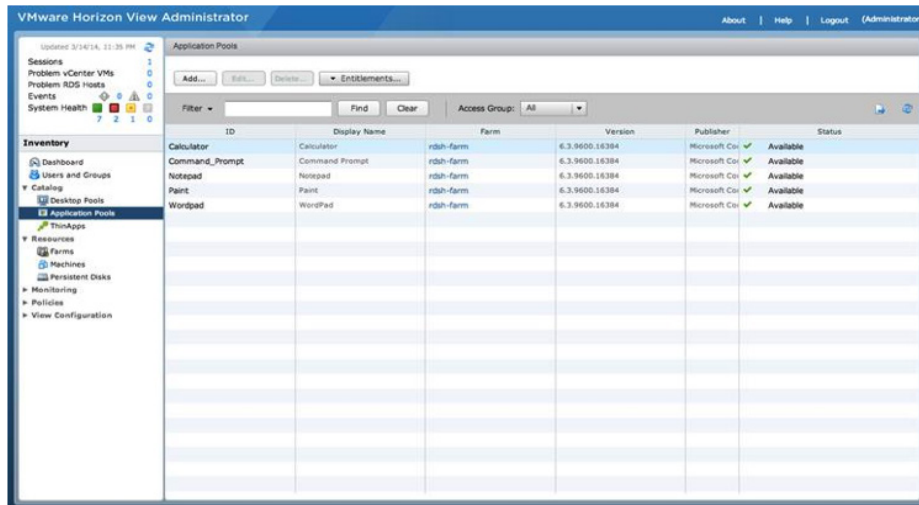
4. Select the applications you want created as application pools and click **Next**.



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

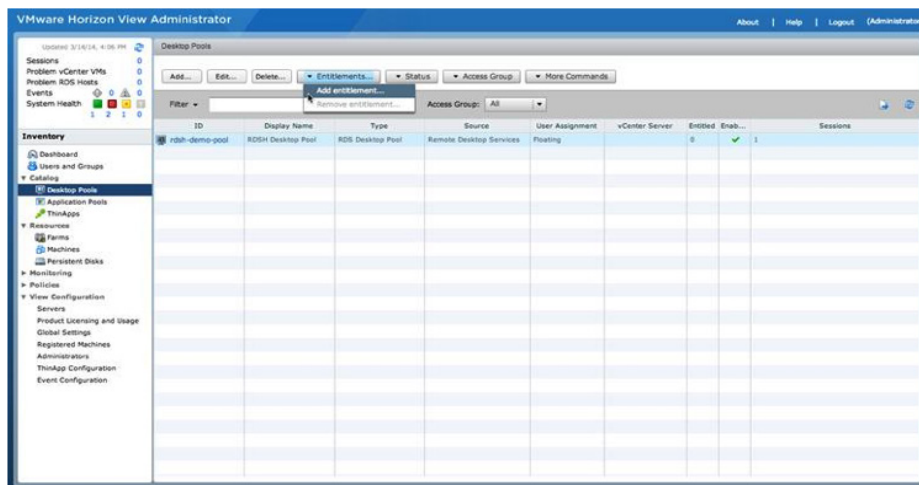
Now that you have deployed three different desktop pools, you are ready to entitle users to use them.

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

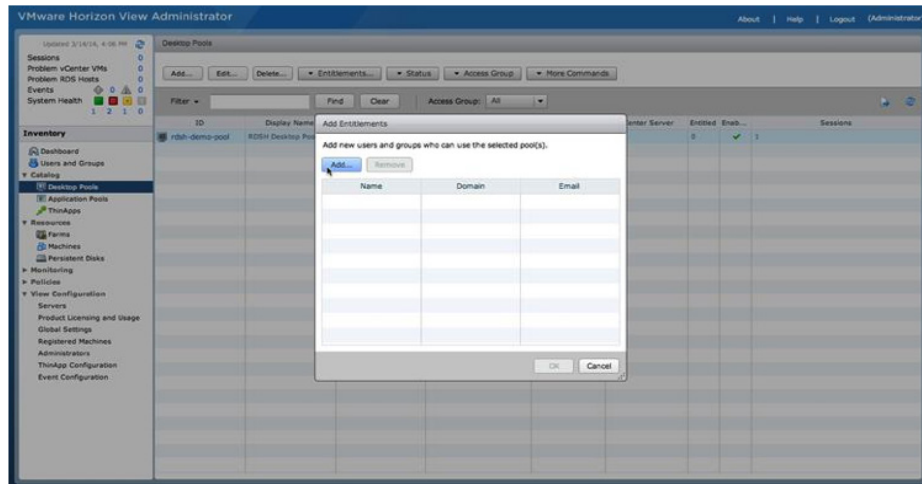
Entitle Users to a Desktop Pool

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

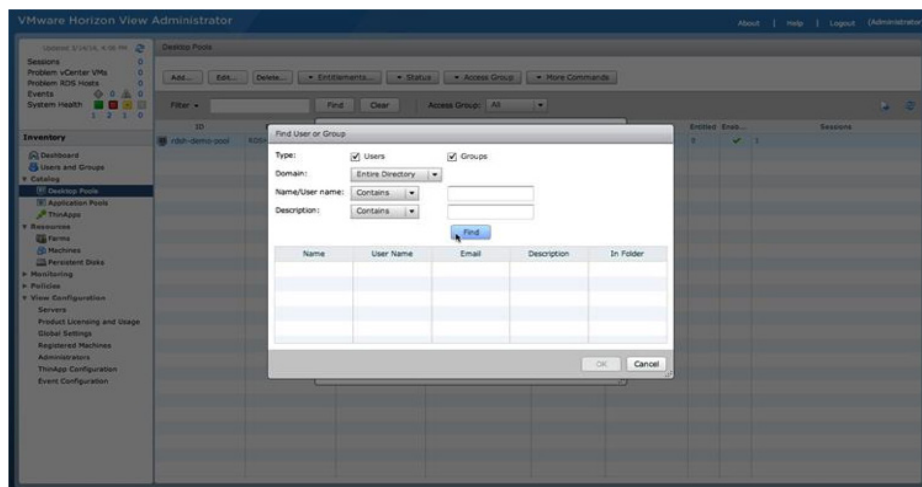
1. Log in to the View Administrator console, and navigate to **Catalog > Desktop Pools** to see a list of all your deployed desktop pools and click the desktop pool that you want to entitle.
2. Click the **Entitlements** tab and then click **Add Entitlement**.



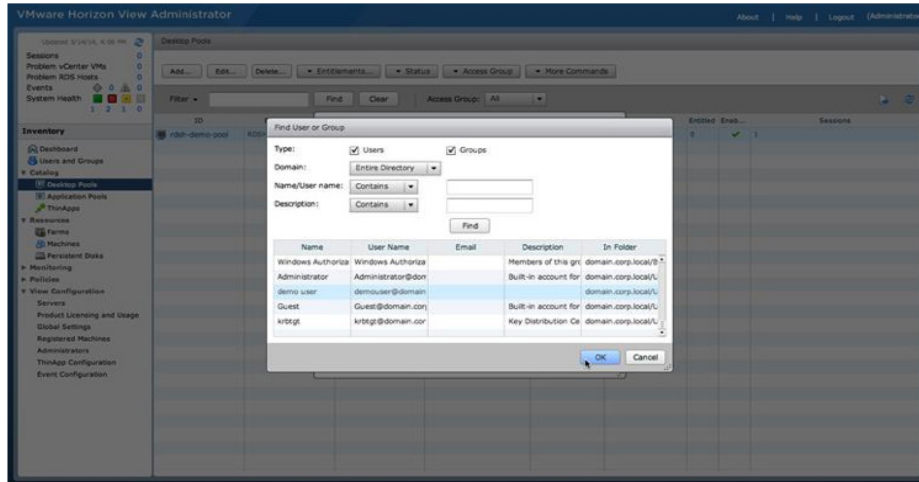
- The Add Entitlements dialog box lists the pool's entitled users and groups. Click **Add** to entitle new users or groups to the desktop pool.



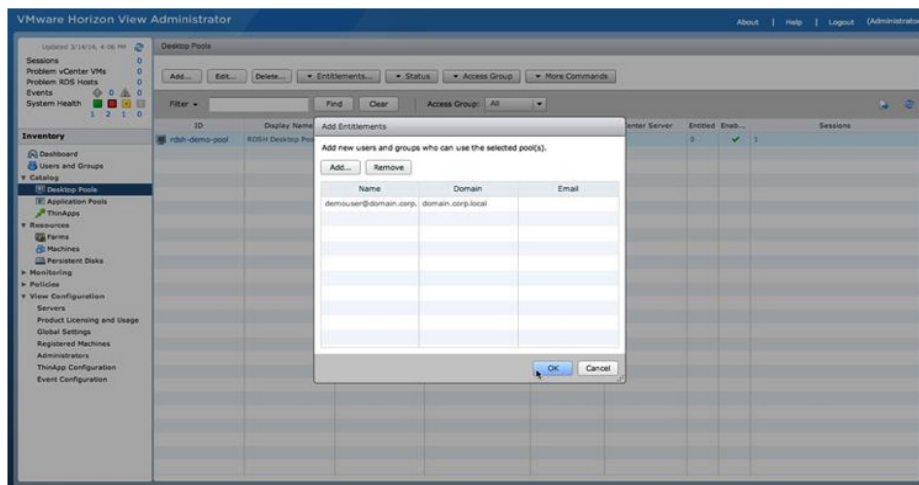
- In the Find User or Group dialog box, search your domain controller for users or groups to entitle to this desktop pool. You can narrow your query using the drop-down menus to add search terms and modifiers. Click **Find**.



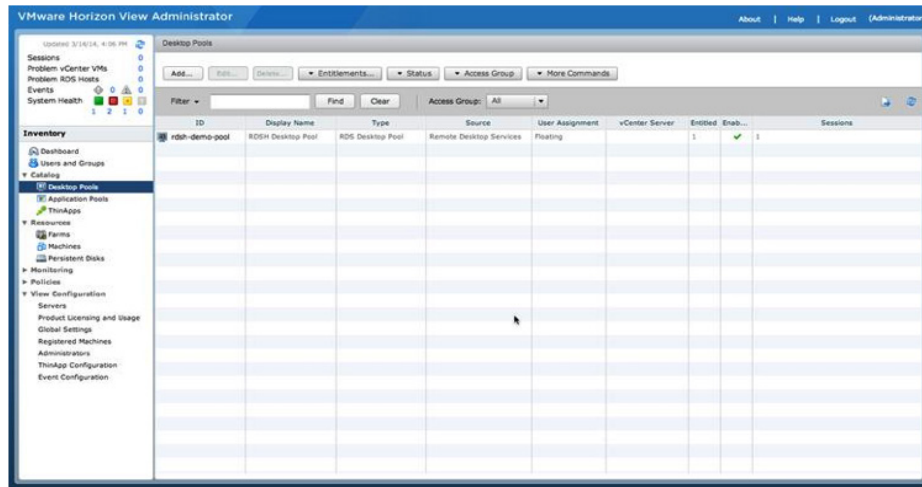
5. Scroll through the results to select all the users or groups to entitle, and then click **OK**.



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



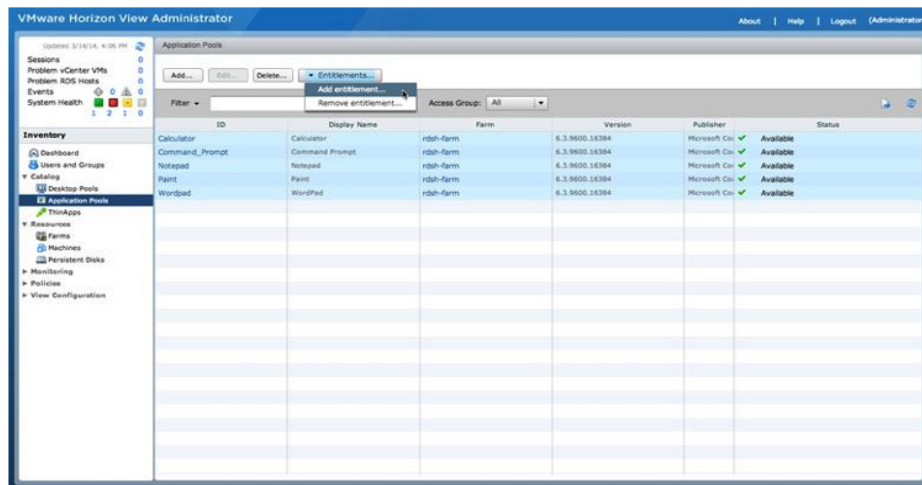
- You can verify the total number of entitlements for the pool in the Entitled column.



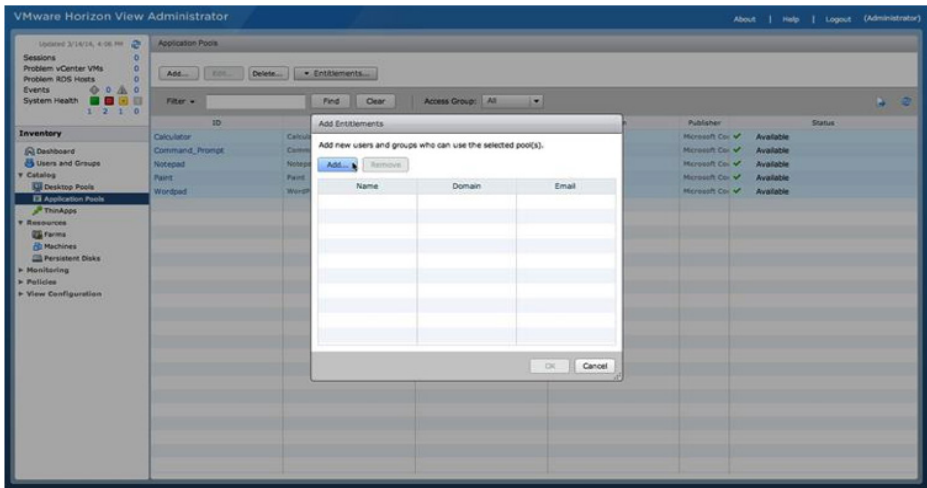
Repeat these steps to entitle other users or groups to the rest of your desktop pools or unentitle them. Proceed to the next exercise to entitle users to application pools.

Entitle Users to an Application Pool

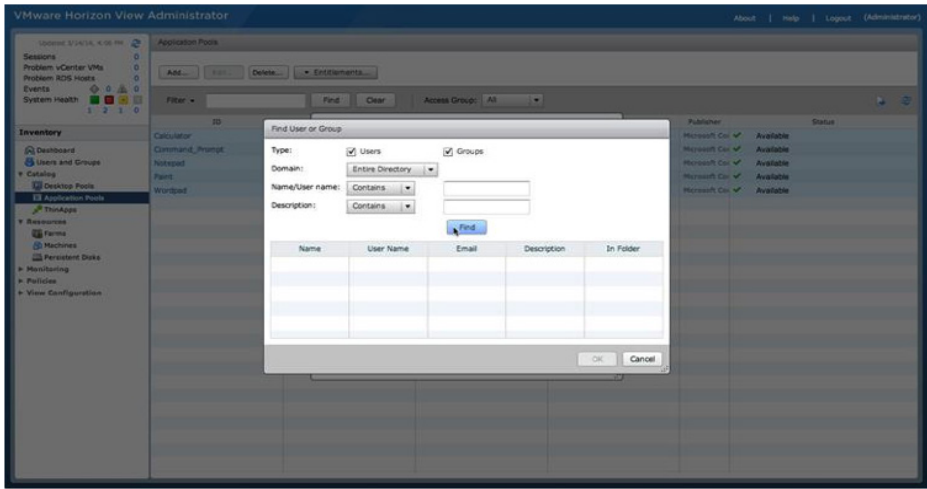
- Log in to the View Administrator console, and navigate to **Catalog > Application Pools** to see a list of all your application pools.
- Click the application pool or select multiple application pools to entitle.
- Click the **Entitlements** tab and then click **Add Entitlement**.



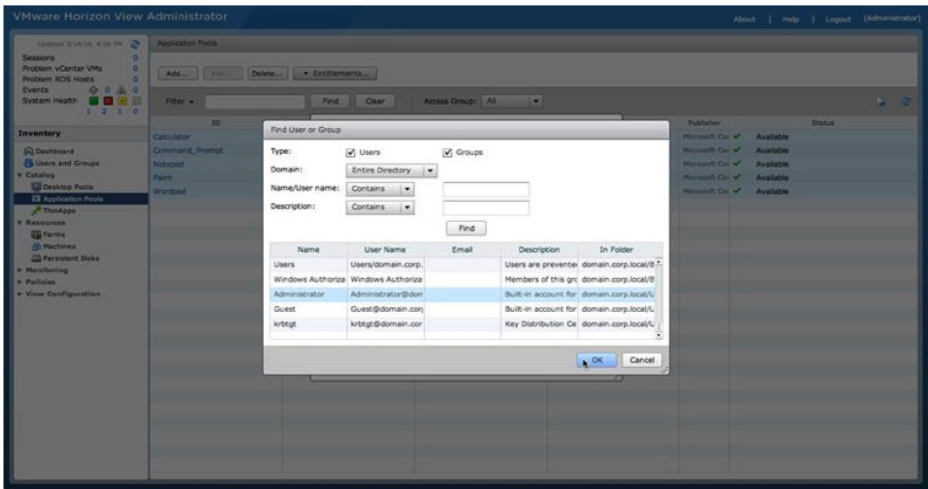
4. The Add Entitlements dialog box lists the pool's entitled users and groups. Click **Add** to entitle new users or groups to the application pool.



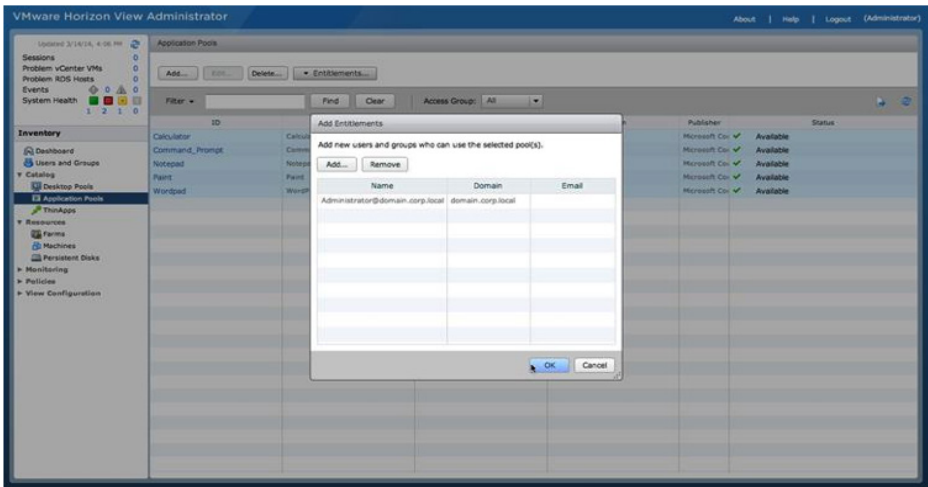
5. In the Find User or Group dialog box, search your domain controller for users or groups to entitle to this application pool. You can narrow your query using the drop-down menus to add search terms and modifiers. Click **Find**.



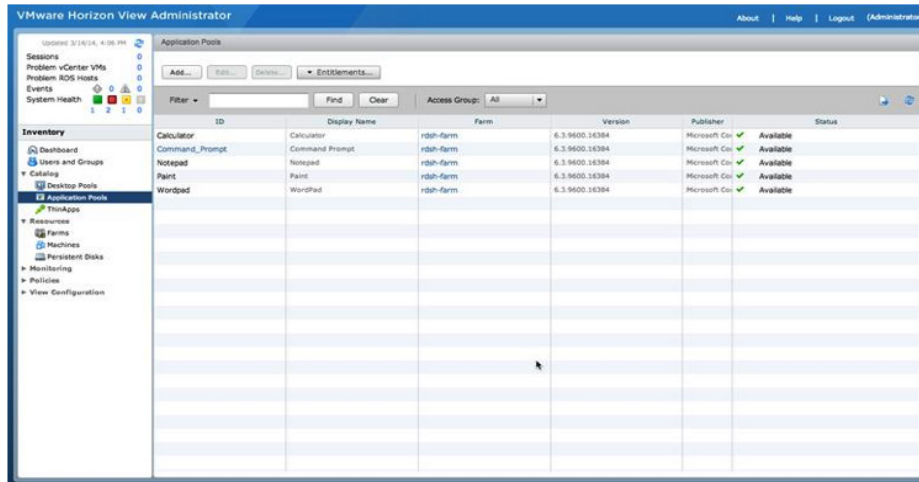
6. Scroll through the results to selected all the users or groups to entitle, and then click **OK**.



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



8. You are returned to the Application Pools window. You can repeat these steps to entitle additional users or group or unentitle them.



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 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.

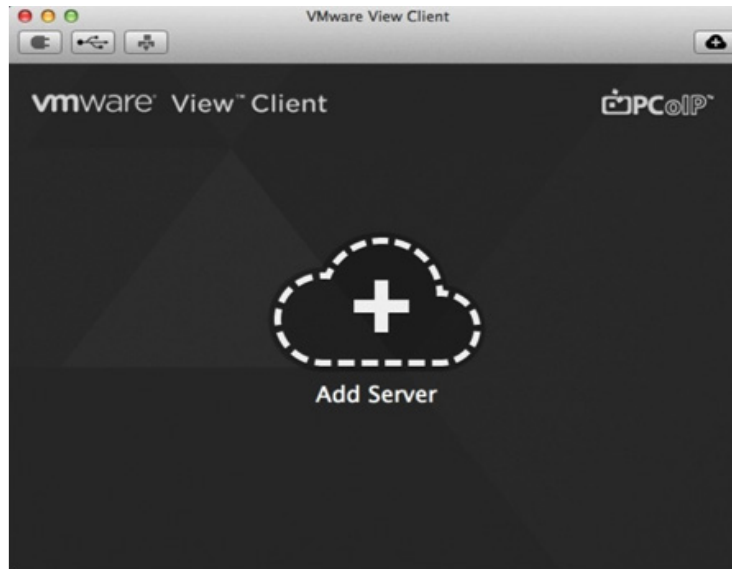
- [Connect to View Desktops Using Horizon Client](#)
- [Connect to View Desktops Using HTML Access](#)
- [Connect to View Desktops from a Mobile View Client](#)
- [Connect to an Application Using the Horizon Client](#)

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

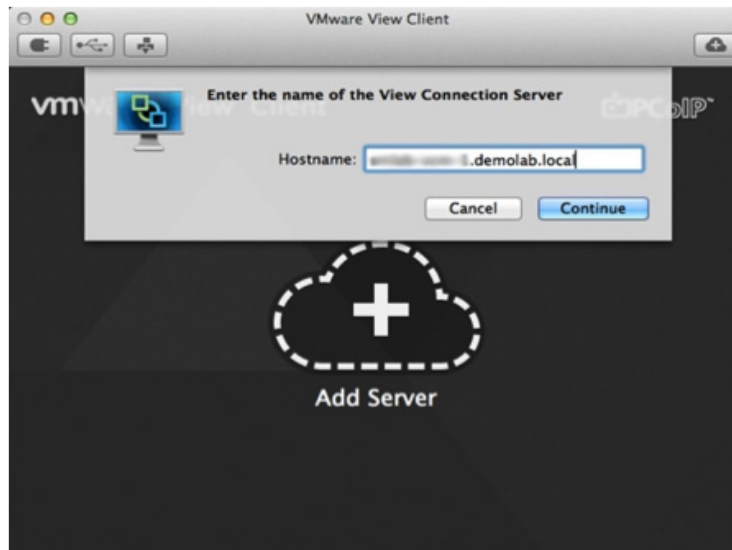
Connect to View Desktops Using Horizon Client

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

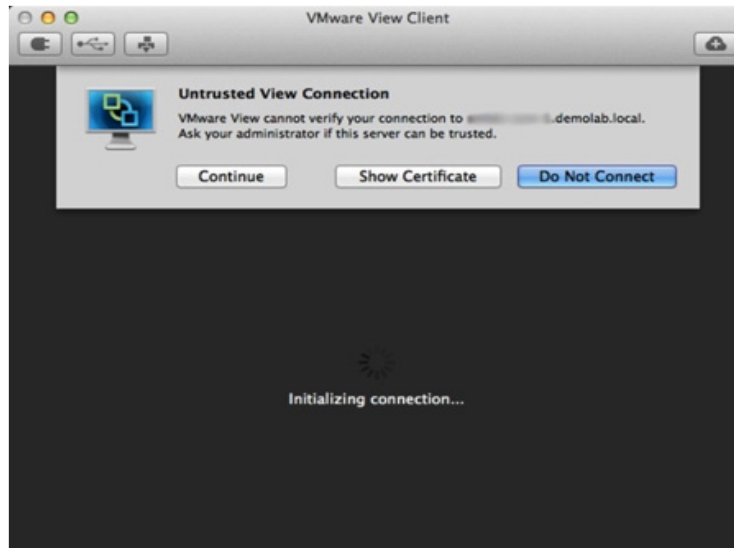
1. On your target client, install the Horizon Client.
2. On your target client, launch Horizon Client, and click **Add Server**.



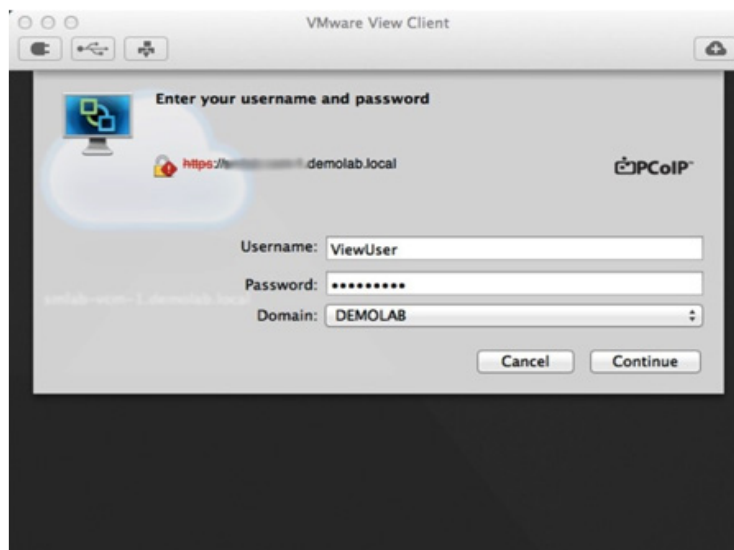
3. In the Hostname text box, type the fully qualified domain name of your View Connection Server, and click **Continue**.



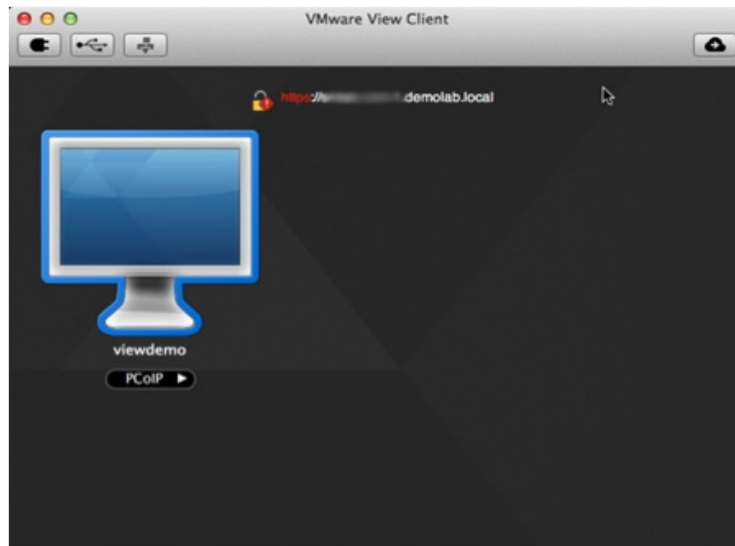
4. If you are using the default self-signed SSL certificate, an Untrusted View Connection warning appears.
 - a. To ensure the certificate is valid, click **Show Certificate**.
 - b. To proceed, click **Continue**.



5. Type your user credentials in the Username and Password text boxes, and then click **Continue**.
Note: You must be entitled to a desktop pool or specific desktop to access it.



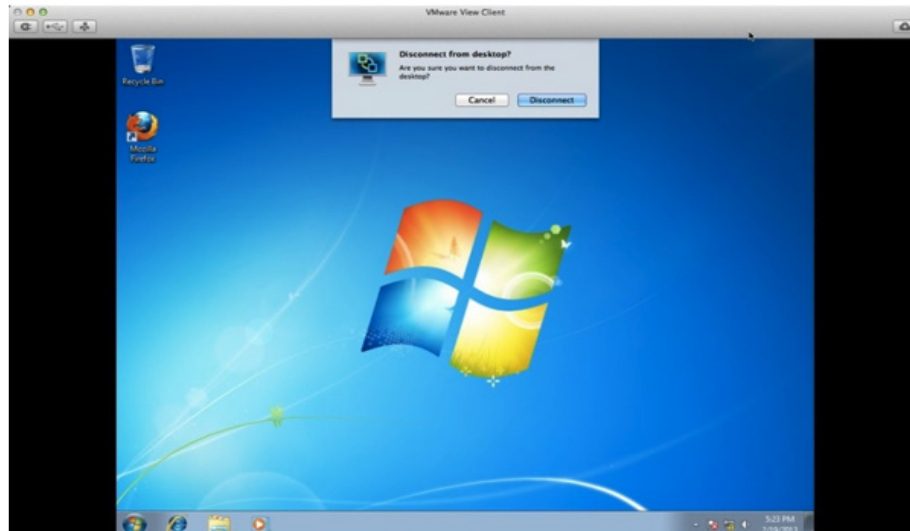
6. From the group of desktops available to your credentials, click the desktop to connect to.



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 then 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

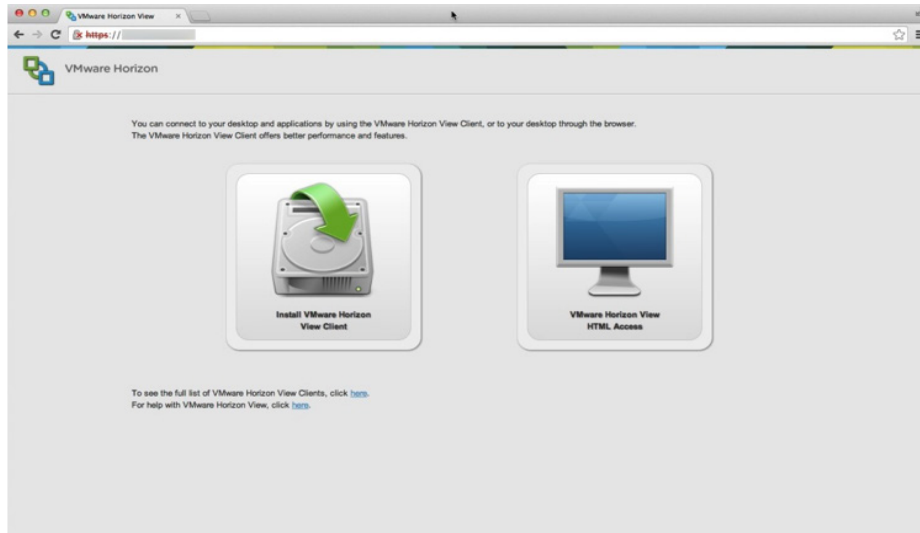
You can connect to a View desktop from an HTML5-enabled Web browser.

The supported Web browsers are:

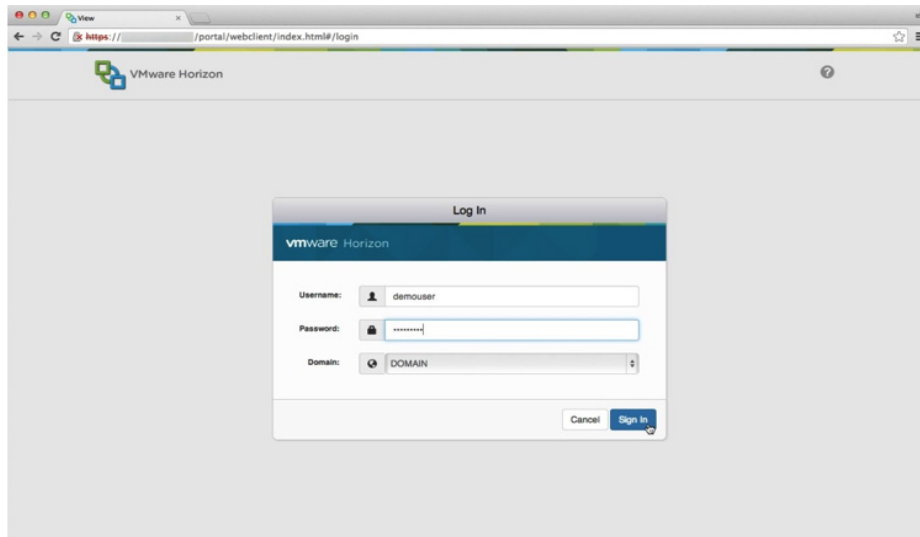
- Chrome 28 or later
- IE 9 or later
- Safari 6 or later
- Firefox 21 or later
- Mobile Safari, iOS 6 or later

The desktop you are connecting to via HTML must be in a pool with the HTML Access feature enabled, as discussed in [Deploy a Linked-Clone Desktop Pool](#).

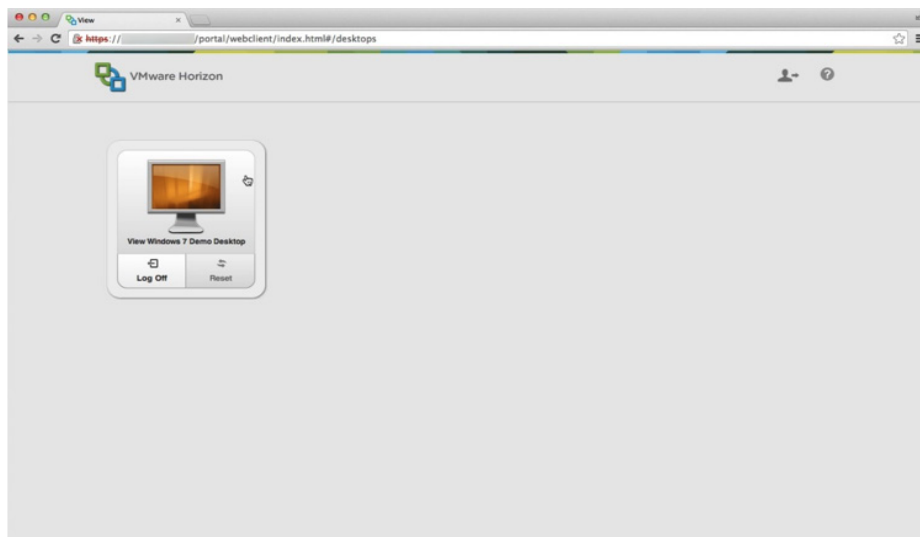
1. Open a supported Web browser and navigate to the address of your View Connection Server.
2. Click **VMware Horizon View HTML Access**.



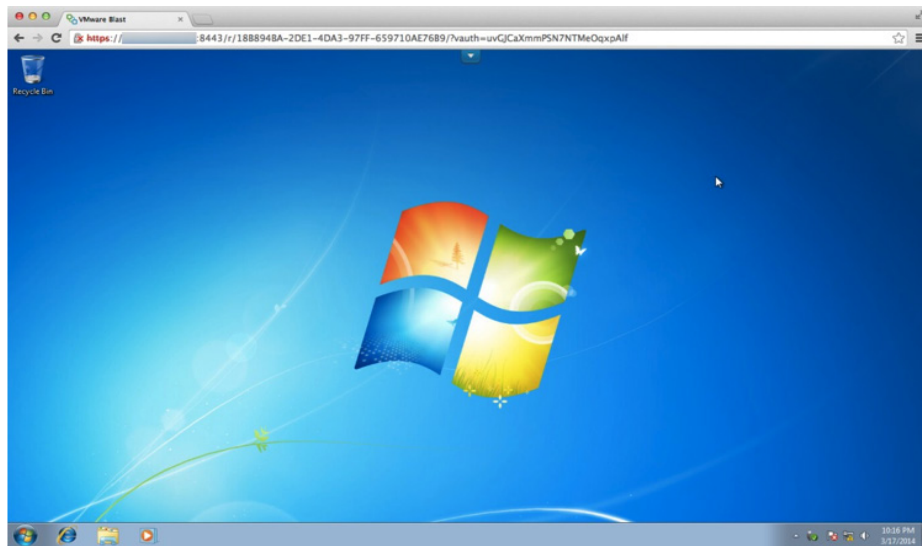
3. Enter your user credentials. You must be entitled to a desktop pool or specific desktop.



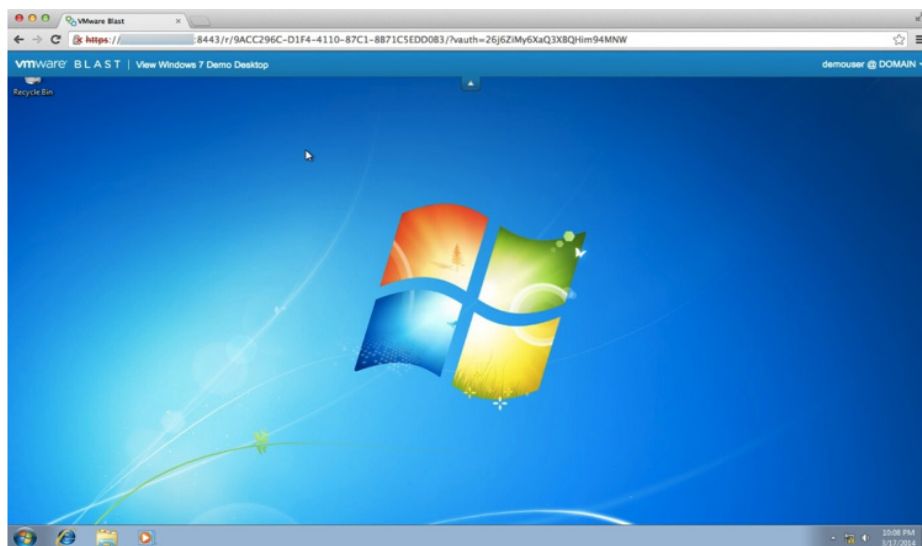
4. After the credentials are validated, the available desktops for the user are shown. Click the desktop that you want to connect to.



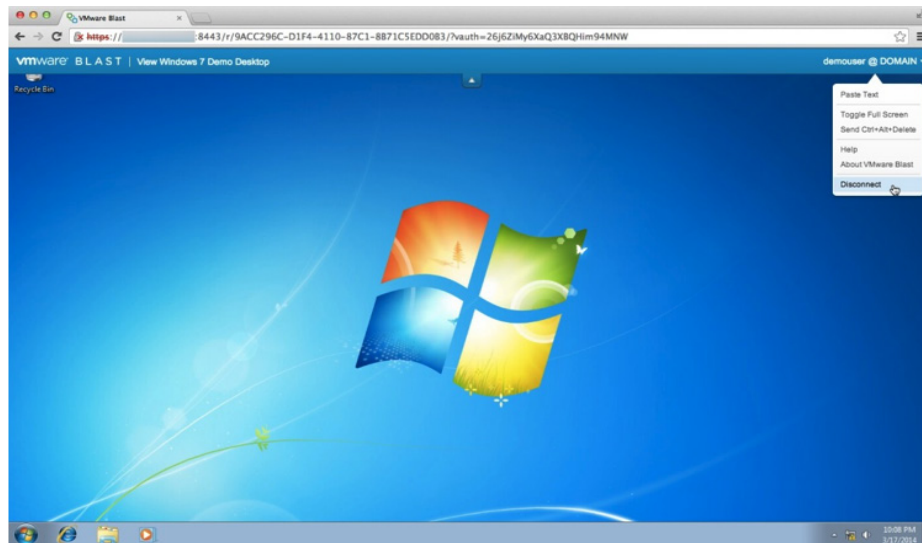
5. You are connected to your View desktop using HTML Access.



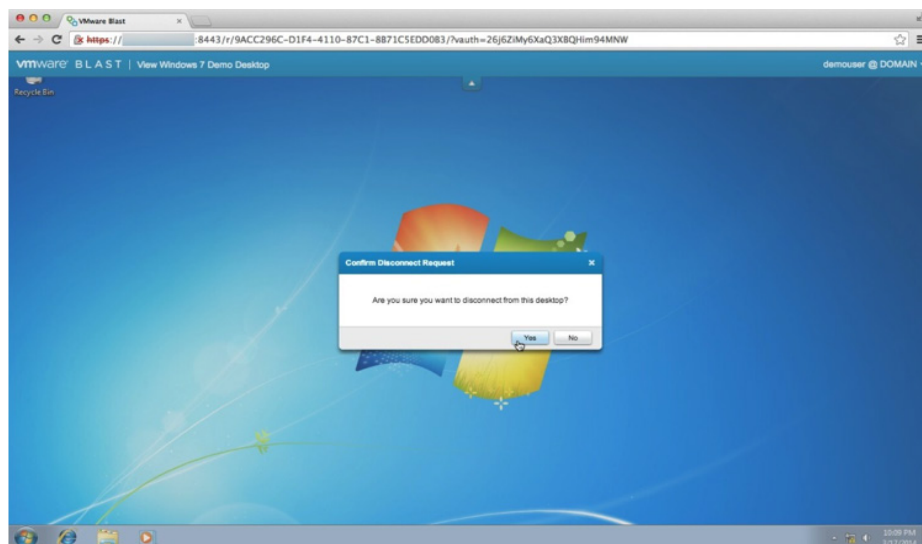
6. You can navigate and use your desktop as you normally would. The View HTML Access menu hides at the top of the Web browser. Click the down arrow to make it visible.



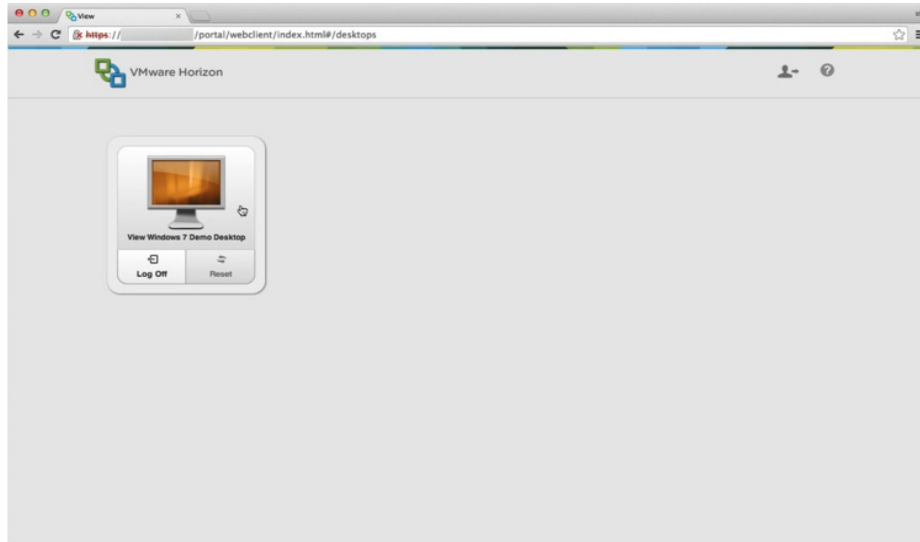
7. To disconnect from your session, click your username at the top right of the HTML Access menu bar. From the drop-down menu, select **Disconnect**.



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



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

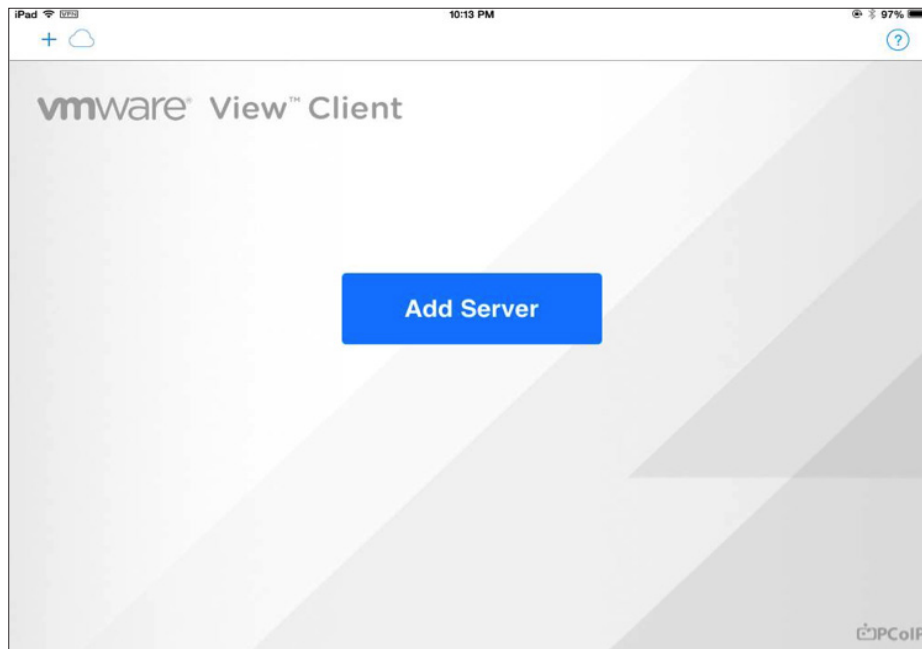


You have now connected to a View desktop using HTML Access. Proceed to the next exercise to connect to desktops from a mobile client.

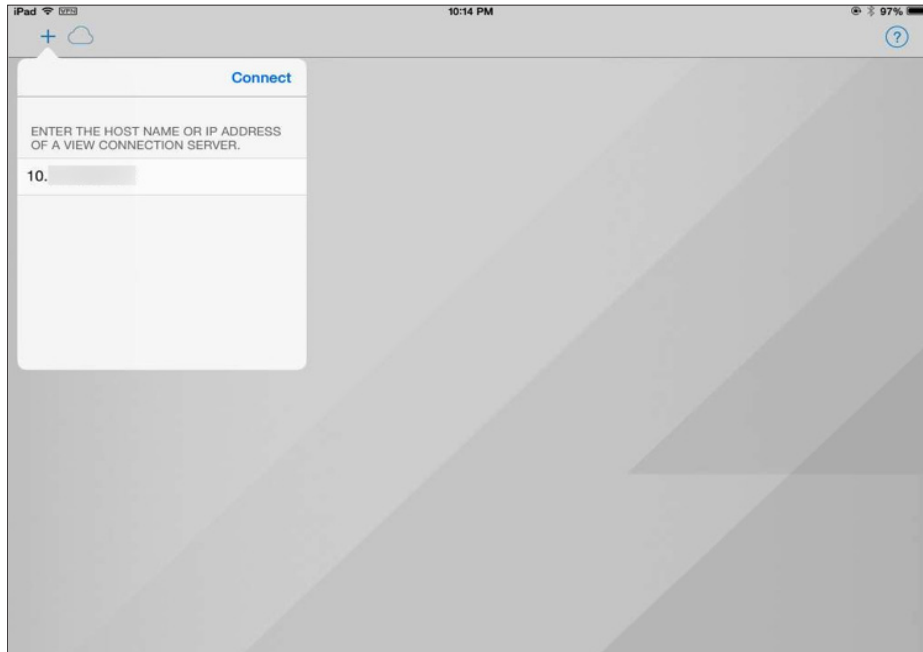
Connect to View Desktops from a Mobile View Client

This exercise shows you how you can connect to a View Desktop from the iOS View 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.

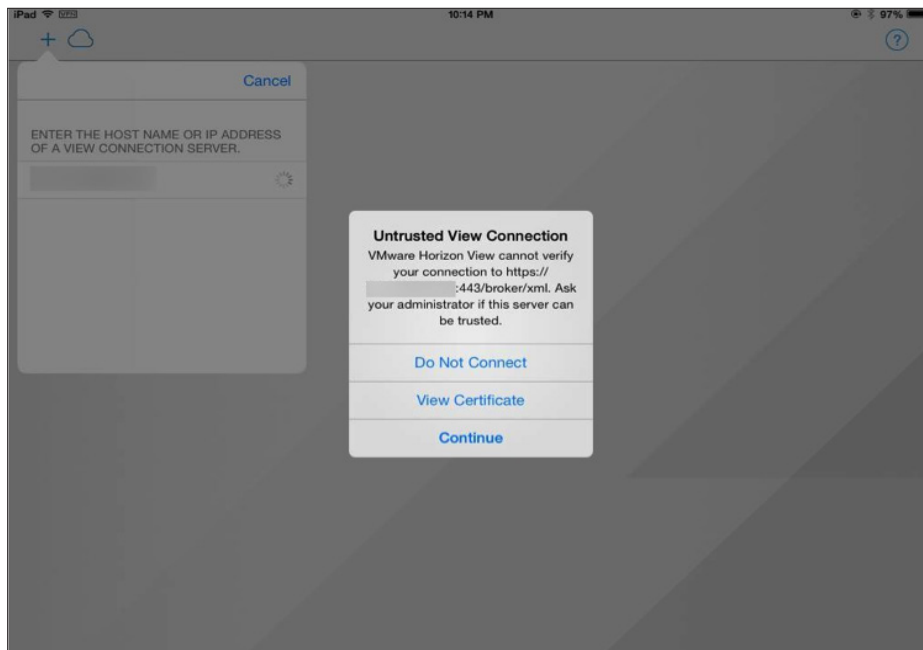
1. Launch View Client from your iOS mobile device. Tap **+** in the top left menu bar or the **Add Server** button.



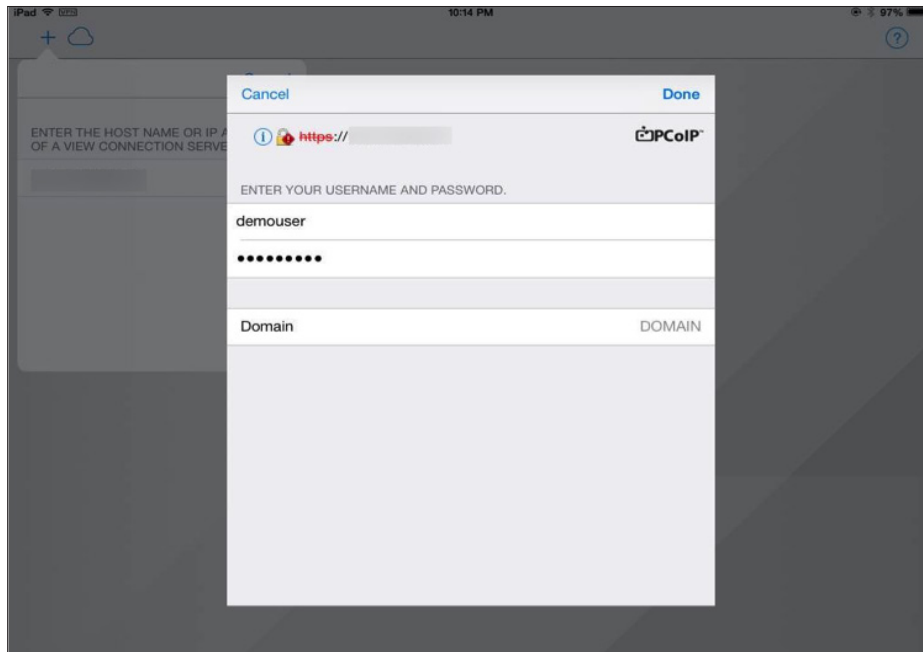
2. Enter the host name or IP address of View Connection Server and tap **Connect**.



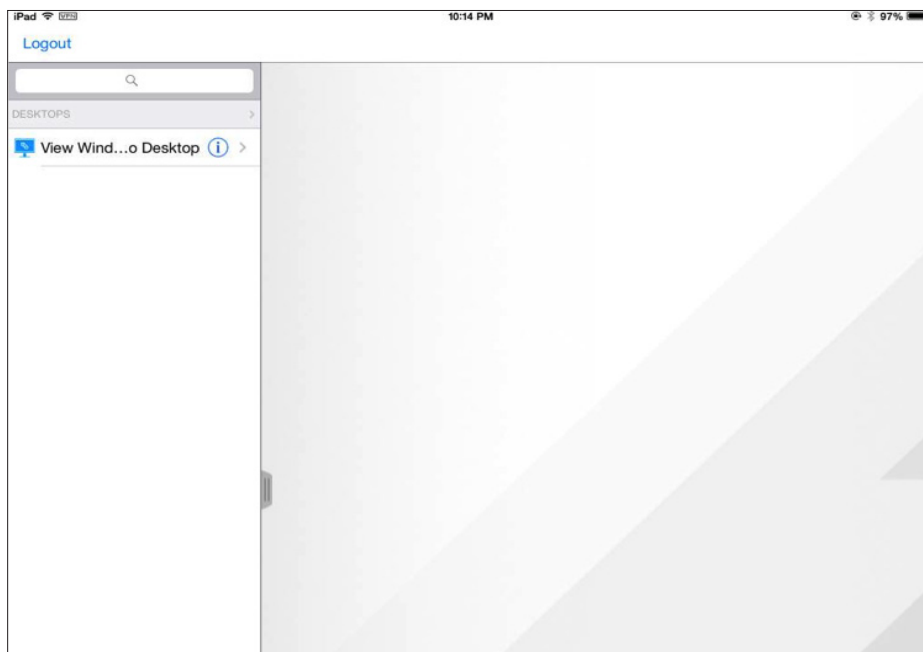
3. If you are using the default self-signed SSL certificate, an **Untrusted View Connection** warning appears. You can modify the Horizon Client security settings in the Properties or Preferences menu. Tap **View Certificate** to ensure that the certificate is valid. To accept the certificate, tap **Continue**.



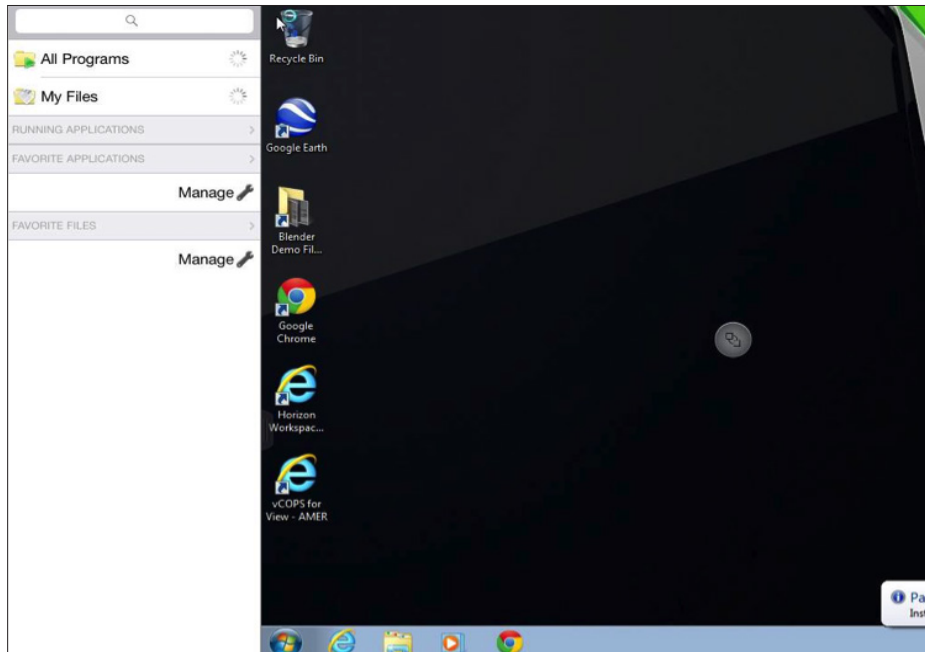
4. Enter your user credentials. You must be entitled to a desktop pool.



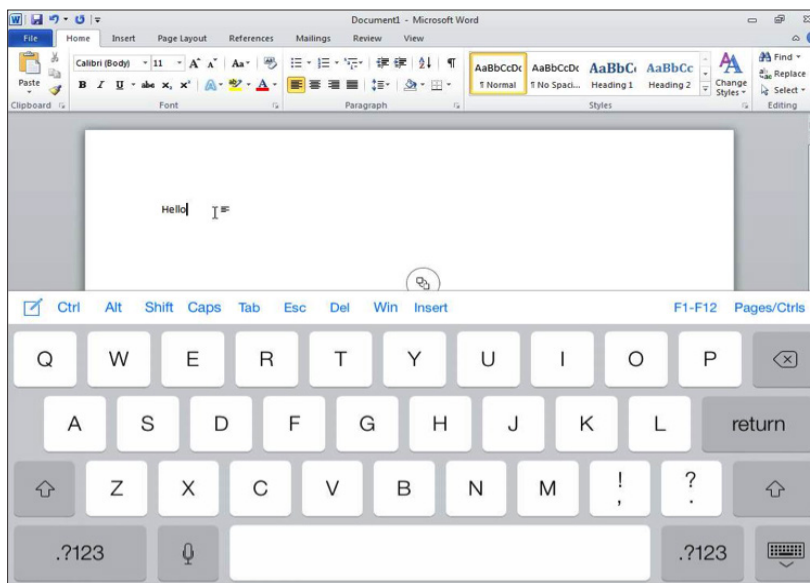
5. After your credentials are validated, your available desktops are listed. Tap the desktop that you want to connect to.



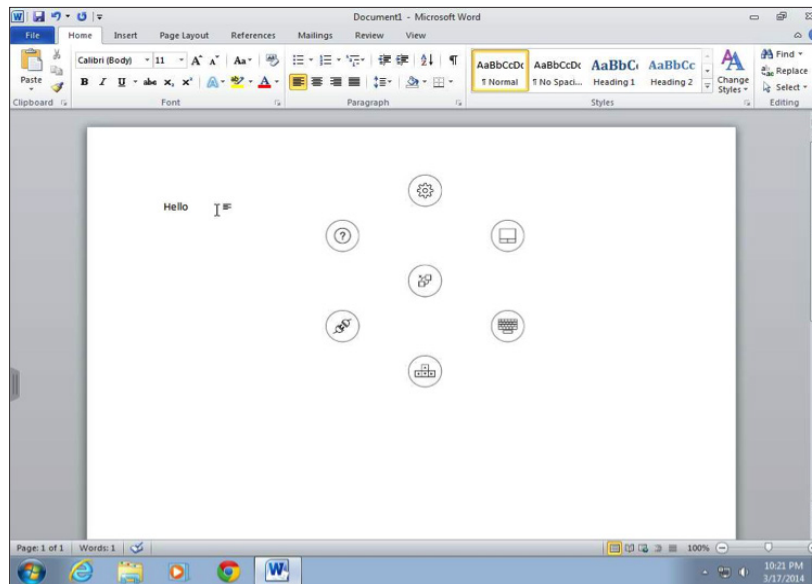
6. You have connected to your View desktop from the iOS Horizon Client. By default, at first login, the Unity Touch menu appears on the left side. Unity Touch allows you to easily interact with your View desktop. The menu provides the functionality of a typical Windows Start menu but without having to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



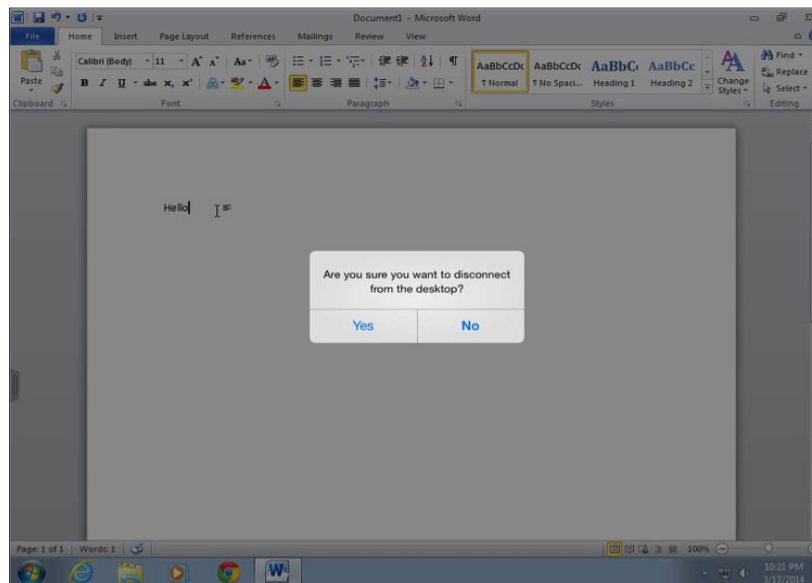
In the example shown, we have launched a word processing application. Interacting with the application triggered the keyboard overlay.



- On the iOS Horizon Client, menu buttons that allow you to perform various actions are placed on your screen, such as disconnect from the session or bring up the keyboard. Tap the **Disconnect** button to end the session.



- A dialog box appears for you to confirm your session disconnect. Tap **Yes**.



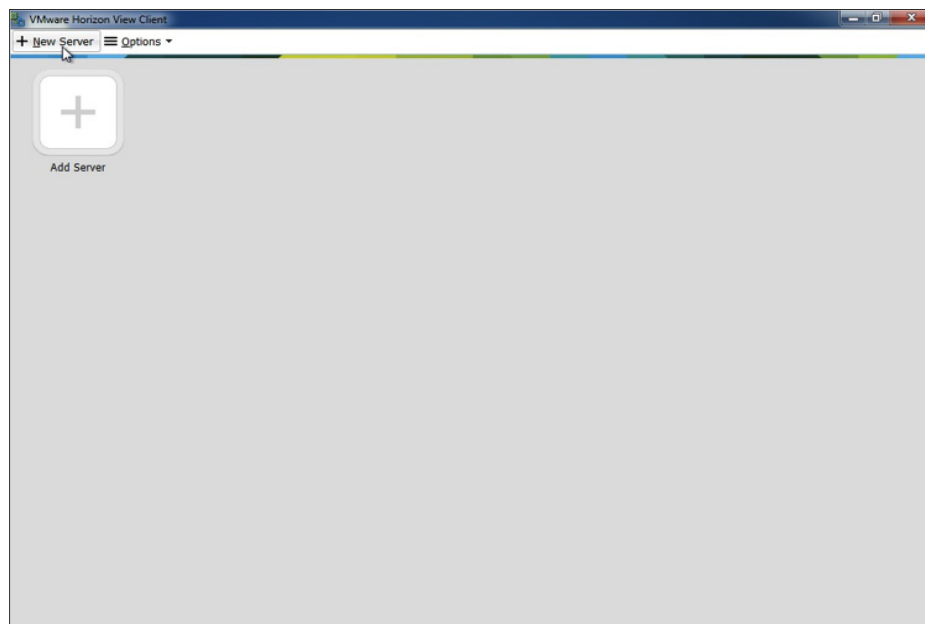
9. You are disconnected from your View desktop session and returned to the list of available View desktops. You can close the application or reconnect to your View desktop.



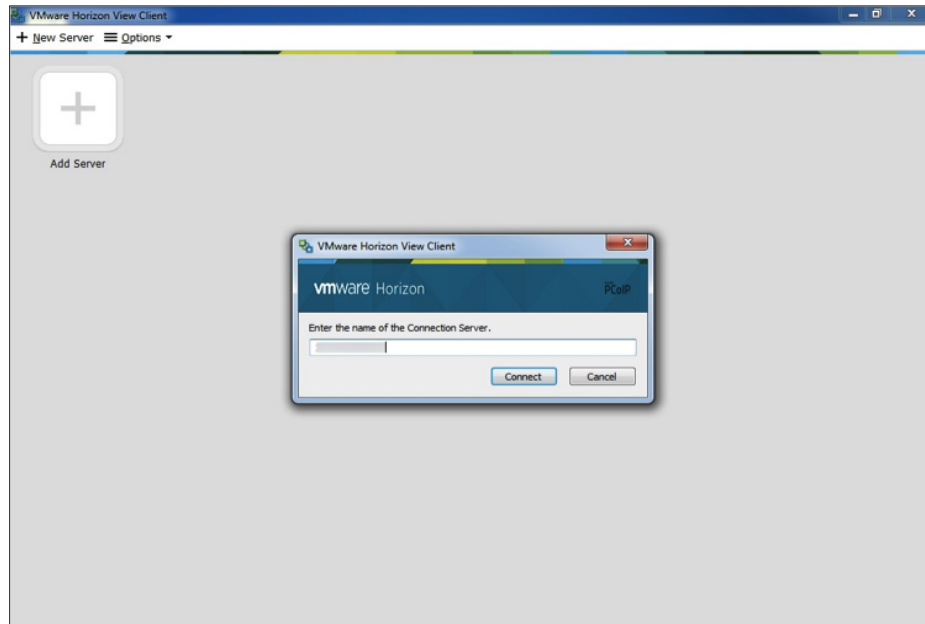
Connect to an Application Using the Horizon Client

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

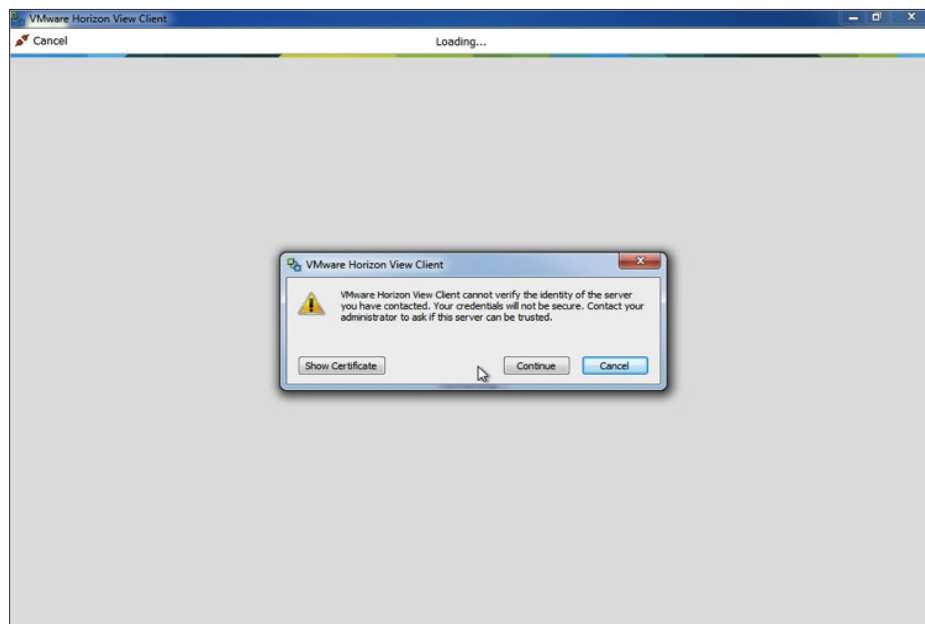
1. Launch Horizon Client. Tap **+ New Server** in the top left menu bar.



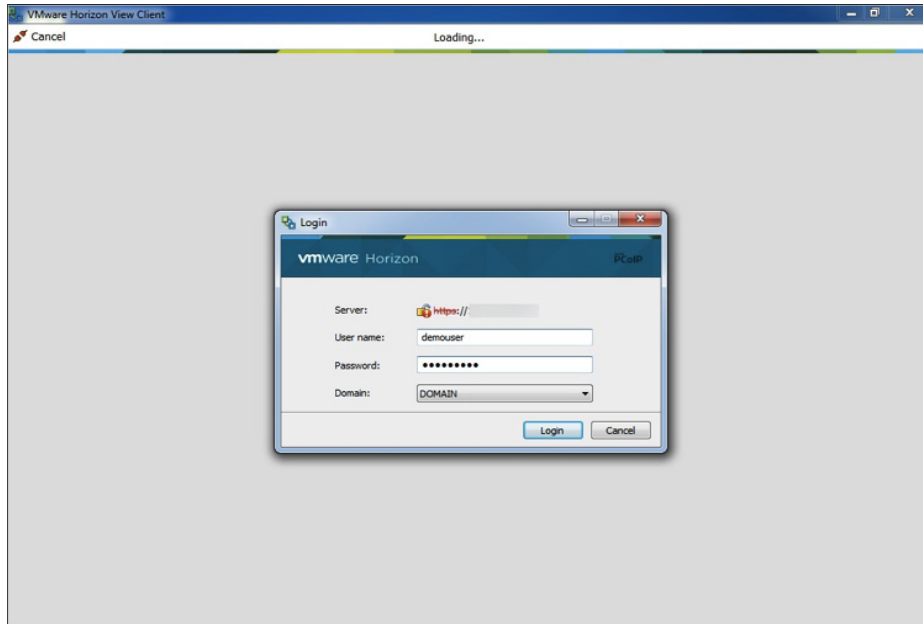
2. Enter the host name or IP address of View Connection Server and tap **Connect**.



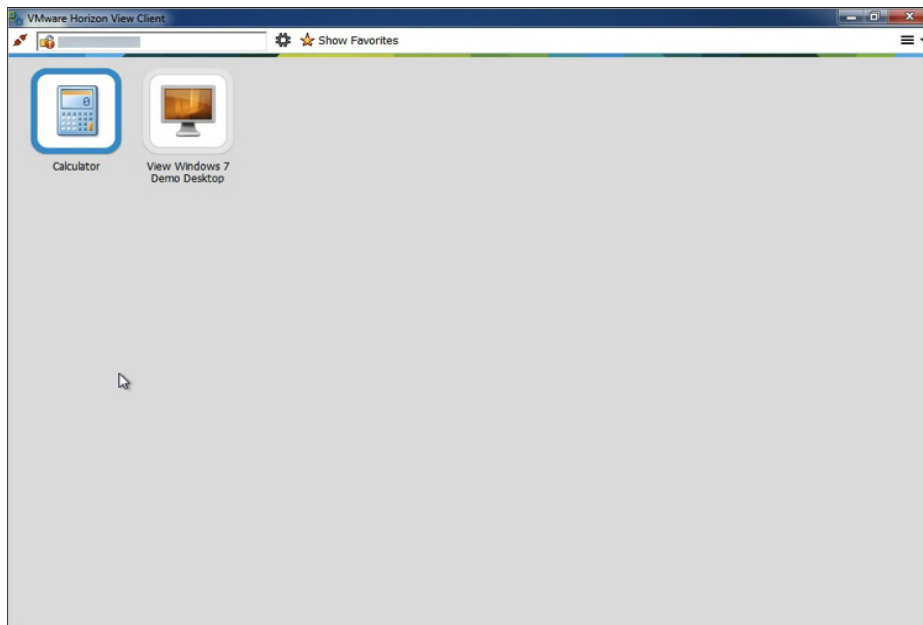
3. If you are using the default self-signed SSL certificate, an Untrusted View Connection warning appears. You can modify View Client security settings in the Properties or Preferences menu. Tap **View Certificate** to ensure that the certificate is valid. To accept the certificate, tap **Continue**.



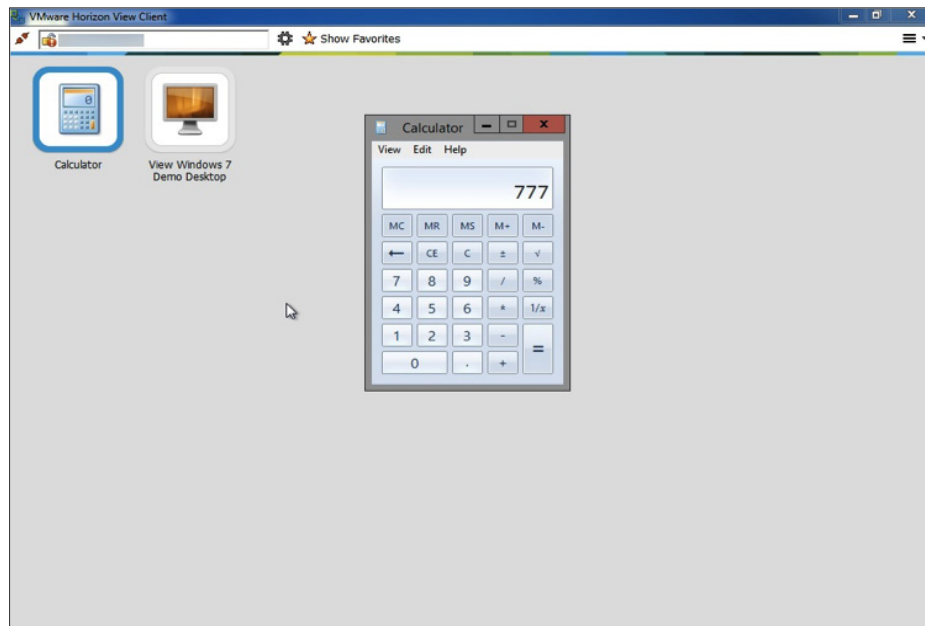
4. Enter your user credentials and tap **Login**. You must be entitled to an application pool to launch an application.



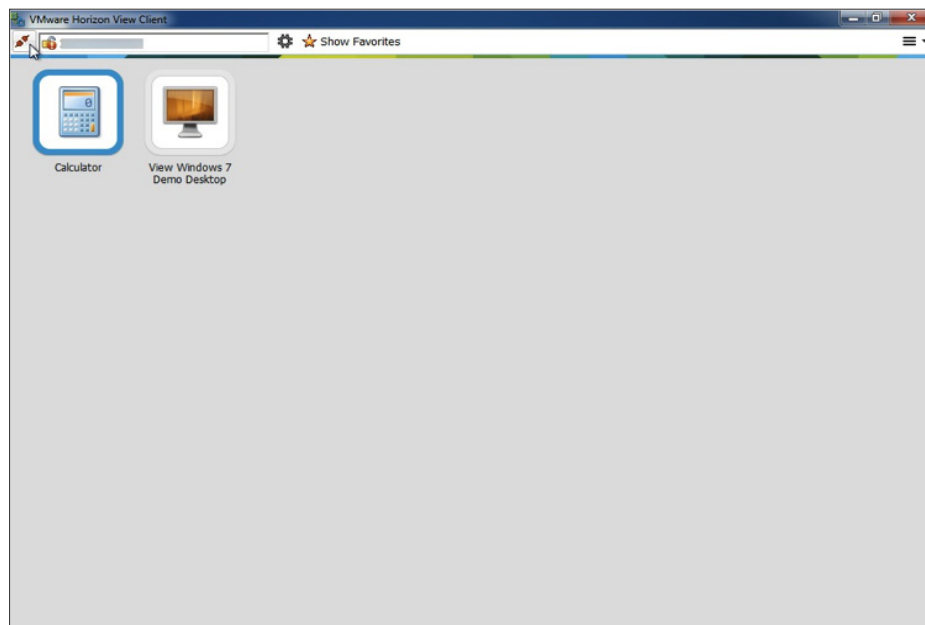
5. After your credentials are validated, your available applications and desktops appear. Tap the application that you want to connect to. For this step, tap the **Calculator** icon.



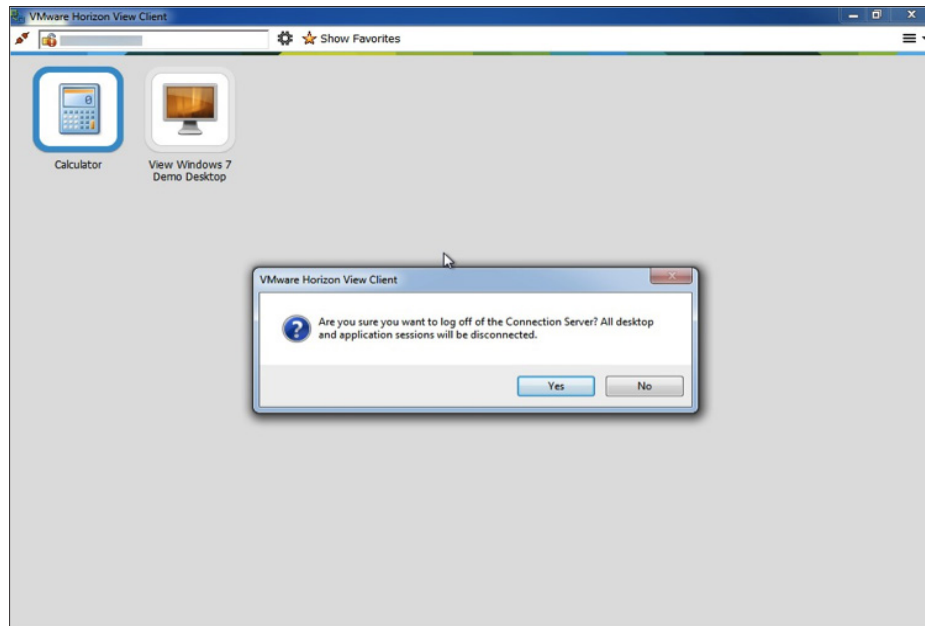
6. Use the application as you normally would. Tap **X** in the menu bar to close the application.



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



8. Tap the **Disconnect** button to disconnect from Horizon Client. Tap **Yes** to confirm. You can now close the application.



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 [View 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 with View Documentation](#)
- [VMware Horizon Product](#)
- [VMware Horizon Clients Download Center](#)
- [Storage Considerations for Horizon View 5.2](#)
- [Graphics Acceleration in VMware Horizon View Virtual Desktops](#)
- [View Configuration Tool: automated installation tool for View](#)
- [vCloud Automation Center](#)
- [vCenter Orchestrator](#)
- [vCenter 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 Author

This version of the reviewer's guide was written and updated by

- Marilyn Basanta, Solutions Architect in End-User Computing, Solutions Management at VMware

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing team at twitter.com/vmwarehorizon.

