Setting Up Published Desktops and Applications in Horizon 7

VMware Horizon 7 7.1

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Setting Up Published Desktops and Applications in Horizon 7

1

*Setting Up Published Desktops and Applications in Horizon 7*describes how to create, and deploy pools of desktops and applications that run on Microsoft Remote Desktop Services (RDS) hosts. It includes information about configuring policies, entitling users and groups, and configuring remote application features.

Intended Audience

This information is intended for anyone who wants to create and provision desktop and application pools. The information is written for Windows system administrators who are familiar with virtual machine technology and data center operations.

Introduction to Published Desktops and Applications 2

With Horizon 7, you can create published desktops associated with a farm, which is a group of Windows Remote Desktop Services (RDS) hosts. You can also deliver a published application to many users by creating application pools. The published applications in application pools run on a farm of RDS hosts.

This chapter includes the following topics:

Farms, RDS Hosts, and Published Desktops and Applications

You can use Microsoft Remote Desktop Services (RDS) to provide users with desktop sessions on RDS hosts and deliver applications to many users.

RDS Host

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. These servers host applications that users can access remotely. To access RDS applications, Horizon Client 3.0 or later is required.

Farms

Farms are collections of RDS hosts and facilitate the management of those hosts. Farms can have a variable number of RDS hosts and provide a common set of published applications or RDS published desktops to users. When you create an RDS application pool, you must specify a farm. The RDS hosts in the farm provide application sessions to users. A farm can contain up to 200 RDS host servers.

Published Desktops

Published desktops are RDS desktop pools, which provide users with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously.

Published Applications

Published applications are application pools that run on a farm of RDS hosts. Published applications let you deliver seamless applications to many users.

Advantages of RDS Desktop Pools

Horizon 7 offers the ability to create RDS desktop pools as its basis of centralized management.

You can create an RDS desktop pool from a physical system such as an RDS host. Use RDS desktop pools to provide multiple users with desktop sessions on an RDS host.

Advantages of Application Pools

With application pools, you give users access to applications that run on servers in a data center instead of on their personal computers or devices.

Application pools offer several important benefits:

- Accessibility

  Users can access applications from anywhere on the network. You can also configure secure network access.

- Device independence

  With application pools, you can support a range of client devices, such as smart phones, tablets, laptops, thin clients, and personal computers. The client devices can run various operating systems, such as Windows, iOS, Mac OS, or Android.

- Access control

  You can easily and quickly grant or remove access to applications for one user or a group of users.

- Accelerated deployment

  With application pools, deploying applications can be accelerated because you only deploy applications on servers in a data center and each server can support multiple users.

- Manageability

  Managing software that is deployed on client computers and devices typically requires significant resources. Management tasks include deployment, configuration, maintenance, support, and upgrades. With application pools, you can simplify software management in an enterprise because the software runs on servers in a data center, which requires fewer installed copies.

- Security and regulatory compliance

  With application pools, you can improve security because applications and their associated data are centrally located in a data center. Centralized data can address security concerns and regulatory compliance issues.

- Reduced cost

  Depending on software license agreements, hosting applications in a data center can be more cost-effective. Other factors, including accelerated deployment and improved manageability, can also reduce the cost of software in an enterprise.

Setting Up Remote Desktop Services Hosts

3

Microsoft Remote Desktop Services (RDS) hosts provide desktop sessions and applications that users can access from client devices. If you plan to create RDS desktop pools or application pools, you must first set up RDS hosts.

This chapter includes the following topics:

Remote Desktop Services Hosts

An RDS host is a server computer that hosts applications and desktop sessions for remote access. An RDS host can be a virtual machine or a physical server.

An RDS host has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. Remote Desktop Services was previously known as Terminal Services. The Remote Desktop Session Host service allows a server to host applications and remote desktop sessions. With Horizon Agent installed on an RDS host, users can connect to applications and desktop sessions by using the display protocol PCoIP or Blast Extreme. Both protocols provide an optimized user experience for the delivery of remote content, including images, audio and video.

The performance of an RDS host depends on many factors. For information on how to tune the performance of different versions of Windows Server, see http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx.

Horizon 7 supports at most one desktop session and one application session per user on an RDS host.

When users submit print jobs concurrently from RDS desktops or applications that are hosted on the same RDS host, the ThinPrint server on the RDS host processes the print requests serially rather than in parallel. This can cause a delay for some users. Note that the print server does not wait for a print job to complete before processing the next one. Print jobs that are sent to different printers will print in parallel.

If a user launches an application and also an RDS desktop, and both are hosted on the same RDS host, they share the same user profile. If the user launches an application from the desktop, conflicts may result if both applications try to access or modify the same parts of the user profile, and one of the applications may fail to run properly.

The process of setting up applications or RDS desktops for remote access involves the following tasks:

1 Set up RDS hosts.

2 Create a farm. See Chapter 4, "Creating Farms," on page 21.

3 Create an application pool or an RDS desktop pool. See Chapter 6, "Creating Application Pools," on page 41 or Chapter 5, "Creating RDS Desktop Pools," on page 37.

4 Entitle users and groups. See Chapter 7, "Entitling Users and Groups," on page 45.

5 (Optional) Enable time zone redirection for RDS desktop and application sessions. See "Enable Time Zone Redirection for RDS Desktop and Application Sessions," on page 16.

Note If smart card authentication is enabled, make sure that the Smart Card service is disabled on RDS hosts. Otherwise, authentication might fail. By default, this service is disabled.

Caution When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. To prevent this type of access to the RDS host, follow the procedure that is described in http://support.microsoft.com/kb/179221 to prevent an application from running Windows Explorer.

Because the procedure described in http://support.microsoft.com/kb/179221 affects both desktop and application sessions, it is recommended that you do not create RDS desktop pools and application pools on the same farm if you plan to follow the procedure in the Microsoft KB article, so that desktop sessions are not affected.

Installing Applications

If you plan to create application pools, you must install the applications on the RDS hosts. If you want Horizon 7 to automatically display the list of installed applications, you must install the applications so that they are available to all users from the **Start** menu. You can install an application at any time before you create the application pool. If you plan to manually specify an application, you can install the application at any time, either before or after creating an application pool.

Important When you install an application, you must install it on all the RDS hosts in a farm and in the same location on each RDS host. If you do not, a health warning will appear on the View Administrator dashboard. In such a situation, if you create an application pool, users might encounter an error when they try to run the application.

When you create an application pool, Horizon 7 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all of the RDS hosts in a farm. You can choose any applications from that list. In addition, you can manually specify an application that is not available to all users from the **Start** menu. There is no limit on the number of applications that you can install on an RDS host.

Install Remote Desktop Services on Windows Server 2008 R2

Remote Desktop Services (RDS) is one of the roles that a Windows Server can have. You must install this role to set up an RDS host that runs Windows Server 2008 R2.

Prerequisites

- Verify that the RDS host is running Windows Server 2008 R2 Service Pack 1 (SP1).
- Verify that the RDS host is part of the Active Directory domain for the Horizon 7 deployment.
- Install the Microsoft hotfix rollup that is documented in http://support.microsoft.com/kb/2775511.
- Install the Microsoft update https://support.microsoft.com/en-us/kb/2973201.

Procedure

1 Log in to the RDS host as an administrator.

2 Start Server Manager.

3 Select **Roles** in the navigation tree.

4 Click **Add Roles** to start the Add Role wizard.

5 Select the role **Remote Desktop Services**.

6 On the Select Role Services page, select **Remote Desktop Session Host**.

7 On the Specify Authentication Method page, select either **Require Network Level Authentication** or **Do not require Network Level Authentication**, whichever is appropriate.

8 On the Configure Client Experience page, select the functionality that you want to provide to users.

9 Follow the prompts and finish the installation.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature. The steps for installing Desktop Experience differ on Windows Server 2008 R2 and Windows Server 2012 or 2012 R2.

Restrict users to a single desktop session. See "Restrict Users to a Single Session," on page 13.

Install Remote Desktop Services on Windows Server 2012 or 2012 R2

Remote Desktop Services is one of the roles that a Windows Server 2012 or 2012 R2 can have. You must install this role to set up an RDS host.

Prerequisites

- Verify that the RDS host is running Windows Server 2012 or Windows Server 2012 R2.
- Verify that the RDS host is part of the Active Directory domain for the Horizon 7 deployment.

Procedure

1 Log in to the RDS host as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, select **Remote Desktop Services**.

7 On the Select Features page, accept the defaults.

8 On the Select Role Services page, select **Remote Desktop Session Host**.

9 Follow the prompts and finish the installation.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature. The steps for installing Desktop Experience differ on Windows Server 2008 R2 and Windows Server 2012 or 2012 R2.

Restrict users to a single desktop session. See "Restrict Users to a Single Session," on page 13.

Install Desktop Experience on Windows Server 2008 R2

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Procedure

1 Log in as an administrator.

2 Start Server Manager.

3 Click **Features**.

4 Click **Add Features**.

5 On the Select Features page, select the **Desktop Experience** checkbox.

6 Review the information about other features that are required by the Desktop Experience feature, and click **Add Required Features**.

7 Follow the prompts and finish the installation.

Install Desktop Experience on Windows Server 2012 or 2012 R2

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Windows Server 2012 and Windows Server 2012 R2 are supported on machines that are used as RDS hosts. Windows Server 2012 R2 is supported on single-user virtual machines.

Procedure

1 Log in as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, accept the default selection and click **Next**.

7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.

8 Follow the prompts and finish the installation.

Restrict Users to a Single Session

Horizon 7 supports at most one desktop session and one application session per user on an RDS host. You must configure the RDS host to restrict users to a single session. For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, you can can restrict users to a single session by enabling the group policy setting
`Restrict Remote Desktop Services users to a single Remote Desktop Services session`. This setting is located in the folder `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections`. For Windows Server 2008 R2, you can also use the following procedure to restrict users to a single session.

Prerequisites

- Install the Remote Desktop Services role as described in "Install Remote Desktop Services on Windows Server 2008 R2," on page 11.

Procedure

1. Click **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.
2. On the Edit Settings pane, under General, double-click **Restrict each user to a single session**.
3. In the Properties dialog box, on the General tab, select **Restrict each user to a single session** and click **OK**.

What to do next

Install Horizon Agent on the RDS host. See "Install Horizon Agent on a Remote Desktop Services Host," on page 13.

Install Horizon Agent on a Remote Desktop Services Host

Horizon Agent communicates with Connection Server and supports the display protocols PCoIP and Blast Extreme. You must install Horizon Agent on an RDS Host.

Prerequisites

- Install the Remote Desktop Services role as described in "Install Remote Desktop Services on Windows Server 2008 R2," on page 11 or "Install Remote Desktop Services on Windows Server 2012 or 2012 R2," on page 11.
- Restrict users to a single desktop session. See "Restrict Users to a Single Session," on page 13.
- Familiarize yourself with the Horizon Agent custom setup options. See "Horizon Agent Custom Setup Options for an RDS Host," on page 14.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

Procedure

1. Log in as an administrator.
2. To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.

3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all View components with the same IP version.

4 Select your custom setup options.

Do not select the View Composer Agent option if you are installing Horizon Agent on an RDS host that will be in a manual farm.

5 In the **Server** text box, type the host name or IP address of a Connection Server host.

During installation, the installer registers the RDS host with this Connection Server instance. After registration, the specified Connection Server instance, and any additional instances in the same Connection Server group, can communicate with the RDS host.

6 Select an authentication method to register the RDS host with the Connection Server instance.

Option	Description
Authenticate as the currently logged in user	The **Username** and **Password** text boxes are disabled and you are logged in to the Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a Connection Server administrator in the **Username** and **Password** text boxes.

The user account must be a domain user with access to View LDAP on the View Connection Server instance. A local user does not work.

7 Follow the prompts and finish the installation.

What to do next

Create a farm. See Chapter 4, "Creating Farms," on page 21.

Horizon Agent Custom Setup Options for an RDS Host

When you install Horizon Agent on an RDS host, you can select custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

Table 3-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 Environment

Option	Description
USB Redirection	Gives users access to locally connected USB storage devices. Specifically, redirection of USB flash drives and hard disks is supported in RDS desktops and applications. Redirection of other types of USB devices, and other types of USB storage devices such as security storage drives and USB CD-ROM, is not supported in RDS desktops and applications. This setup option is not selected by default. You must select the option to install it. This option is available on RDS hosts that run Windows Server 2012 or 2012 R2 but not Windows Server 2008 R2. For guidance on using USB redirection securely, see the *View Security* guide. For example, you can use group policy settings to disable USB redirection for specific users.
HTML Access	Allows users to connect to RDS desktops and applications by using HTML Access. The HTML Access Agent is installed when this setup option is selected. This agent must be installed on RDS hosts to allow users to make connections with HTML Access
3D RDSH	Provides 3D graphics support to applications that run on this RDS host.

Table 3-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 Environment (Continued)

Option	Description
View Composer Agent	Select this option if this machine is a parent virtual machine for the creation of an automated farm. Do not select this option if this machine is an RDS host in a manual farm.
Client Drive Redirection	Allows Horizon Client users to share local drives with their RDS desktops and applications. After this setup option is installed, no further configuration is required on the RDS host. Client Drive Redirection is also supported on VDI desktops that run on single-user virtual machines and unmanaged machines.
Virtual Printing	Lets users print to any printer available on their client computers. Users do not have to install additional drivers on their desktops. Virtual printing is supported on the following remote desktops and applications: ■ Desktops that are deployed on single-user machines, including Windows desktop and Windows Server machines. ■ Desktops that are deployed on RDS hosts, where the RDS hosts are virtual machines. ■ Remote applications. ■ Remote applications that are launched from Horizon Client inside remote desktops (nested sessions). The virtual printing feature is supported only when you install it from Horizon Agent. It is not supported if you install it with VMware Tools.
vRealize Operations Desktop Agent	Lets vRealize Operations Manager work with vRealize Operations Manager for Horizon.
Scanner Redirection	Redirects scanning devices that are connected to the client system so that they can be used on the RDS desktop or application. You must install the Desktop Experience feature in the Windows Server operating system on the RDS hosts to make this option available in the Horizon Agent installer. This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it. Scanner redirection is available in Horizon 6.0.2 and later releases.
VMware Client IP Transparency	Enables remote connections to Internet Explorer to use the Client's IP address instead of the remote desktop machine's IP address. This setup option is not selected by default. You must select the option to install it.
Instant Clone	Enables the creation of instant-clone virtual machines on a farm of RDS hosts. This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it.

In an IPv6 environment, there are no optional features.

Table 3-2. Horizon Agent Features That Are Installed Automatically on an RDS Host

Option	Description
PCoIP Agent	Allows users to connect to applications and RDS desktops using the PCoIP display protocol. You must install this component if you plan to create application pools because users can only connect to applications using PCoIP.
Windows Media Multimedia Redirection (MMR)	Provides multimedia redirection for RDS desktops. This feature delivers a multimedia stream directly to the client computer, allowing the multimedia stream to be processed on the client hardware instead of the remote ESXi host.
Unity Touch	Allows tablet and smart phone users to interact with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications without using the Start menu or Taskbar.
PSG Agent	Installs the PCoIP Secure Gateway on RDS hosts to implement the PCoIP display protocol for desktop and application sessions that run on RDS hosts.
VMwareRDS	Provides the VMware implementation of Remote Desktop Services functionality.

In an IPv6 environment, the automatically installed features are PCoIP Agent, PSG Agent, and VMwareRDS.

For additional features that are supported on RDS hosts, see "Feature Support Matrix for Horizon Agent" in the *View Architecture Planning* document.

Printing From a Remote Application Launched Inside a Nested Session

When you enable the Virtual Printing option during Horizon Agent installation, users can print from remote applications that they launch from Horizon Client inside remote desktops (nested sessions) to printers on their local client machine.

Beginning with Horizon 7 version 7.0.2, users can print from remote applications launched inside a nested session to printers connected to the remote desktop machine rather than to printers connected to their local client machine. To enable this feature, change the Thinprint session-in-session mode on the remote desktop machine by changing the value of `SiSActive` to 0 in `HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPClnRDP`.

Note When `SiSActive` is set to 0 on the remote desktop machine, users can no longer print from remote applications launched inside nested sessions to printers connected to their local client machine. To reenable the default ThinPrint session-in-session mode, change the value of `SiSActive` to 1 in `HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPClnRDP` on the remote desktop machine.

For information about enabling the Virtual Printing option during Horizon Agent installation, see "Horizon Agent Custom Setup Options for an RDS Host," on page 14.

Enable Time Zone Redirection for RDS Desktop and Application Sessions

If an RDS host is in one time zone and a user is in another time zone, by default, when the user connects to an RDS desktop, the desktop displays time that is in the time zone of the RDS host. You can enable the Time Zone Redirection group policy setting to make the RDS desktop display time in the local time zone. This policy setting applies to application sessions as well.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

  The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See "Create GPOs for Horizon Group Policies" in the *Configuring Remote Desktop Features in Horizon 7* document.

- Verify that the Horizon 7 RDS ADMX files are added to Active Directory. See "Add the Remote Desktop Services ADMX Files to Active Directory" in the *Configuring Remote Desktop Features in Horizon 7* document.

- Familiarize yourself with the group policy settings. See " RDS Device and Resource Redirection Settings" in the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.
2. Expand your domain and **Group Policy Objects**.
3. Right-click the GPO that you created for the group policy settings and select **Edit**.
4. In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Horizon View RDSH Services > Remote Desktop Session Host > Device and Resource Redirection**.

5 Enable the setting **Allow time zone redirection**.

Enable Windows Basic Theme for Applications

If a user has never connected to a desktop on an RDS host, and the user launches an application that is hosted on the RDS host, the Windows basic theme is not applied to the application even if a GPO setting is configured to load the Aero-styled theme. Horizon 7 does not support the Aero-styled theme but supports the Windows basic theme. To make the Windows basic theme apply to the application, you must configure another GPO setting.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

  The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See "Create GPOs for Horizon 7 Group Policies" in the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

1 On the Active Directory server, open the Group Policy Management Console.

2 Expand your domain and **Group Policy Objects**.

3 Right-click the GPO that you created for the group policy settings and select **Edit**.

4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Administrative Templates > Control Panel > Personalization**.

5 Enable the setting **Force a specific visual style file or force Windows classic** and set the Path to Visual Style as **`%windir%\resources\Themes\Aero\aero.msstyles`**.

Configure Group Policy to Start Runonce.exe

By default, some applications that rely on the Explorer.exe file may not run in an application session. To avoid this issue, you must configure a GPO setting to start runonce.exe.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

  The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See "Create GPOs for Horizon 7 Group Policies" in the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

1 On the Active Directory server, open the Group Policy Management Console.

2 Expand your domain and **Group Policy Objects**.

3 Right-click the GPO that you created for the group policy settings and select **Edit**.

4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.

5 Double-click **Logon** and click **Add**.

6 In the Script Name box, type **`runonce.exe`**.

7 In the Script Parameters box, type **`/AlternateShellStartup`**.

RDS Host Performance Options

You can optimize Windows for either foreground programs or background services by setting performance options. By default, Horizon 7 disables certain performance options for RDS hosts for all supported versions of Windows Server.

The following table shows the performance options that are disabled by Horizon 7.

Table 3-3. Performance Options Disabled by Horizon 7

Performance Options Disabled by Horizon 7
Animate windows when minimizing and maximizing
Show shadows under mouse pointer
Show shadows under windows
Use drop shadow for icon labels on the desktop
Show windows contents while dragging

The five performance options that are disabled by Horizon 7 correspond to four Horizon 7 settings in the registry. The following table shows the Horizon 7 settings and their default registry values. The registry values are all located in the registry subkey `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. You can re-enable the performance options by setting one or more of the Horizon 7 registry values to **`false`**.

Table 3-4. Horizon 7 Settings Related to Windows Performance Options

Horizon 7 Setting	Registry Value
Disable cursor shadow	DisableMouseShadows
Disable full window drag	DisableFullWindowDrag
Disable ListView shadow	DisableListViewShadow
Disable Window Animation	DisableWindowAnimation

Configuring 3D Graphics for RDS Hosts

With 3D graphics configured for RDS hosts, both applications in application pools and applications running on RDS desktops can display 3D graphics.

The following 3D graphics options are available:

NVIDIA GRID vGPU (shared GPU hardware acceleration)
A physical GPU on an ESXi host is shared among multiple virtual machines. Requires ESXi 6.0 or later.

AMD Multiuser GPU using vDGA
A physical GPU on an ESXi host is shared among multiple virtual machines. Requires ESXi 6.0 or later.

Virtual Dedicated Graphics Acceleration (vDGA)
A physical GPU on an ESXi host is dedicated to a single virtual machine. Requires ESXi 5.5 or later.

Note Some Intel vDGA cards require a certain vSphere 6 version. See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

With vDGA, you allocate an entire GPU to a single machine for maximum performance. The RDS host must be in a manual farm.

With AMD Multiuser GPU using vDGA, you can share an AMD GPU between multiple RDS hosts by making it appear as multiple PCI passthrough devices. The RDS host must be in a manual farm.

With NVIDIA GRID vGPU, each graphics card can support multiple RDS hosts and the RDS hosts must be in a manual farm. If an ESXi host has multiple physical GPUs, you can also configure the way the ESXi host assigns virtual machines to the GPUs. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. You can also choose consolidation mode, where the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU. To configure consolidation mode, edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

Overview of Steps for Configuring 3D Graphics

This overview describes tasks that you must perform in vSphere and Horizon 7 to configure 3D graphics. For more information about setting up NVIDIA GRID vGPU, see the document NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1. For more information about setting up vDGA, see the document Graphics Acceleration in View Virtual Desktops. For more information about setting up AMD Multiuser GPU using vDGA, see the *Setting Up Virtual Machine Desktops in Horizon 7* guide.

1. Set up an RDS host virtual machine. For more information, see Chapter 3, “Setting Up Remote Desktop Services Hosts,” on page 9.
2. Add the graphics PCI device to the virtual machine. See "Other Virtual Machine Device Configuration" in the chapter "Configuring Virtual machine Hardware" in the *vSphere Virtual Machine Administration* document. Be sure to click **Reserve all memory** when adding the device.
3. On the virtual machine, install the device driver for the graphics card.
4. Add the RDS host to a manual farm, create an RDS desktop pool, connect to the desktop using PCoIP, and activate the display adapter.

You do not need to configure 3D graphics for RDS hosts in View Administrator. Selecting the option **3D RDSH** when you install Horizon Agent is sufficient. By default, this option is not selected and 3D graphics is disabled.

Creating Farms

4

A farm is a group of RDS hosts that provides a common set of applications or RDS desktops to users.

This chapter includes the following topics:

Farms

Farms simplify the task of managing RDS hosts, RDS desktops, and applications in an enterprise. You can create manual or automated farms to serve groups of users that vary in size or have different desktop or application requirements.

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical or virtual machines. You manually add the RDS hosts when you create the farm.

An automated farm consists of RDS hosts that are instant-clone or linked-clone virtual machines in vCenter Server.

Connection Server creates the instant-clone virtual machines based on the parameters that you specify when you create the farm. Instant clones share a virtual disk of a parent VM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parent VM and are created using the vmFork technology.

View Composer creates the linked-clone virtual machines based on the parameters that you specify when you create the farm. The virtual machines are cloned from a single parent virtual machine and are linked to the parent in a mechanism that reduces the amount of storage that the virtual machines require.

When you create an application pool or an RDS desktop pool, you must specify one and only one farm. The RDS hosts in a farm can host RDS desktops, applications, or both. A farm can support at most one RDS desktop pool, but it can support multiple application pools. A farm can support both types of pools simultaneously.

Farms provide the following conveniences:

- Load balancing

  By default, Horizon 7 balances the load of the RDS desktop sessions and the application sessions across all the RDS hosts in the farm. You can control the placement of new application sessions by writing and configuring load balancing scripts. For more information, see "Configuring Load Balancing for RDS Hosts" in the *View Administration* document.

- Redundancy

  If one RDS host in a farm is offline, the other RDS hosts in the farm continue to provide applications and desktops to users.

- Scalability

  A farm can have a variable number of RDS hosts. You can create farms with different numbers of RDS hosts to serve user groups of different sizes.

Farms have the following properties:

- A Horizon 7 pod can have a maximum of 200 farms.
- A farm can have a maximum of 200 RDS hosts.
- The RDS hosts in a farm can run any supported version of Windows Server. See "System Requirements for Guest Operating Systems" in the *View Installation* document.
- Automated linked-clone farms support the View Composer recompose operation but do not support the refresh or rebalance operation. You can recompose an automated farm but not a subset of the RDS hosts in the farm.

Important Microsoft recommends that you configure roaming profiles for users separately for each farm. The profiles should not be shared between farms or users' physical desktops since profile corruption and data loss may occur if a user is simultaneously logged in to two machines that load the same profile.

Preparing a Parent Virtual Machine for an Automated Farm

To create an automated farm, you must first prepare a parent virtual machine. View Composer or Connection Server uses this parent virtual machine to create linked-clone or instant-clone virtual machines, which are the RDS hosts in the farm.

- Prepare an RDS Host Parent Virtual Machine on page 23

  Both Connection Server and View Composer require a parent virtual machine from which you generate a base image for creating instant clones or linked clones.

- Activating Windows on Linked-Clone RDS Hosts on page 24

  To make sure that View Composer properly activates Windows Server operating systems on linked-clone RDS hosts, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

- Disable Windows Hibernation in the Parent Virtual Machine on page 25

  The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's or a View Composer linked clone's virtual disk.

Prepare an RDS Host Parent Virtual Machine

Both Connection Server and View Composer require a parent virtual machine from which you generate a base image for creating instant clones or linked clones.

Prerequisites

- Verify that an RDS host virtual machine is set up. See Chapter 3, "Setting Up Remote Desktop Services Hosts," on page 9. To set up the RDS host, be sure not to use a virtual machine that was previously registered to View Connection Server.

  A parent virtual machine that you use for View Composer must either belong to the same Active Directory domain as the domain that the linked-clone machines will join or be a member of the local WORKGROUP.

- Verify that the virtual machine was not converted from a View Composer linked clone. A virtual machine that is converted from a linked clone has the clone's internal disk and state information. A parent virtual machine cannot have state information.

  Important Linked clones and virtual machines that were converted from linked clones are not supported as parent virtual machines.

- To create an automated instant-clone farm, you must select the **Instant Clone** option when you install Horizon Agent on the parent virtual machine. See "Install Horizon Agent on a Remote Desktop Services Host," on page 13.

- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.

- Verify that you added an instant-clone domain administrator in Horizon Administrator.

- To create an automated linked-clone farm, you must select the **View Composer Agent** option when you install Horizon Agent on the parent virtual machine.

  To update Horizon Agent in a large environment, you can use standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software. You can also use the recompose operation to update Horizon Agent.

  Note Do not change the log on account for the VMware View Composer Guest Agent Server service in a parent virtual machine. By default, this is the Local System account. If you change this account, the linked clones created from the parent do not start.

- To deploy Windows machines, configure a volume license key and activate the parent virtual machine's operating system with volume activation. See " Activating Windows on Instant Clones and View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.

- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

- To implement the RDS host load balancing feature, modify the RDS host parent virtual machine as described in "Configuring Load Balancing for RDS Hosts" in the *View Administration* document.

Procedure

- Remove the DHCP lease on the parent virtual machine to avoid copying a leased IP address to the linked clones in the farm.

  a On the parent virtual machine, open a command prompt.

  b Type the `ipconfig /release` command.

- Verify that the system disk contains a single volume.

  You cannot deploy linked clones from a parent virtual machine that contains more than one volume. The View Composer service does not support multiple disk partitions. Multiple virtual disks are supported.

- Verify that the virtual machine does not contain an independent disk.

  An independent disk is excluded when you take a snapshot of the virtual machine. Linked clones that are created or recomposed from the virtual machine will not contain the independent disk.

- Disable the hibernation option to reduce the size of linked-clone OS disks that are created from the parent virtual machine.

- Before you take a snapshot of the parent virtual machine, disable searching Windows Update for device drivers.

  This Windows feature can interfere with the customization of linked-clone machines. As each linked clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in repeated searches and customization delays.

- In vSphere Client, disable the vApp Options setting on the parent virtual machine.

- On Windows Server 2008 R2 and Windows Server 2012 R2 machines, disable the scheduled maintenance task that recovers disk space by removing unused features.

  For example: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

  If left enabled, this maintenance task can remove the Sysprep customization script after the linked clones are created, which would cause subsequent recompose operations to fail with customization operation timeout errors. For more information, see the Microsoft KB article available at http://support.microsoft.com/kb/2928948.

- On Windows Server 2012 machines, apply the Microsoft hotfix available at https://support.microsoft.com/en-us/kb/3020396.

  This hotfix allows Sysprep to customize a Windows Server 2012 virtual machine that has the RDS role enabled. Without the hotfix, Sysprep customization will fail on the Windows Server 2012 linked-clone machines that are deployed in an automated farm.

What to do next

Use vSphere Client or vSphere Web Client to take a snapshot of the parent virtual machine in its powered-down state. This snapshot is used as the baseline configuration for the first set of linked-clone machines that are anchored to the parent virtual machine.

Important Before you take a snapshot, completely shut down the parent virtual machine by using the **Shut Down** command in the guest operating system.

Activating Windows on Linked-Clone RDS Hosts

To make sure that View Composer properly activates Windows Server operating systems on linked-clone RDS hosts, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

To activate Windows with volume activation, you use Key Management Service (KMS), which requires a KMS license key. See your Microsoft dealer to acquire a volume license key and configure volume activation.

Note View Composer does not support Multiple Activation Key (MAK) licensing.

Before you create linked-clone machines with View Composer, you must use volume activation to activate the operating system on the parent virtual machine.

When a linked-clone machine is created, and each time the linked clone is recomposed, the View Composer agent uses the parent virtual machine's KMS server to activate the operating system on the linked clone.

For KMS licensing, View Composer uses the KMS server that is configured to activate the parent virtual machine. The KMS server treats an activated linked clone as a computer with a newly issued license.

Disable Windows Hibernation in the Parent Virtual Machine

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's or a View Composer linked clone's virtual disk.

Caution When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Disable the hibernation option.

   a Click **Start** and type **`cmd`** in the **Start Search** box.

   b In the search results list, right-click **Command Prompt** and click **Run as Administrator**.

   c At the User Account Control prompt, click **Continue**.

   d At the command prompt, type **`powercfg.exe /hibernate off`** and press Enter.

   e Type **`exit`** and press Enter.

Worksheet for Creating a Manual Farm

When you create a manual farm, the Add Farm wizard prompts you to configure certain settings.

You can print this worksheet and write down the values you want to specify when you run the Add Farm wizard.

Table 4-1. Worksheet: Configuration Settings for Creating a Manual Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in View Administrator.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the *View Administration* document.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **RDP**. RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to RDS desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is **Yes**.	

Table 4-1. Worksheet: Configuration Settings for Creating a Manual Farm (Continued)

Setting	Description	Fill in Your Value Here
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never** or set the number of minutes as the timeout value. The default is **After 1 minute**.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the **Enabled** box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	

Note Unlike an automated farm, a manual farm does not have the setting **Max sessions per RDS server**, because a manual farm can have RDS hosts that are not identical. For RDS hosts in a manual farm, you can edit individual RDS hosts and change the equivalent setting **Number of connections**.

Worksheet for Creating an Automated Linked-Clone Farm

When you create an automated linked-clone farm, the Add Farm wizard prompts you to configure certain settings.

You can print this worksheet and write down the values you want to specify when you run the Add Farm wizard.

Table 4-2. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in Horizon Administrator.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the *View Administration* document.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **RDP**. RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to RDS desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is **Yes**.	

Table 4-2. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never** or set the number of minutes as the timeout value. The default is **After 1 minute**.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the **Enabled** box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	
Max sessions per RDS server	Determines the maximum number of sessions that an RDS host can support. Select **Unlimited** or **No More Than ...**. The default is **Unlimited**.	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	
Naming pattern	Specify a prefix or a name format. Horizon 7 will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify **{n}** anywhere in a character string and **{n}** will be replaced by the number. You can also specify **{n:fixed=<number of digits>}**, where **fixed=<number of digits>** indicates the number of digits to be used for the number. For example, specify **vm-{n:fixed=3}-sales** and the machine names will be vm-001-sales, vm-002-sales, and so on. **Note** Each machine name, including the automatically generated number, has a 15-character limit.	
Max number of machines	The number of machines to be provisioned.	
Minimum number of ready (provisioned) machines during View Composer maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while View Composer recomposes the machines in the farm.	
Use vSphere Virtual SAN	Specify whether to use VMware Virtual SAN, if available. Virtual SAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts. For more information, see "Using Virtual SAN for High-Performance Storage and Policy-Based Management" in the *Setting Up Virtual Desktops in Horizon 7* document.	

Table 4-2. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Select separate datastores for replica and OS disks	(Available only if you do not use Virtual SAN) You can place replica and OS disks on different datastores for performance or other reasons.	
Parent VM	Select a parent virtual machine from the list. Be aware that the list includes virtual machines that do not have View Composer Agent installed. You must not select any of those machines because View Composer Agent is required. A good practice is to use a naming convention that indicates whether a virtual machine has View Composer Agent installed.	
Snapshot	Select the snapshot of the parent virtual machine to use as the base image for the farm. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no linked clones in the farm use the default image, and no more linked clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new linked clones in the farm, according to farm policies. The parent virtual machine and snapshot are also required for View Composer maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	
Cluster	Select the ESXi host or cluster on which the desktop virtual machines run. With Virtual SAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts if the replicas are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts.	
Resource pool	Select the vCenter Server resource pool in which the farm resides.	
Datastores	Select one or more datastores on which to store the farm. A table on the Select Linked Clone Datastores page of the Add Farm wizard provides high-level guidelines for estimating the farm's storage requirements. These guidelines can help you determine which datastores are large enough to store the linked-clone disks. For details, see "Storage Sizing for Instant-Clone and Linked-Clone Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document. You can use shared or local datastores for an individual ESXi host or for ESXi clusters. If you use local datastores in an ESXi cluster, you must consider the vSphere infrastructure constraints that are imposed on your desktop deployment. For details, see "Storing Linked Clones on Local Datastores" in the *Setting Up Virtual Desktops in Horizon 7* document.. **Note** If you use Virtual SAN, select only one datastore.	

Table 4-2. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Storage Overcommit	Determine the storage-overcommit level at which linked-clones are created on each datastore. As the level increases, more linked clones fit on the datastore and less space is reserved to let individual clones grow. A high storage-overcommit level lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore. For details, see "Storage Overcommit for View Composer Linked-Clone Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document. **Note** This setting has no effect if you use Virtual SAN.	
Use native NFS snapshots (VAAI)	(Available only if you do not use Virtual SAN) If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can use native snapshot technology to clone virtual machines. You can use this feature only if you select datastores that reside on NAS devices that support native cloning operations through VAAI. You cannot use this feature if you store replicas and OS disks on separate datastores. You cannot use this feature on virtual machines with space-efficient disks. This feature is supported on vSphere 5.0 and later. For details, see "Using VAAI Storage for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document..	
Reclaim VM disk space	(Available only if you do not use Virtual SAN or Virtual Volumes) Determine whether to allow ESXi hosts to reclaim unused disk space on linked clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for linked-clone desktops. This feature is supported on vSphere 5.1 and later. The linked-clone virtual machines must be virtual hardware version 9 or later. For details, see "Reclaim Disk Space on Linked-Clone Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Initiate reclamation when unused space on VM exceeds:	(Available only if you do not use Virtual SAN or Virtual Volumes) Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, View initiates the operation that directs the ESXi host to reclaim space on the OS disk. This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before View starts the space reclamation process on that machine. For example: **2** GB. The default value is 1 GB.	
Blackout Times	Configure days and times during which the reclamation of virtual machine disk space do not take place. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days. For details, see " Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.	

Table 4-2. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Farm**, **Pod**, or **Global**. If you turn on TPS for all the machines in the farm, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the farm level but the farm is spread across multiple ESXi hosts, only virtual machines on the same host and within the same farm will share pages. At the global level, all machines managed by View on the same ESXi host can share memory pages, regardless of which farm the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Domain	Select the Active Directory domain and user name. View Composer requires certain user privileges to farm. The domain and user account are used by Sysprep to customize the linked-clone machines. You specify this user when you configure View Composer settings for vCenter Server. You can specify multiple domains and users when you configure View Composer settings. When you use the Add Farm wizard to create a farm, you must select one domain and user from the list. For information about configuring View Composer, see the *View Administration* document.	
AD container	Provide the Active Directory container relative distinguished name. For example: **`CN=Computers`** When you run the Add Farm wizard, you can browse your Active Directory tree for the container.	
Allow reuse of pre-existing computer accounts	Select this setting to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This setting lets you control the computer accounts that are created in Active Directory. When a linked clone is provisioned, if an existing AD computer account name matches the linked clone machine name, View Composer uses the existing computer account. Otherwise, a new computer account is created. The existing computer accounts must be located in the Active Directory container that you specify with the **Active Directory container** setting. When this setting is disabled, a new AD computer account is created when View Composer provisions a linked clone. This setting is disabled by default. For details, see "Use Existing Active Director Computer Accounts for Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Use a customization specification (Sysprep)	Provide a Sysprep customization specification to customize the virtual machines.	

Worksheet for Creating an Automated Instant-Clone Farm

When you create an automated instant-clone farm, the Add Farm wizard prompts you to configure certain settings.

You can print this worksheet and write down the values you want to specify when you run the Add Farm wizard.

Table 4-3. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in Horizon Administrator.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the *View Administration* document.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **RDP**. RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to RDS desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is **Yes**.	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never** or set the number of minutes as the timeout value. The default is **After 1 minute**.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the **Enabled** box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	
Max sessions per RDS server	Determines the maximum number of sessions that an RDS host can support. Select **Unlimited** or **No More Than ...**. The default is **Unlimited**.	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	

Table 4-3. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Naming pattern	Specify a prefix or a name format. Horizon 7 will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify **{n}** anywhere in a character string and **{n}** will be replaced by the number. You can also specify **{n:fixed=<number of digits>}**, where **fixed=<number of digits>** indicates the number of digits to be used for the number. For example, specify **vm-{n:fixed=3}-sales** and the machine names will be vm-001-sales, vm-002-sales, and so on. **Note** Each machine name, including the automatically generated number, has a 15-character limit.	
Max number of machines	The number of machines to be provisioned.	
Minimum number of ready (provisioned) machines during Instant Clone maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while Connection Server performs maintenance operations on the machines in the farm. This setting is not honored if you schedule immediate maintenance.	
Use vSphere Virtual SAN	Specify whether to use VMware Virtual SAN, if available. Virtual SAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts. For more information, see "Using Virtual SAN for High-Performance Storage and Policy-Based Management" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Select separate datastores for replica and OS disks	(Available only if you do not use Virtual SAN) You can place replica and OS disks on different datastores for performance or other reasons. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.	
Parent VM	Select a parent virtual machine from the list. Be aware that the list includes virtual machines that do not have View Composer Agent installed. You must not select any of those machines because View Composer Agent is required. A good practice is to use a naming convention that indicates whether a virtual machine has View Composer Agent installed.	
Snapshot	Select the snapshot of the parent virtual machine to use as the base image for the farm. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no instant clones in the farm use the default image, and no more instant clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new instant clones in the farm, according to farm policies. The parent virtual machine and snapshot are also required for Connection Server maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	

Table 4-3. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Cluster	Select the ESXi host or cluster on which the desktop virtual machines run. With Virtual SAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts if the replicas are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts.	
Resource pool	Select the vCenter Server resource pool in which the farm resides.	
Datastores	Select one or more datastores on which to store the farm. A table on the Select Instant Clone Datastores page of the Add Farm wizard provides high-level guidelines for estimating the farm's storage requirements. These guidelines can help you determine which datastores are large enough to store the instant-clones. The Storage Overcommit value is always set to Unbounded and is not configurable. For details, see "Storage Sizing for Instant-Clone and Linked-Clone Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document. **Note** If you use Virtual SAN, select only one datastore.	
Replica disk datastores	Select one or more replica disk datastores on which to store the instant-clones. This option appears if you select separate datastores for replica and OS disks. A table on the Select Replica Disk Datastores page of the Add Farm wizard provides high-level guidelines for estimate the farm's storage requirements. These guidelines can help you determine which replica disk datastores are enough to store the instant-clones.	
Networks	Select the networks to use for the automated instant-clone farm. You can select multiple vLAN networks to create a larger instant-clone desktop pool. The default setting uses the network from the current parent VM image. A table on the Select Networks wizard provides the networks, ports, and port bindings that are available to use. To use multiple networks, you must unselect **Use network from current parent VM** and then select the networks to use with the instant-clone farm.	
Domain	Select the Active Directory domain and user name. Connection Server requires certain user privileges to farm. The domain and user account are used by ClonePrep to customize the instant-clone machines. You specify this user when you configure Connection Server settings for vCenter Server. You can specify multiple domains and users when you configure Connection Server settings. When you use the Add Farm wizard to create a farm, you must select one domain and user from the list. For information about configuring Connection Server, see the *View Administration* document.	
AD container	Provide the Active Directory container relative distinguished name. For example: **`CN=Computers`** When you run the Add Farm wizard, you can browse your Active Directory tree for the container. You can cut, copy, or paste in the container name.	

Table 4-3. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Use ClonePrep	Provide a ClonePrep customization specification to customize the virtual machines. ■ **Power-off script name**. Name of the customization script that ClonePrep runs on instant-clone machines before they are powered off. Provide the path to the script on the parent virtual machine. ■ **Power-off script parameters**. Provide parameters that ClonePrep can use to run a customization script on instant-clone machines before they are powered off. For example, use p1. ■ **Post-synchronization script name**. Name of the customization script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. Provide the path to the script on the parent virtual machine. ■ **Post-synchronization script parameters**. Provide parameters for the script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. For example, use p2. For details on how ClonePrep runs customization scripts, see "ClonePrep Guest Customization" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Ready to Complete	Review the settings for the automated instant-clone farm.	

Create a Manual Farm

You create a manual farm as part of the process to give users access to applications or RDS desktops.

Prerequisites

- Set up the RDS hosts that belong to the farm. See Chapter 3, "Setting Up Remote Desktop Services Hosts," on page 9.
- Verify that all the RDS hosts have the Available status. In View Administrator, select **View Configuration > Registered Machines** and check the status of each RDS host on the RDS Hosts tab.
- Gather the configuration information you must provide to create the farm. See "Worksheet for Creating a Manual Farm," on page 25.

Procedure

1 In View Administrator, click **Resources > Farms**.

2 Click **Add** to enter the configuration information that you gathered in the worksheet.

3 Select **Manual Farm**.

4 Follow the prompts in the wizard to create the farm.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

5 Select the RDS hosts to add to the farm and click **Next**.

6 Click **Finish**.

In View Administrator, you can now view the farm by clicking **Resources > Farms**.

What to do next

Create an application pool or an RDS desktop pool. See Chapter 6, "Creating Application Pools," on page 41 or Chapter 5, "Creating RDS Desktop Pools," on page 37.

Create an Automated Linked-Clone Farm

You create an automated linked-clone farm as part of the process to give users access to applications or RDS desktops.

Prerequisites

- Verify that the View Composer service is installed. See the *View Installation* document.
- Verify that View Composer settings for vCenter Server are configured in Horizon Administrator. See the *View Administration* document.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.
- Verify that you prepared a parent virtual machine. Both Horizon Agent and View Composer Agent must be installed on the parent virtual machine. See "Preparing a Parent Virtual Machine for an Automated Farm," on page 22.
- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

  NOTE You cannot create a linked-clone pool from a virtual machine template.

- Gather the configuration information you must provide to create the farm. See "Worksheet for Creating an Automated Linked-Clone Farm," on page 26.

Procedure

1. In Horizon Administrator, click **Resources > Farms**.
2. Click **Add** to enter the configuration information that you gathered in the worksheet.
3. Select **Automated Farm** and click **Next**.
4. Select **View Composer linked clones** and click **Next**.
5. Follow the prompts in the wizard to create the farm.

   Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In Horizon Administrator, you can now view the farm by clicking **Resources > Farms**.

What to do next

Create an application pool or an RDS desktop pool. See Chapter 6, "Creating Application Pools," on page 41 or Chapter 5, "Creating RDS Desktop Pools," on page 37.

Create an Automated Instant-Clone Farm

You create an automated instant-clone farm as part of the process to give users access to applications or RDS desktops.

Prerequisites

- Verify that Connection Server is installed. See the *View Installation* document.
- Verify that Connection Server settings for vCenter Server are configured in Horizon Administrator. See the *View Administration* document.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools.
- Verify that you prepared a parent virtual machine. Horizon Agent must be installed on the parent virtual machine. See "Preparing a Parent Virtual Machine for an Automated Farm," on page 22.
- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. Connection Server uses the snapshot as the base image from which the clones are created.
- Gather the configuration information you must provide to create the farm. See "Worksheet for Creating an Automated Instant-Clone Farm," on page 31.

Procedure

1 In Horizon Administrator, click **Resources > Farms**.

2 Click **Add** to enter the configuration information that you gathered in the worksheet.

3 Select **Automated Farm** and click **Next**.

4 Select **Instant clones** and click **Next**.

5 Follow the prompts in the wizard to create the farm.

   Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In Horizon Administrator, you can now view the farm by clicking **Resources > Farms**.

What to do next

Create an application pool or an RDS desktop pool. See Chapter 6, "Creating Application Pools," on page 41 or Chapter 5, "Creating RDS Desktop Pools," on page 37.

Creating RDS Desktop Pools

5

One of the tasks that you perform to give users remote access to session-based desktops is to create a Remote Desktop Services (RDS) desktop pool. An RDS desktop pool has properties that can satisfy some specific needs of a remote desktop deployment.

This chapter includes the following topics:

Understanding RDS Desktop Pools

An RDS desktop pool is one of three types of desktop pools that you can create. This type of pool was known as a Microsoft Terminal Services pool in previous View releases.

An RDS desktop pool and an RDS desktop have the following characteristics:

- An RDS desktop pool is associated with a farm, which is a group of RDS hosts. Each RDS host is a Windows server that can host multiple RDS desktops.
- An RDS desktop is based on a session to an RDS host. In contrast, a desktop in an automated desktop pool is based on a virtual machine, and a desktop in a manual desktop pool is based on a virtual or physical machine.
- An RDS desktop supports the RDP, PCoIP, and VMware Blast display protocols. To enable HTML Access, see "Prepare Desktops, Pools, and Farms for HTML Access," in the "Setup and Installation" chapter in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- An RDS desktop pool is only supported on Windows Server operating systems that support the RDS role and are supported by View. See "System Requirements for Guest Operating Systems" in the *View Installation* document.
- View provides load balancing of the RDS hosts in a farm by directing connection requests to the RDS host that has the least number of active sessions.
- Because an RDS desktop pool provides session-based desktops, it does not support operations that are specific to a linked-clone desktop pool, such as refresh, recompose, and rebalance.

- If an RDS host is a virtual machine that is managed by vCenter Server, you can use snapshots as base images. You can use vCenter Server to manage the snapshots. The use of snapshots on RDS host virtual machines is transparent to View.
- RDS desktops do not support View Persona Management.
- The copy and paste feature is disabled by default for HTML Access. To enable the feature, see "HTML Access Group Policy Settings" in the chapter "Configuring HTML Access for End Users" in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Create an RDS Desktop Pool

You create an RDS desktop pool as part of the process to give users access to RDS desktops.

Prerequisites

- Set up RDS hosts. See Chapter 3, "Setting Up Remote Desktop Services Hosts," on page 9.
- Create a farm that contains the RDS hosts. See Chapter 4, "Creating Farms," on page 21.
- Decide how to configure the pool settings. See "Desktop Pool Settings for RDS Desktop Pools," on page 38.

Procedure

1. In View Administrator, select **Catalog > Desktop Pools**.
2. Click **Add**.
3. Select **RDS Desktop Pool**.
4. Provide a pool ID, display name, and description.

   The pool ID is the unique name that identifies the pool in View Administrator. The display name is the name of the RDS desktop pool that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as the pool ID.
5. Select pool settings.
6. Select or create a farm for this pool.

In View Administrator, you can now view the RDS desktop pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 45.

Make sure that your end users have access to Horizon Client 3.0 or later software, which is required to support RDS desktop pools.

Desktop Pool Settings for RDS Desktop Pools

You can specify certain pool settings when you create an RDS desktop pool. Not all pool settings apply to all types of desktop pools.

For descriptions of all pool settings, see "Desktop and Pool Settings for All Desktop Pools Types" in the *Setting Up Virtual Desktops in Horizon 7* document. The following pool settings apply to an RDS desktop pool.

Table 5-1. Settings for an RDS Desktop Pool

Setting	Default Value
State	Enabled
Connection Server restrictions	None
Adobe Flash quality	Do not control
Adobe Flash throttling	Disabled

Troubleshooting Instant Clones in the Internal VM Debug Mode

You can use the internal VM debug mode to troubleshoot internal virtual machines in instant-clone farms. With the internal VM debug mode, you can analyze failed internal virtual machines before these virtual machines are deleted.

Prerequisites

- Create an instant-clone farm.

Procedure

1. In the vSphere Web Client, select the master VM, and click **Manage > Configure > VM Options > Edit > VM Options > Advanced > Edit Configuration**.

   The Configuration Parameters window displays a list of parameter names and values.

2. In the Configuration Parameters window, search for the `cloneprep.debug.mode` parameter.

   If the master VM does not have the `cloneprep.debug.mode` parameter, you must add `cloneprep.debug.mode` as the parameter name and add a value of ON or OFF. If the master VM has the `cloneprep.debug.mode` parameter, you can change the value of the parameter to ON or OFF.

3. Enable or disable the internal VM debug mode for internal VMs.

   - To enable the internal VM debug mode, set the value of `cloneprep.debug.mode` to ON. If you enable the internal VM debug mode, the internal VMs are not locked and cannot be deleted by Horizon Server.
   - To disable the internal VM debug mode, set the value of `cloneprep.debug.mode` to OFF. If you disable the internal VM debug mode, the internal VMs are locked and can be deleted by Horizon Server.

   For instant clones actions such as prime, provision, resync, or unprime, the internal virtual machines use the value set in the master virtual machine. If you do not disable the internal VM debug mode, then the VMs remain in vSphere till you delete the VMs.

Adobe Flash Quality and Throttling

You can specify a maximum allowable level of quality for Adobe Flash content that overrides Web page settings. If Adobe Flash quality for a Web page is higher than the maximum level allowed, quality is reduced to the specified maximum. Lower quality results in more bandwidth savings.

To make use of Adobe Flash bandwidth-reduction settings, Adobe Flash must not be running in full screen mode.

Table 5-2 shows the available Adobe Flash render-quality settings.

Table 5-2. Adobe Flash Quality Settings

Quality Setting	Description
Do not control	Quality is determined by Web page settings.
Low	This setting results in the most bandwidth savings.
Medium	This setting results in moderate bandwidth savings.
High	This setting results in the least bandwidth savings.

If no maximum level of quality is specified, the system defaults to a value of **Low**.

Adobe Flash uses timer services to update what is shown on the screen at a given time. A typical Adobe Flash timer interval value is between 4 and 50 milliseconds. By throttling, or prolonging, the interval, you can reduce the frame rate and thereby reduce bandwidth.

Table 5-3 shows the available Adobe Flash throttling settings.

Table 5-3. Adobe Flash Throttling Settings

Throttling Setting	Description
Disabled	No throttling is performed. The timer interval is not modified.
Conservative	Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.
Moderate	Timer interval is 500 milliseconds.
Aggressive	Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.

Audio speed remains constant regardless of which throttling setting you select.

Configure Adobe Flash Throttling with Internet Explorer for RDS Desktop Pools

To ensure that Adobe Flash throttling works with Internet Explorer in RDS desktops, users must enable third-party browser extensions.

Procedure

1 Start Horizon Client and log in to a user's desktop.

2 In Internet Explorer, click **Tools > Internet Options**.

3 Click the **Advanced** tab, select **Enable third-party browser extensions**, and click **OK**.

4 Restart Internet Explorer.

Creating Application Pools 6

One of the tasks that you perform to give users remote access to an application is to create an application pool. Users who are entitled to an application pool can access the application remotely from a variety of client devices.

This chapter includes the following topics:

Application Pools

With application pools, you can deliver a single application to many users. The application runs on a farm of RDS hosts.

When you create an application pool, you deploy an application in the data center that users can access from anywhere on the network.

An application pool has a single application and is associated with a single farm. To avoid errors, you must install the application on all of the RDS hosts in the farm.

When you create an application pool, Horizon 7 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all the RDS hosts in the farm. You can select one or more applications from the list. If you select multiple applications from the list, a separate application pool is created for each application. You can also manually specify an application that is not on the list. If an application that you want to manually specify is not already installed, Horizon 7 displays a warning message.

When you create an application pool, you cannot specify the access group in which to place the pool. For application pools and RDS desktop pools, you specify the access group when you create a farm.

An application supports the PCoIP and VMware Blast display protocols. To enable HTML Access, see "Prepare Desktops, Pools, and Farms for HTML Access," in the "Setup and Installation" chapter in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Worksheet for Creating an Application Pool Manually

When you create an application pool and manually specify an application, the Add Application Pools wizard prompts you for information about the application. It is not a requirement that the application is already installed on any RDS host.

You can print this worksheet and write down the properties of an application when you specify the application manually.

Table 6-1. Worksheet: Application Properties for Creating an Application Pool Manually

Property	Description	Fill in Your Value Here
ID	Unique name that identifies the pool in View Administrator. This field is required.	
Display Name	Pool name that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as **ID**.	
Version	Version of the application.	
Publisher	Publisher of the application.	
Path	Full pathname of the application. For example, `C:\Program Files\app1.exe`. This field is required.	
Start Folder	Full pathname of the starting directory for the application.	
Parameters	Parameters to pass to the application when it starts. For example, you can specify `–username user1 –loglevel 3`.	
Description	Description of this application pool.	

Create an Application Pool

You create an application pool as part of the process to give users access to an application that runs on RDS hosts.

Prerequisites

- Set up RDS hosts. See Chapter 3, "Setting Up Remote Desktop Services Hosts," on page 9.
- Create a farm that contains the RDS hosts. See Chapter 4, "Creating Farms," on page 21.
- If you plan to add the application pool manually, gather information about the application. See "Worksheet for Creating an Application Pool Manually," on page 42.

Procedure

1 In View Administrator, click **Catalog > Application Pools**.

2 Click **Add**.

3 Follow the prompts in the wizard to create the pool.

If you choose to add an application pool manually, use the configuration information you gathered in the worksheet. If you select applications from the list that View Administrator displays, you can select multiple applications. A separate pool is created for each application.

In View Administrator, you can now view the application pool by clicking **Catalog > Application Pools**.

What to do next

Entitle users to access the pool. See Chapter 7, “Entitling Users and Groups,” on page 45.

Make sure that your end users have access to Horizon Client 3.0 or later software, which is required to support RDS applications.

If you need to ensure that View Connection Server launches the application only on RDS hosts that have sufficient resources to run the application, configure an anti-affinity rule for the application pool. For more information, see "Configure an Anti-Affinity Rule for an Application Pool" in the *View Administration* document.

Entitling Users and Groups 7

You configure entitlements to control which remote desktops and applications your users can access. You can configure the restricted entitlements feature to control desktop access based on the View Connection Server instance that users connect to when they select remote desktops. You can also restrict access to a set of users outside the network from connecting to remote desktops and applications within the network.

In a Cloud Pod Architecture environment, you create global entitlements to entitle users or groups to multiple desktops across multiple pods in a pod federation. When you use global entitlements, you do not need to configure and manage local entitlements for remote desktops. For information about global entitlements and setting up a Cloud Pod Architecture environment, see the *Administering View Cloud Pod Architecture* document.

This chapter includes the following topics:

Add Entitlements to a Desktop or Application Pool

Before users can access remote desktops or applications, they must be entitled to use a desktop or application pool.

Prerequisites

Create a desktop or application pool.

Procedure

1 Select the desktop or application pool.

Option	Action
Add an entitlement for a desktop pool	In View Administrator, select **Catalog > Desktop Pools** and click the name of the desktop pool.
Add an entitlement for an application pool	In View Administrator, select **Catalog > Application Pools** and click the name of the application pool.

2 Select **Add entitlement** from the **Entitlements** drop-down menu.

3 Click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria.

Note Domain local groups are filtered out of search results for mixed-mode domains. You cannot entitle users in domain local groups if your domain is configured in mixed mode.

4 Select the users or groups you want to entitle to the desktops or applications in the pool and click **OK**.

5 Click **OK** to save your changes.

Remove Entitlements from a Desktop or Application Pool

You can remove entitlements from a desktop or application pool to prevent specific users or groups from accessing a desktop or application.

Procedure

1 Select the desktop or application pool.

Option	Description
Remove an entitlement for a desktop pool	In View Administrator, select **Catalog > Desktop Pools** and click the name of the desktop pool.
Remove an entitlement for an application pool	In View Administrator, select **Catalog > Application Pools** and click the name of the application pool.

2 Select **Remove entitlement** from the **Entitlements** drop-down menu.

3 Select the user or group whose entitlement you want to remove and click **Remove**.

4 Click **OK** to save your changes.

Review Desktop or Application Pool Entitlements

You can review the desktop or application pools to which a user or group is entitled.

Procedure

1 In View Administrator, select **Users and Groups** and click the name of the user or group.

2 Click the **Entitlements** tab and review the desktop or application pools to which the user or group is entitled.

Option	Action
List the desktop pools to which the user or group is entitled	Click **Desktop Pools**.
List the application pools to which the user or group is entitled	Click **Application Pools**.

Restricting Remote Desktop Access

You can configure the restricted entitlements feature to restrict remote desktop access based on the Connection Server instance to which users connect when they select desktops.

With restricted entitlements, you assign one or more tags to a Connection Server instance. Then, when you configure a desktop pool, you select the tags of the Connection Server instances that you want to have access to the desktop pool.

When users log in to a tagged Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

You cannot configure the restricted entitlements feature to restrict access to remote applications.

For information about using tags to restrict access to global entitlements in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

- Restricted Entitlement Example on page 47

  This example shows a Horizon deployment that includes two Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

- Tag Matching on page 48

  The restricted entitlements feature uses tag matching to determine whether a Connection Server instance can access a particular desktop pool.

- Considerations and Limitations for Restricted Entitlements on page 49

  Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- Assign a Tag to a Connection Server Instance on page 49

  When you assign a tag to a Connection Server instance, users who connect to that Connection Server instance can access only those desktop pools that have a matching tag or no tags.

- Assign a Tag to a Desktop Pool on page 49

  When you assign a tag to a desktop pool, only users who connect to a Connection Server instance that has a matching tag can access the desktops in that pool.

Restricted Entitlement Example

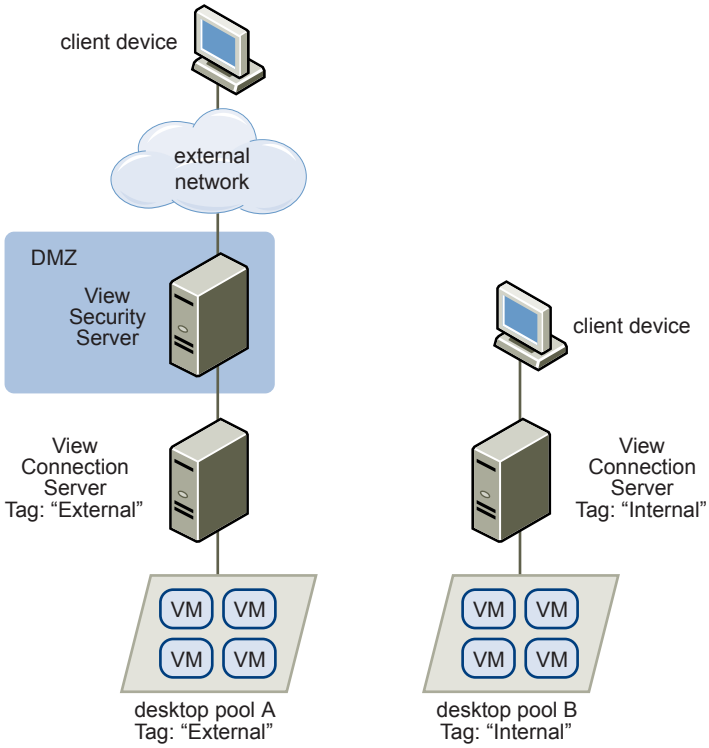
This example shows a Horizon deployment that includes two Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

- Assign the tag "Internal" to the Connection Server instance that supports your internal users.
- Assign the tag "External" to the Connection Server instance that is paired with the security server and supports your external users.
- Assign the "Internal" tag to the desktop pools that should be accessible only to internal users.
- Assign the "External" tag to the desktop pools that should be accessible only to external users.

External users cannot see the desktop pools tagged as Internal because they log in through the Connection Server instance that is tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the Connection Server instance that is tagged as Internal. Figure 7-1 illustrates this configuration.

Figure 7-1. Restricted Entitlement Configuration



You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular Connection Server instance. For example, you can make certain desktop pools available only to users who have authenticated with a smart card.

Tag Matching

The restricted entitlements feature uses tag matching to determine whether a Connection Server instance can access a particular desktop pool.

At the most basic level, tag matching determines that a Connection Server instance that has a specific tag can access a desktop pool that has the same tag.

The absence of tag assignments can also affect whether a Connection Server instance can access a desktop pool. For example, Connection Server instances that do not have any tags can access only desktop pools that also do not have any tags.

Table 7-1 shows how the restricted entitlement feature determines when a Connection Server can access a desktop pool.

Table 7-1. Tag Matching Rules

View Connection Server	Desktop Pool	Access Permitted?
No tags	No tags	Yes
No tags	One or more tags	No
One or more tags	No tags	Yes
One or more tags	One or more tags	Only when tags match

The restricted entitlements feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular Connection Server instance.

Considerations and Limitations for Restricted Entitlements

Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- A single Connection Server instance or desktop pool can have multiple tags.
- Multiple Connection Server instances and desktop pools can have the same tag.
- Any Connection Server instance can access a desktop pool that does not have any tags.
- Connection Server instances that do not have any tags can access only desktop pools that also do not have any tags.
- If you use a security server, you must configure restricted entitlements on the Connection Server instance with which the security server is paired. You cannot configure restricted entitlements on a security server.
- You cannot modify or remove a tag from a Connection Server instance if that tag is still assigned to a desktop pool and no other Connection Server instances have a matching tag.
- Restricted entitlements take precedence over other desktop entitlements or assignments. For example, even if a user is assigned to a particular machine, the user cannot access that machine if the tag assigned to the desktop pool does not match the tag assigned to the Connection Server instance to which the user is connected.
- If you intend to provide access to your desktops through VMware Identity Manager and you configure Connection Server restrictions, the VMware Identity Manager app might display desktops to users when those desktops are actually restricted. When a VMware Identity Manager user attempts to log in to a desktop, the desktop does not start if the tag assigned to the desktop pool does not match the tag assigned to the Connection Server instance to which the user is connected.

Assign a Tag to a Connection Server Instance

When you assign a tag to a Connection Server instance, users who connect to that Connection Server instance can access only those desktop pools that have a matching tag or no tags.

Procedure

1 In Horizon Administrator, select **View Configuration > Servers**.

2 Click the **Connection Servers** tab, select the Connection Server instance, and click **Edit**.

3 Type one or more tags in the **Tags** text box.

Separate multiple tags with a comma or semicolon.

4 Click **OK** to save your changes.

What to do next

Assign the tag to desktop pools. See "Assign a Tag to a Desktop Pool," on page 49.

Assign a Tag to a Desktop Pool

When you assign a tag to a desktop pool, only users who connect to a Connection Server instance that has a matching tag can access the desktops in that pool.

You can assign a tag when you add or edit a desktop pool.

Prerequisites

Assign tags to one or more Connection Server instances.

Procedure

1 In Horizon Administrator, select **Catalog > Desktop Pools**.

2 Select the desktop pool.

Option	Action
Assign a tag to a new pool	Click **Add** to start the Add Desktop Pool wizard and define and identify the pool.
Assign a tag to an existing pool	Select the pool and click **Edit**.

3 Go to the Desktop Pool Settings page.

Option	Action
Pool settings for a new pool	Click **Desktop Pool Settings** in the Add Desktop Pool wizard.
Pool settings for an existing pool	Click the **Desktop Pool Settings** tab.

4 Click **Browse** next to **Connection Server restrictions** and configure the Connection Server instances that can access the desktop pool.

Option	Action
Make the pool accessible to any Connection Server instance	Select **No Restrictions**.
Make the pool accessible only to Connection Server instances that have those tags	Select **Restricted to these tags** and select one or more tags. You can use the check boxes to select multiple tags.

5 Click **OK** to save your changes.

Restricting Remote Desktop Access Outside the Network

You can allow access to specific entitled users and groups from an external network while restricting access to other entitled users and groups. All entitled users will have access to desktops and applications from within the internal network. If you choose not to restrict access to specific users from the external network, then all entitled users will have access from the external network.

For security reasons, administrators might need to restrict users and groups outside the network from accessing remote desktops and applications inside the network. When a restricted user accesses the system from an external network, a message stating that the user is not entitled to use the system appears. The user must be inside the internal network to get access to desktop and application pool entitlements.

Restrict Users Outside the Network

You can allow access to the View Connection Server instance from outside the network to users and groups while restricting access for other users and groups.

Prerequisites

- An Access Point appliance, security server, or load balancer must be deployed outside the network as a gateway to the View Connection Server instance to which the user is entitled. For more information about deploying an Access Point appliance, see the *Deploying and Configuring Access Point* document.
- The users who get remote access must be entitled to desktop or application pools.

Procedure

1 In View Administrator, select **Users and Groups**.

2 Click the **Remote Access** tab.

3 Click **Add** and select one or more search criteria, and click **Find** to find users or groups based on your search criteria.

4 To provide remote access for a user or group, select a user or group and click **OK**.

5 To remove a user or group from remote access, select the user or group, click **Delete**, and click **OK**.

Index

S

T

V

W