Setting Up Published Desktops and Applications in Horizon

VMware Horizon 2106

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

https://docs.vmware.com/

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

Contents

Setting Up Published Desktops and Applications in Horizon

1

Setting Up Published Desktops and Applications in Horizon 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, 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 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.

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. See https://kb.vmware.com/s/article/2150348 for the maximum number of RDSH host servers supported per farm.

Published Desktops

Published desktops are desktop pools, which provide users with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously. You can create a published desktop pool from a physical system such as an RDS host. Use published desktop pools to provide multiple users with desktop sessions on an RDS host.

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, giving them access to published applications that run on servers in a data center instead of on their personal computers or devices.

Configure Horizon for Published Desktops Delivery

You can enable Horizon to deliver published desktops on existing or new RDS hosts.

Procedure

1 To configure Horizon to deliver published desktops on existing RDS hosts, complete the following tasks:

   a Prepare existing RDS hosts for Horizon. The RDS hosts can be physical or virtual machines. See Chapter 3 Setting Up Remote Desktop Services Hosts

   b Create a manual farm. A manual farm consists of RDS hosts that already exist. You manually add the RDS hosts when you create the farm. See Create a Manual Farm in Horizon.

   c Create a published desktop pool for the manual farm you created. See Create a Published Desktop Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

2 To configure Horizon to deliver published desktops on new RDS hosts, complete the following tasks:

   a Prepare an RDS host golden image virtual machine. Horizon clones the RDS hosts from this machine as part of the farm creation process. See Prepare an RDS Host Golden Image Virtual Machine.

   b Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See Create an Automated Instant-Clone Farm in Horizon.

   c Create a published desktop pool for the automated farm you created. See Create a Published Desktop Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

Configure Horizon for Published Applications Delivery

You can enable Horizon to deliver published applications on existing or new RDS hosts.

Procedure

1 To configure Horizon to deliver published applications on existing RDS hosts, complete the following tasks:

   a Prepare existing RDS hosts for Horizon. The RDS hosts can be physical or virtual machines. See Chapter 3 Setting Up Remote Desktop Services Hosts

   b Create a manual farm. A manual farm consists of RDS hosts that already exist. You manually add the RDS hosts when you create the farm. See Create a Manual Farm in Horizon.

   c Create a published application pool for the manual farm you created. See Create an Application Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

2 To configure Horizon to deliver published desktops on new RDS hosts, complete the following tasks:

   a Prepare an RDS host golden image virtual machine. Horizon clones the RDS hosts from this machine as part of the farm creation process. See Prepare an RDS Host Golden Image Virtual Machine.

   b Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See Create an Automated Instant-Clone Farm in Horizon.

   c Create a published application pool for the automated farm you created. See Create an Application Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

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 published 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.

To set up an RDS host, you must complete the following tasks:

1 Prepare Windows Server operating systems for RDS host use. See Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.

2 Install Remote Desktop Services on Windows Server operating systems. See Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019.

3 Install desktop experience on Windows Server operating systems. See Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019.

4 Restrict users to a single session. See Restrict Users to a Single Session.

5 Install Horizon Agent on an RDS host. See Install Horizon Agent on a Remote Desktop Services Host .

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. Do not create published desktop pools and application pools on the same farm 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 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 Horizon Console 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 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.

Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use

To use a Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 machine as an RDS host, you must perform certain steps before you install Horizon Agent in the virtual machine.

When the Remote Desktop Session Host (RDSH) role is not present, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or desktop mode. If RDS mode is selected, the installer will install the RDSH role as well as the Desktop Experience role for the supported operating systems and prompt you to reboot the system. At this time the installer has not yet installed Horizon Agent. After rebooting the system you must run the installer again to continue installing Horizon Agent in RDS mode.

When the Remote Desktop Session Host role is present, the Horizon Agent installer does not display these options. The installer treats the Windows Server machine as an RDS host instead of a single-session Horizon desktop and installs Horizon Agent in RDS mode. During this installation, the Horizon Agent installer will not automatically install the Desktop Experience role. If you need the Desktop Experience role, you must install the role manually. See Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019.

Note The Desktop Experience Role is required for the following features:

- HTML Access
- Scanner redirection
- Windows Aero

For Windows Server 2012 R2, if the Horizon Agent installer does not find an RDSH role and you select RDS mode, then the Horizon Agent installer will automatically install the Desktop Experience role with the RDSH role. You do not have to explicitly install the Desktop Experience role. Windows Server 2016 and later do not have a separate installable Desktop Experience role. The Desktop Experience option is available only during the OS installation, so the Horizon Agent installer installs the RDSH role on Windows Server 2016 and later.

Prerequisites

- Verify that the RDS host is part of the Active Directory domain for the Horizon deployment.
- Familiarize yourself with the steps to install the Desktop Experience feature on supported Windows Server operating systems. See Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019.
- On Windows Server 2016 machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur. See Configure the Windows Firewall Service to Restart After Failures in the *Setting Up Virtual Desktops in Horizon* document.
- 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-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.
3. Accept the VMware license terms.

4 Select **RDS mode** to install the RDSH role and/or the Desktop Experience role. After it is installed, the installer will prompt you to restart the system. After the system is restarted, launch the installer again to continue installing Horizon Agent in RDS mode.

5 On Windows Server 2012 R2 or Windows Server 2016 machines, configure the Windows Firewall service to restart after failures occur.

What to do next

Install Horizon Agent on the remote desktop services host. See Install Horizon Agent on a Remote Desktop Services Host .

Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019

Remote Desktop Services is one of the roles that a Windows Server 2012 R2, 2016, or 2019 can have. You must install this role to set up an RDS host.

To use a Windows Server machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.

Prerequisites

- Verify that the RDS host is running a supported Wiindows Server version.
- Verify that the RDS host is part of the Active Directory domain for the Horizon 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 Remote Desktop Services, Role Services page, select the **Remote Desktop Session Host** role and accept the prompts to add in the additional features required to support the Desktop Session Host role.

9 Follow the prompts to finish the installation.

10 Restart the Windows server.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature.

Restrict users to a single desktop session. See Restrict Users to a Single Session.

Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019

For published desktops and applications, and for virtual 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.

Note A Windows Server 2016 and Windows Server 2019 installation with the Desktop Experience option installs the standard user interface and all tools, including the client experience and the desktop experience features. For Windows Server 2012 RS, the client experience and desktop experience features require a separate installation. For Windows Server 2016 or Windows Server 2019 installation, select **Windows Server 2016** or **Windows Server 2019** or **Windows Server (Server with Desktop Experience)**. If you do not make a choice in the Setup wizard, Windows Server 2016 or Windows Server 2019 is installed as the Server Core installation option. You cannot switch between the installation options. If you install **Windows Server (Server with Desktop Experience)**, and later decide to use **Windows Server 2016** or **Windows Server 2019**, you must perform a fresh installation of Windows Server 2016 or Windows Server 2019.

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 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 2012 R2, Windows Server 2016, or Windows Server 2019, you can restrict users to a single session in a group policy setting.

Procedure

1 In the folder `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections`, Click **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.

2 Enable the group policy setting `Restrict Remote Desktop Services users to a single Remote Desktop Services session`.

What to do next

Install Horizon Agent on the RDS host. See Install Horizon Agent on a Remote Desktop Services Host.

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. Do not create published desktop pools and application pools on the same farm so that desktop sessions are not affected.

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

- Verify that you have prepared Active Directory. See the *Horizon Installation* document.
- To use a Windows Server virtual machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.
- Install the Remote Desktop Services role described in Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019.
- Restrict users to a single desktop session. See Restrict Users to a Single Session.
- Familiarize yourself with the Horizon Agent custom setup options. See Horizon Agent Custom Setup Options for an RDS Host.
- 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-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number and *xxxxxx* is the build number.

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

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

4 Select your custom setup options.

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

Horizon Agent installer prompts this step only if you are installing Horizon Agent on an RDS host that will be in a manual farm. 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 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 and Managing Farms.

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, see Modify Installed Components with the Horizon Agent Installer.

Table 3-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment

Option	Description
USB Redirection	Gives users access to locally connected USB storage devices. This setup option is not selected by default. You must select the option to install it. For information about using USB redirection securely, see the *Horizon Security* document. For example, you can use group policy settings to disable USB redirection for specific users. For information about using the USB redirection feature, and USB device type limitations, see "Using USB Devices with Remote Desktops and Applications" in the *Configuring Remote Desktop Features in Horizon* document.
HTML Access	Enables users to connect to published desktops and published 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 enable users to make connections with HTML Access
3D RDSH	Provides 3D graphics support to applications that run on this RDS host.
Client Drive Redirection	Enables Horizon Client users to share local drives with their published desktops and published applications. After this setup option is installed, no further configuration is required on the RDS host.
Help Desk Plugin for Horizon Agent	You must have a Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon to use the Help Desk Tool. This option is installed and enabled by default.
Horizon Monitoring Service Agent	Enables Horizon Monitoring Agent, which is used to provide metrics to Cloud Monitoring Service (CMS).
Scanner Redirection	Redirects scanning devices that are connected to the client system so that they can be used on the published desktop or published 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.
Serial Port Redirection	Redirects serial COM ports that are connected to the client system so that they can be used on the published desktop or published application. This 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.
Horizon Performance Tracker	Monitors the performance of the display protocol and system resource usage. This option is not selected by default. You must select the option to install it. .NET Framework 4.0 or later is required if you install Horizon Performance Tracker.
VMware Integrated Printing	Enables users to print to any printer available on their client machines. Location-based printing is supported. VMware Integrated Printing is supported on the following remote desktops and applications: ■ Virtual desktops deployed on Windows Server operating systems or Windows Client operating systems. ■ Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines

Table 3-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment (continued)

Option	Description
Hybrid Logon	Provides unauthenticated access users access to network resources without the need to enter credentials. This setup option is not installed by default. You must select the option to install it.
Geolocation Redirection	Enables the Geolocation Redirection feature. This option is not selected by default. You must select the option to install it.

Seome remote experience features are installated automatically on an RDS host.

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

Feature	Description
PCoIP Agent	Enables users to use the PCoIP display protocol to connect to applications and published desktops.
Windows Media Multimedia Redirection (MMR)	Provides multimedia redirection for published desktops. This feature delivers a multimedia stream directly to the client computer, which enables the multimedia stream to be processed on the client hardware instead of on the remote ESXi host.
Unity Touch	Enables 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.
HTML5 Multimedia Redirection	Redirects HTML5 multimedia content in a Chrome or Edge browser to the client for performance optimization.
Browser Redirection	Renders a website on the client system instead of the agent system, and displays the website over the remote browser's viewport, when a user uses the Chrome browser in a remote desktop.

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 *Horizon Architecture Planning* document.

Modify Installed Components with the Horizon Agent Installer

Horizon Agent installer allows you to modify already installed components without needing to uninstall and reinstall Horizon Agent.

You can run Horizon Agent installer on a virtual machine where Horizon Agent is already installed to modify, repair, or remove previously installed components. You can also change custom setup options silently using the command line.

Note You cannot swtich between installation types, such as managed to unmanaged machines. You also cannot modify Instant Clone Agent (NGVC).

Procedure

1 To start the Horizon Agent installation program, double-click the installer file. The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

   You can also use the **Uninstall or change a program** in the Control Panel: Click **VMware Horizon Agent**, then click **Change**.

2 Select **Modify** from these three options:

   - Modify: add or remove the components that are installed.
   - Repair: fix missing or corrupt files, shortcuts, and registry entries.
   - Remove: remove Horizon Agent from the computer.

3 Select or deselect features to add or remove them from the list.

4 Follow the prompts to finish the installation.

5 Restart the system for the changes to take effect.

What to do next

You can confirm the components that were removed (Absent) or added (Local) in the registry located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Installer\Features_HorizonAgent`.

Silent Installation Properties for Horizon Agent

You can include specific properties when you silently install Horizon Agent from the command line. You must use a *`PROPERTY=value`* format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

The following table shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 3-3. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
`INSTALLDIR`	Path and folder in which the Horizon Agent software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	`%ProgramFiles%\VMware\VMware View\Agent`
`RDP_CHOICE`	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting disabled. This MSI property is optional.	1
`SUPPRESS_RUNONCE_CHECK`	Ignores pending Windows Update tasks scheduled at the next operating system reboot in `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` and `RunOnceEx` keys. Using this flag allows concurrent installation but does not guarantee the installation outcome when the system updates affect the Horizon Agent run-time dependencies. This MSI property is optional.	None
`URL_FILTERING_ENABLED`	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection in the *Configuring Remote Desktop Features in Horizon* document. This MSI property is optional.	0
`VDM_SKIP_BROKER_REGISTRATION`	A value of 1 skips unmanaged desktops.	None
`VDM_VC_MANAGED_AGENT`	Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required. **Note** The installer repair option is not supported for an unmanaged installation. Repairing such an installation will result in an installation of a managed Horizon Agent.	None
`VDM_SERVER_NAME`	Host name or IP address of the Connection Server instance on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: `VDM_SERVER_NAME=10.123.01.01` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None

Table 3-3. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
`VDM_SERVER_USERNAME`	User name of the administrator on the Connection Server instance. This MSI property applies only to unmanaged desktops. For example: `VDM_SERVER_USERNAME=domain\username` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
`VDM_SERVER_PASSWORD`	Connection Server administrator user password. For example: `VDM_SERVER_PASSWORD=secret` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
`VDM_IP_PROTOCOL_USAGE`	Specifies the IP version that Horizon Agent uses. Valid values are IPv4 and IPv6.	IPv4
`VDM_FIPS_ENABLED`	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will abort.	0
`VDM_FORCE_DESKTOP_AGENT`	If you install Horizon Agent on a Windows Server machine and configure it as a single-user Horizon desktop rather than as an RDS host, set the value to 1. This requirement applies to machines that are managed by vCenter Server and unmanaged machines. For non-server Windows guests that host application sessions, set the value to 0. This MSI property is optional.	0

In a silent installation command, you can use the `ADDLOCAL` property to specify options that the Horizon Agent installer configures.

The following table shows the Horizon Agent options that you can type at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation.

For more information about the custom setup options, see Horizon Agent Custom Setup Options for an RDS Host.

When you do not use the `ADDLOCAL` property at the command line, Horizon Agent installs all of the options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use `ADDLOCAL=ALL`, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system, except NGVC. NGVC and SVIAgent are mutually exclusive. To install NGVC, you must specify it explicitly.

For more information, see the `ADDLOCAL` table entry in "Microsoft Windows Installer Command-Line Options" in *Setting Up Virtual Desktops in Horizon*

If you use `ADDLOCAL` to specify features individually (you do not specify `ADDLOCAL=ALL`), you must always specify `Core`.

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties. Use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the ModifyPath base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* |
        Select-Object DisplayName, ModifyPath | Where-Object {$_.DisplayName -eq 'VMware
Horizon
        Agent'} | Format-Table –AutoSize
```

The output:

```
DisplayName                ModifyPath
          VMware Horizon Agent      MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}
```

The following example modifies and removes the USB component from an existing installation: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"`

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker”`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection”`

Table 3-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
Core	The core Horizon Agent functions. If you specify `ADDLOCAL=ALL`, the Core features are installed.	Yes
BlastProtocol	VMware Blast	Yes
PCoIP	PCoIP Protocol Agent	Yes
USB	USB Redirection	No
NGVC	Instant Clone Agent	Yes
RTAV	Real-Time Audio-Video	Yes
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
GEOREDIR	Geolocation Redirection	No

Table 3-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
V4V	Horizon Monitoring Service Agent	Yes
SmartCard	PCoIP Smartcard This feature is not installed by default in an interactive installation.	No
VmwVaudio	VMware Audio (virtual audio driver)	Yes
VmVideo	VMware Video (virtual video driver)	Yes
VmwVidd	VMware Indirect Display Driver	Yes
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes
RDP	Enables RDP in the registry if you use the `RDP_CHOICE=1` property on the command line or select RDP as the default display protocol when you create or edit a desktop pool. This feature is hidden during interactive installations.	Yes
VMWMediaProviderProxy	VMware Virtualization Pack for Skype for Business	No
RDSH3D	3D rendering on RDS hosts	No
BlastUDP	UDP Transport support for Blast	Yes
SdoSensor	SDO Sensor Redirection	No
PerfTracker	Horizon Performance Tracker	No
HelpDesk	Horizon Help Desk Tool	No
PrintRedir	VMware Integrated Printing	Yes
UnityTouch	Unity Touch	Yes
PSG	This feature sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.	Yes

Enable Time Zone Redirection for Published 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 a published 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 published 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.
- Verify that the Horizon 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* document.
- Familiarize yourself with the group policy settings. See " RDS Device and Resource Redirection Settings" in the *Configuring Remote Desktop Features in Horizon* 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 > Remote Desktop 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. HorizonHorizon 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.

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.

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 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.

Table 3-5. Performance Options Disabled by Horizon

Performance Options Disabled by Horizon
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 correspond to four Horizon settings in the registry. The following table shows the Horizon 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 registry values to **`false`**.

Table 3-6. Horizon Settings Related to Windows Performance Options

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

RDS Host Printing Options

Horizon supports both local printer redirection and native network printers.

Local printer redirection is designed for the following use cases:

- Printers directly connected to USB or serial ports on the client device.
- Specialized printers such as bar code printers and label printers connected to the client.
- Network printers on a remote network that are not addressable from the virtual session.

Network printers are managed using corporate print servers, which allows for greater management and control of printer resources. Native printer drivers for all possible printers need to be installed on the virtual machine or RDSH host. If you consider this challenging, there are third-party options such as advanced versions of ThinPrint that can provide network printing without the need to install additional printer drivers on each virtual machine or RDSH host. The Print and Document Services option included with Microsoft Windows Server is another option for managing your network printers.

When users submit print jobs concurrently from published 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.

Configuring 3D Graphics for RDS Hosts

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

Horizon supports several 3D Graphics options for RDS hosts. Note that the options differ based whether your RDS hosts are vSphere virtual machines (automated or manual farm), non-vSphere virtual machines, or physical RDS.

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.

For details on 3D graphics support for automated farm of RDS hosts using instant clones, see Configuring 3D Rendering for Automated Instant Clone Farms.

For details on 3D graphics support for manual farm of RDS hosts, see 3D Graphics Options for Manual Farms.

Understanding RDS Per-Device Client Access Licensing in Horizon

When a Windows client device connects to a published desktop or application on an RDS host, it receives an RDS Per-Device Client Access License (CAL), if the Per-Device licensing mode is configured on the RDS host.

By default, the CAL is stored only on the client device.

Note Storage of Per-Device CALs is supported only on Windows clients. Windows Zero clients, and non-Windows clients, do not support this feature. For clients that do not support this feature, CALs are stored only on the Connection Server host.

Storing the CAL makes CAL use more efficient in RDS deployments and prevents the following problems.

- If you deploy multiple license servers, and users run multiple sessions from a client device that connects to different RDS hosts that use different license servers, each license server can potentially issue a separate RDS Per-Device CAL to the same client device.

Considerations for Cloud Pod Architecture Environments

A typical Cloud Pod Architecture environment consists of multiple pods. Each pod can point to a different license server, and a single client device can use published desktops and applications on different pods in the pod federation.

If the client device has a license, it always presents that license. If the client device does not present a license, the most up-to-date license that can be found on any pod involved in the published desktop or application launch is used. If a license cannot be found on any pod involved in the launch, the client device's ID is presented to the license server and a license is issued.

Note VMware recommends that you upgrade to the latest Windows client and server software for the best handling of RDS licensing.

Creating and Managing Farms 4

A farm is a group of Windows Remote Desktop Services (RDS) hosts. You can create published desktops associated with a farm. 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.

Farms simplify the task of managing RDS hosts, published 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.

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 an internal parentVM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parentVM and are created using the vmFork technology.

Although helpful in speeding up the provisioning speed, the use of parentVM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon automatically chooses to provision instant clones directly from replicaVM, without creating any parentVM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parentVMs.

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

For more information on farms, see the *Horizon Administration* document.

This chapter includes the following topics:

Creating an Automated Instant-Clone Farm

An automated farm consists of RDS hosts that are instant-clone virtual machines in vCenter Server. There is no other cloning technology available for automated farms.

An automated instant-clone farm created from a golden image using the vmFork technology (called instant clone API) in vCenter Server. Instant clone technology replaces View Composer linked clone as the process for creating automated farms in Horizon. In addition to using the instant clone API from vCenter Server, Horizon also creates several types of internal VMs (Internal Template, Replica VM, and ParentVM) in order to manage these clones in a more scalable way.

Although helpful in speeding up the provisioning speed, the use of parentVM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon automatically chooses to provision instant clones directly from replicaVM, without creating any parentVM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parentVMs.

When parentVM is used, instant clones share the virtual disk of the parentVM and therefore consume less storage than full VMs. In addition, instant clones share the memory of the parentVM when they are first created, which contributes to fast provisioning. Once the instant clone VM is provisioned and the machine starts to be used, additional memory is utilized.

An instant-clone desktop farm has the following benefits:

- The provisioning of instant clones is fast, with or without using parentVM.
- Instant clones are always created in a powered-on state, ready for use.
- You can patch a farm of instant clones in a rolling process with zero downtime.

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 parentVM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parentVM and are created using the vmFork technology.

Before you create an automated instant-clone farm, you must prepare an RDS host golden image virtual machine. See Prepare an RDS Host Golden Image Virtual Machine.

Instant Clone Image Publishing and Creation Workflow for Farms

Publishing an image is a process by which internal VMs needed for instant cloning are created from a golden image and its snapshot. This process only happens once per image and may take some time.

Horizon performs the following steps to create a pool of instant clones:

1 Horizon publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`,

ClonePrepReplicaVmFolder, and ClonePrepResyncVmFolder) are created if they do not exist, and some internal VMs that are required for cloning are created. In Horizon Console, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

Note Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes. If there are no internal VMs in all four folders, these folders are unprotected and you can delete these folders.

2 After the image is published, Horizon creates the instant clones.. This process is fast. During this process, the Current Image pane in Horizon Console shows the name and state of the image.

After the farm is created, you can change the image through the push-image operation. As with the creation of a farm, the new image is first published. Then the clones are recreated.

When an instant clone pool farm is created, Horizon spreads the pool across datastores automatically in a balanced way. If you edit a farm to add or remove datastores, rebalancing of the cloned VMs happens automatically when a new clone is created.

Preparing a Golden Image Virtual Machine for an Automated Farm

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

- Prepare an RDS Host Golden Image Virtual Machine

  Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

- Disable Windows Hibernation in the Golden Image

  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 virtual disk.

Prepare an RDS Host Golden Image Virtual Machine

Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

Prerequisites

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

- To create an automated instant-clone farm, you must select the **Instant Clone** option when you install Horizon Agent on the golden image virtual machine. See Install Horizon Agent on a Remote Desktop Services Host.
- 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 Console. See *Add an Instant-Clone DomainAdministrator* in the *Horizon Installation* document.
- To deploy Windows machines, configure a volume license key and activate the golden image virtual machine's operating system with volume activation. See " Activating Windows on Instant Clones" in the *Setting Up Virtual Desktops in Horizon* 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 golden image virtual machine.

Procedure

- Verify that the system disk contains a single volume.
- 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.
- Before you take a snapshot of the golden image virtual machine, disable searching Windows Update for device drivers.
- In vSphere Client, disable the vApp Options setting on the golden image virtual machine.
- On 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"`

What to do next

Use vSphere Client to take a snapshot of the golden image virtual machine in its powered-down state.

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

Disable Windows Hibernation in the Golden Image

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 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 golden image 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 an Automated Instant-Clone Farm in Horizon

When you create an automated instant-clone farm, you can configure certain settings.

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **Microsoft RDP**. Microsoft RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **Microsoft 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 published desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is **Yes**.	
3D Renderer	Select 3D graphics rendering for desktops. NVIDIA GRID vGPU is the only 3D rendering option offered for automated farm of instant clone RDS hosts.	

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Pre-launch session timeout (applications only)	Determines the amount of time that an application configured for pre-launch is kept open. The default is **10 minutes**. If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out. If you want to end the pre-launch session after timeout, you must set the **Log off disconnected session** option to **Immediate**.	
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**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs off or disconnects within 30 seconds. You can further reduce the time the session logs off or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session log off to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session log off to 5 seconds.	
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 sessions	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**.	
Bypass Session Timeout	Enable this setting to allow application sessions to run forever. Application sessions that run forever are supported on Windows and Linux clients. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Allow Session Collaboration	Select **Enabled** to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.	
Max sessions per RDS Host	Determines the maximum number of sessions that an RDS host can support. Select **Unlimited** or **No More Than ...**. The default is **Unlimited**.	
Load Balancing	See Load Balancing Settings for the list of settings.	
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 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 VMware vSAN	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	
Select separate datastores for replica and OS disks	(Available only if you do not use vSAN) 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.	
Golden image	Select a golden image virtual machine from the list.	

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Snapshot	Select the snapshot of the golden image virtual machine to use as the base image for the farm. Do not delete the snapshot and golden image 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 golden image virtual machine and snapshot to provision new instant clones in the farm, according to farm policies. The golden image 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.	
Cluster	Select the ESXi host or cluster on which the desktop virtual machines run. For the maximum limit on the cluster, see the KB article on Sizing Limits and Recommendations.	
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. **Note** If you use vSAN, there is 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.	

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
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 farm. The default setting uses the network from the current golden image. The **Select Networks** wizard provides a list of networks based on the golden image network type: DVS, NSX-T, VDS, and Standard. To use multiple networks, you must unselect **Use network from current golden image** and then select the networks to use with the instant-clone farm. The **Show All Networks** switch shows or hides (greys out) incompatible networks within the selected network type. By default, only compatible networks are shown. If you select an incompatible network, such as vmcNetworks, you see this error message: **This network belongs to VMC internal network**. The wizard also provides the list of ports and port bindings that are available to use: static (early binding) and ephemeral. All selected NSX-T or VDS network segments must be the same size, such as all /24 networks. Unequal sized segments can result in provisioning errors.	
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.	
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.	
Allow reuse of pre-existing computer accounts	Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names. When an instant clone is created, if an existing AD computer account name matches the instant-clone virtual machine name, Horizon 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 AD container setting. When this option is disabled, a new AD computer account is created when Horizon creates an instant clone. This option is disabled by default.	

Table 4-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Image Publish Computer Account	Publishing instant-clones requires an additional computer account in the same AD domain as the clones. If you want to use pre-created computer accounts instead of auto-created computer accounts, you must also create the additional computer account and specify its name here. Then you do not need to delegate Create and Delete of computer objects to the provisioning account.	
Use ClonePrep or a customization specification (Sysprep)	Choose whether to use ClonePrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the 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 golden image 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 golden image 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. After you use ClonePrep or Sysprep when you create a farm, you cannot switch to the other customization method later on, when you create or recompose machines in the farm. After you use ClonePrep or Sysprep when you create a farm, you can edit the customization type or spec name. Changes to the customization spec are not reflected on the farm until a new push image is scheduled, and the currently published image continues to use the old spec even if it has been edited or deleted. If push image fails, the farm continues using the old unedited spec. However, the farm settings continue to point to the new spec name if it has been changed.	
Ready to Complete	Review the settings for the automated instant-clone farm.	

Create an Automated Instant-Clone Farm in Horizon

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

Prerequisites

- Verify that Connection Server is installed. See the *Horizon Installation* document.

- Verify that Connection Server settings for vCenter Server are configured in Horizon Console. See the *Horizon 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 golden image virtual machine. Horizon Agent must be installed on the golden image virtual machine. See Preparing a Golden Image Virtual Machine for an Automated Farm.
- Take a snapshot of the golden image virtual machine in vCenter Server. You must shut down the golden image 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 in Horizon.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click **Add**.
3. Select **Automated Farm**.
4. Select **Instant clone**.
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.

What to do next

Create a published application pool or a published desktop pool. See Create an Application Pool or Create a Published Desktop Pool.

Configuring 3D Rendering for Automated Instant Clone Farms

When you create or edit a farm of instant clone RDS machines, you can configure 3D graphics rendering for your farm. Instant clone farms support NVIDIA GRID vGPU for 3D rendering.

Horizon does not directly control settings for 3D rendering of an instant-clone farm as it does with full-clone virtual machines. You need to configure 3D settings in the ESXi hosts, and then in your golden image using the vSphere Client. Instant-clone virtual machines will inherit those settings from the golden image. Horizon Console will display some of the settings you configured, but you cannot edit or interact with those settings.

The ESXi host assigns GPU hardware resources to virtual machines on a first-come, first-served basis as virtual machines are created. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is the **best performance** mode. If you would rather have 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, you can use the **GPU consolidation** mode. You can configure this mode in vCenter Server for each ESXi host that has vGPU installed. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/55049.

If you are only using a single vGPU profile per vSphere cluster, set the GPU assignment policy for all GPU hosts within the cluster to the **best performance** mode in order to maximize performance. In this case, you can also have instant-clone pools and full-clone pools that use the same vGPU profile in the same vSphere cluster.

You can have a cluster with some GPU enabled hosts and some non-GPU enabled hosts.

NVIDIA GRID vGPU has these potential constraints:

- RDP is not supported.
- The virtual machines must be hardware version 11 or later.
- vMotion of a VM between vGPU-enabled hosts is supported starting with vSphere 6.7. You cannot use vSphere Distributed Resource Scheduler (DRS) with vGPU.
- Horizon does support creating a vGPU instant-clone farm using a cluster with some vGPU enabled hosts and non-vGPU enabled hosts, and will just ignore the non-vGPU enabled hosts when creating the farm. You can not use vMotion to move an instant-clone from a GPU-enabled ESXi host to an ESXi host that does not have GPU hardware configured.

To enable an instant-clone farm to use NVIDIA GRID vGPU:

Procedure

1. Install NVIDIA GRID vGPU in the physical ESXi hosts.
2. In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared Direct**.

   ESXi host uses the NVIDIA GRID card for vGPU.
3. Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile you want to use.
4. Take a snapshot of the golden image.
5. In Horizon Console, when you create an instant-clone farm, select this golden image and snapshot.

Results

Horizon automatically displays **NVIDIA GRID vGPU** in the 3D Render field. Horizon also displays the vGPU profile you chose in the golden image. Instant clones inherit the settings configured in the vSphere Client for the golden image.

The vGPU profile cannot be edited from Horizon Console during the instant-clone farm creation process, To edit the vGPU profile for a farm once the farm has been created, you can create a new image with the updated vGPU profile, take a snapshot, and then do a push-image operation. For information on push-image operations, see the *Setting Up Virtual Desktops in Horizon* document.

Creating a Manual Farm

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical, vSphere virtual machines (excluding instant clones), or non-vSphere virtual machines.You manually add the RDS hosts when you create the farm.

Before you create a manual farm, you must prepare existing RDS hosts for Horizon. See Chapter 3 Setting Up Remote Desktop Services Hosts.

Worksheet for Creating a Manual Farm in Horizon

When you create a manual farm, you can configure certain farm settings.

Table 4-2. Worksheet: Configuration Settings for Creating a Manual Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **Microsoft RDP**. Microsoft RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **Microsoft 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 published desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is **Yes**.	
Pre-launch session timeout (applications only)	Determines the amount of time that an application configured for pre-launch is kept open. The default is **10 minutes**. If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out. If you want to end the pre-launch session after timeout, you must set the **Log off disconnected session** option to **Immediate**.	

Table 4-2. 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**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs off or disconnects within 30 seconds. You can further reduce the time the session logs off or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session log off to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session log off to 5 seconds.	
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 sessions	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**.	
Bypass Session Timeout	Enable this setting to allow application sessions to run forever. Application sessions that run forever are supported on Windows and Linux clients. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	
Allow Session Collaboration	Select **Enabled** to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and collaborators must use the VMware Blast protocol.	

Table 4-2. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon does not consider other load balancing settings and reads the `CustomLoadValue` registry key in the following location to get the server load index: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. See, Writing a Load Balancing Script for an RDS Host.	
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.	
Select RDS Hosts	Select the RDS host from the list.	
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Memory usage threshold	Threshold value for the memory in percentage. Horizon uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.	
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	

Create a Manual Farm in Horizon

Create a manual farm as part of the process to give users access to published applications or desktops.

Prerequisites

- Set up the RDS hosts that belong to the farm. See Chapter 3 Setting Up Remote Desktop Services Hosts.
- Verify that all the RDS hosts have the Available status. In Horizon Console, select **Settings > 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 in Horizon.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click **Add**.

3 Select **Manual Farm**.

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

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

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

6 Click **Finish**.

What to do next

Create a published application or desktop pool.

3D Graphics Options for Manual Farms

3D graphics options are available for a manual farm of RDS using vSphere virtual machines.

These options are applicable to vSphere virtual machines. If you have a manual farm of non-vSphere virtual machines or physical servers, you can leverage GPU capabilities that are available to the OS.

NVIDIA GRID vGPU (shared GPU hardware acceleration)

A physical GPU on an ESXi host is shared among multiple virtual machines.

AMD Multiuser GPU using vDGA

A physical GPU on an ESXi host is shared among multiple virtual machines.

Virtual Dedicated Graphics Acceleration (vDGA)

A physical GPU on an ESXi host is dedicated to a single virtual machine.

Note 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.

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.

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 or virtual machines. 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"
```

Overview of Steps for Configuring 3D Graphics

This overview describes tasks that you must perform in vSphere and Horizon 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.

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 a published 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 Horizon Console. Selecting the option **3D RDSH** when you install Horizon Agent is sufficient. By default, this option is not selected and 3D graphics is disabled.

Managing Farms

In Horizon Console, you can add, edit, delete, enable, and disable farms.

After you create a farm, you can add or remove RDS hosts to support more or fewer users.

Edit a Farm

For an existing farm, you can make changes to the configuration settings.

Prerequisites

Familiarize yourself with the settings of a farm.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select a farm and click **Edit**.

3 Make changes to the farm settings.

4 Click **OK**.

Delete a Farm

You can delete a farm if you no longer need it or if you want to create a new one with different RDS hosts. You can only delete a farm that is not associated with published desktop or application pool.

Prerequisites

Verify that the farm is not associated with any published desktop pool or application pool.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select one or more farms and click **Delete**.

3 Click **OK** to confirm.

Disable or Enable a Farm

When you disable a farm, users can no longer launch published desktops or applications from the published desktop pools and the application pools that are associated with the farm. Users can continue to use published desktops and applications that are currently open.

You can disable a farm if you plan to do maintenance on the RDS hosts in the farm or on the published desktop and application pools that are associated with the farm. After you disable a farm, some users might still be using published desktops or applications that they opened before you disable the farm.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Select one or more farms and click **More Commands**.
3. Click **Enable** or **Disable**.
4. Click **OK** to confirm.

Results

You can view the status of the pools by selecting **Inventory > Desktops** or **Inventory > Applications**.

Schedule Maintenance for an Automated Instant-Clone Farm in Horizon

With the maintenance operation, you can schedule recurring or immediate maintenance of all the RDS hosts in an automated instant-clone farm. During each maintenance cycle, all the RDS hosts are refreshed from the golden image virtual machine.

You can make changes to the golden image virtual machine without affecting the RDS host instant clones because the snapshot of the current golden image VM is used for maintenance. The instant clones created in the automated farm use the information in the golden image VM for their system configuration.

You can schedule maintenance on an automated farm but not on individual RDS hosts in the farm.

If possible, schedule maintenance operations during off-peak hours to ensure all that RDS hosts have finished maintenance and are available during peak hours.

Prerequisites

- Decide when to schedule the maintenance operation. By default, Connection Server starts the operation immediately.

  You can schedule an immediate maintenance or recurring maintenance or both for a farm. You can schedule maintenance operations on multiple farms concurrently.

- Decide whether to force all users to log off when the maintenance operation begins or wait for each user to log off before refreshing that user's machine.

  If you force users to log off, Horizon notifies users before they are disconnected and allows them to close their applications and log off.

- Decide the minimum farm size. The minimum farm size is the number of RDS hosts that are kept available at all times to allow users to continue to use the farm. For example, if the farm size is ten and the minimum farm size is two, then maintenance will be performed on eight RDS hosts. As each RDS host becomes available again then the remaining hosts will go through maintenance. All RDS hosts are managed individually, so as one host becomes available then one of the remaining hosts will be put into maintenance.

However, if you schedule immediate maintenance, then all the RDS hosts in the farm will be put into maintenance.

All RDS hosts will also be subject to policy and will wait for logoff or force users to logoff depending upon what policy is configured.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when Connection Server provisions an instant-clone, provisioning stops. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

  Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on an instant-clone, other clones continue to be provisioned and customized.

- Verify that provisioning is enabled. When provisioning is disabled, Horizon stops the machines from being customized after they are refreshed.

- If your deployment includes replicated Connection Server instances, verify that all instances are the same version.

Procedure

1. In Horizon Console, select **Inventory > Farms**.

2. Click the pool ID of the farm for which you want to schedule a maintenance.

3. Click **Maintain > Schedule**.

4 In the **Schedule Recurring Maintenance** wizard, choose a maintenance mode.

◆

Option	Action
Recurring	Schedules periodic maintenance of all the RDS host servers in a farm. ■ Select a date and time from which the maintenance is effective. ■ Select a maintenance period. You can select daily, monthly, or weekly maintenance periods. ■ Select a repeat interval in days for the maintenance operation to recur. If an immediate maintenance is scheduled on a farm, then the immediate maintenance date becomes the effective date for any recurring maintenance. If you cancel the immediate maintenance, then the current date becomes the effective date for recurring maintenance.
Immediate	Schedules immediate maintenance of all the RDS host servers in a farm. Immediate maintenance creates a one-time maintenance schedule for immediate or near future maintenance. Use immediate maintenance to refresh the farm from a new golden image VM or snapshot when you want to apply urgent security patches. Select an immediate maintenance configuration. ■ Select **Start Now** to start the maintenance operation instantly. ■ Select **Start at** to start the maintenance operation at a near future date and time. Enter the date and Web browser local time. **Note** Recurring maintenance will be put on hold until immediate maintenance is complete.

5 Click **Next**.

6 (Optional) Click **Change** to change the golden image virtual machine.

7 Select a snapshot.

You cannot select a different snapshot unless you clear the **Use current parent VM image** checkbox.

8 (Optional) Click **Snapshot Details** to display details about the snapshot.

9 Click **Next**.

10 (Optional) Specify whether to force users to log off or wait for users to log off.

The option to force users to log off is selected by default.

11 (Optional) Specify whether to stop provisioning at first error.

This option is selected by default.

12 Click **Next**.

The **Ready to Complete** page is displayed.

13 Click **Finish**.

Creating Published Desktop Pools

5

One of the tasks that you perform to give users remote access to session-based desktops is to create a published desktop pool. A published desktop pool runs on a farm of RDS hosts and has properties that can satisfy some specific needs of a remote desktop deployment.

This chapter includes the following topics:

Understanding Published Desktop Pools

An published 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 Horizon releases.

A published desktop pool and a published desktop have the following characteristics:

- A published desktop pool is associated with a farm, which is a group of RDS hosts. The farm can be an automated farm or a manual farm. Each RDS host is a Windows server that can host multiple published desktops.
- A published 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.
- A published desktop supports the RDP, PCoIP, and VMware Blast display protocols.
- A published desktop pool is only supported on Windows Server operating systems that support the RDS role and are supported by Horizon. See "System Requirements for Guest Operating Systems" in the *Horizon Installation* document.
- Horizon 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.

Published Desktop Pools Settings

You can specify certain pool settings when you create an published desktop pool that run on a farm of RDS hosts. Not all pool settings apply to all types of desktop pools. These settings are specific to published desktop pools.

Table 5-1. Settings for a Published Desktop Pool

Setting	Description	Default Value
State	■ **Enabled**. After being created, the desktop pool is enabled and ready for immediate use. ■ **Disabled**. After being created, the desktop pool is disabled and unavailable for use, and provisioning is stopped for the pool. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. When this state is in effect, remote desktops are unavailable for use.	Enabled
Connection Server restrictions	You can restrict access to the desktop pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	None
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices.	Disabled

Table 5-1. Settings for a Published Desktop Pool (continued)

Setting	Description	Default Value
Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	Disabled
Allow user to initiate separate sessions from different client devices	When you enable this setting, users that connect to the same desktop pool from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not select this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. The RDP display protocol is not supported if you select this setting. Default is **No**. **Note** If you enable this policy, all the desktop pools in the global entitlement must also support multiple sessions per user. For more information about understanding the multiple sessions per user policy for global desktop entitlements, see the *Administering Cloud Pod Architecture in Horizon* document.	

Create a Published Desktop Pool

You create a published desktop pool as part of the process to give users access to desktops that run on a farm of RDS hosts.

Prerequisites

- Set up RDS hosts. See Chapter 3 Setting Up Remote Desktop Services Hosts.
- Create a farm that contains the RDS hosts. See Chapter 4 Creating and Managing Farms.
- Decide how to configure the pool settings. See Published Desktop Pools Settings.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Click **Add**.
3. Select **RDS Desktop Pool** and click **Next**.

4 Provide a pool ID, display name, and description.

The pool ID is the unique name that identifies the pool in Horizon Console. The display name is the name of the published 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 an existing farm or create a farm for this pool.

What to do next

Entitle users to access the pool.

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. You must enable the internal VM debug mode before you create an instant clone farm.

Procedure

1 In the vSphere Web Client, select the golden 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 golden 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 golden 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 Connection 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 Connection Server.

For instant clone actions such as prime, provision, resync, or unprime, the internal virtual machines use the value set in the golden virtual machine. If you do not disable the internal VM debug mode, then the VMs remain in vSphere till you delete the VMs. For further debugging on instant clone actions, you can also log in to the internal VM and view the instant clone logs. You can also see the following VMware Knowledge Base articles for further debugging on instant clone actions:

- Differences between VMware ClonePrep, QuickPrep and Microsoft Sysprep (2003797) https://kb.vmware.com/s/article/2003797
- Initial publish of an Instant Clone desktop pool image fails and the template VMs are deleted (2144938) https://kb.vmware.com/s/article/2144938
- Computer-based Global Policy Objects (GPOs) that require reboot are not applied on Instant Clones (2150495) https://kb.vmware.com/s/article/2150495
- How to change SVGA settings for Instant Clone Pools (2151745) https://kb.vmware.com/s/article/2151745

See also "Upgrade Instant-Clone Desktop Pools When You Upgrade vCenter Server to vSphere 6.7 or Later" in the *Horizon Upgrades* document.

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.

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

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 or desktop pool. To avoid errors, you must install the application on all of the RDS hosts in the farm or desktop pool.

When you create an application pool, Horizon 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 or desktop pool. 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 displays a warning message.

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

An application supports the PCoIP and VMware Blast display protocols.

This chapter includes the following topics:

Worksheet for Creating an Application Pool Manually

When you create an application pool and manually specify an application, you can add information about the application. It is not a requirement that the application is already installed on any RDS host.

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

Property	Description	Fill in Your Value Here
Select an RDS Farm or Desktop Pool	Select a farm or a desktop pool from the list of desktops with supported session type Application or Application and Desktop.	
ID	Unique name that identifies the pool in Horizon Console. 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.	
Pre-launch	Select this option to configure an application so that an application session is launched before a user opens the application in Horizon Client. When a published application is launched, the application opens more quickly in Horizon Client. If you enable this option, the configured application session is launched before a user opens the application in Horizon Client, regardless of how the user connects to the server from Horizon Client. If you enable this option on applications published from a desktop with session type Application and Desktop, the desktop session may not be available. **Note** Application sessions can be disconnected when the **Pre-launch session timeout (applications only)** option is set when you add or edit the application farm.	

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

Property	Description	Fill in Your Value Here
Connection Server Restrictions	You can restrict access to the application pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the application pool entitlement on Windows client devices.	

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

Property	Description	Fill in Your Value Here
Client Restrictions	Select whether to restrict access to entitled application pools from certain client computers. You must add the names of the computers that are allowed to access the application pool in an Active Directory security group. You can select this security group when you add users or groups to the application pool entitlement.	
Multi-Session Mode	You can start published application sessions in the following modes: Single-session: If the user opens a published application on client A in single-session mode, and then opens the same published application or another published application based on the same farm on client B then, the session on client A is disconnected and reconnected on client B. Multi-session: If the user opens a published application on client A in multi-session mode, and then opens the same published application or another published application based on the same farm on client B, the published application remains open on client A and a new session of the published application opens on client B. Such sessions are logged off on disconnect. You cannot enable the session pre-launch feature when multi-session mode is enabled. The multi-session mode has the following values: ■ **Disabled**. Multi-session mode is not supported. ■ **Enabled (Default Off)**. Multi-session mode is supported, but it is disabled by default. To use multi-session mode, users must enable the **Multi-Launch** setting in Horizon Client. ■ **Enabled (Default On)**. Multi-session mode is supported, and it is enabled by default. Users can disable multi-session mode by disabling the **Multi-Launch** setting in Horizon Client. ■ **Enabled (Enforced)**. Multi-session mode is always enabled. Users cannot disable it in any version of Horizon Client and the application is always launched in multi-session mode.	

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

Property	Description	Fill in Your Value Here
	When multi-session mode is enabled you can also configure the **max-sessions count** setting. This sets the maximum number of concurrent multi-sessions that can be started by a user for the same published application from different client devices. You can open a published application from a client in both the single-session mode and multi-session mode, which is based on the multi-session mode configuration. In this case, the client has one single-session and one multi-session. Enabling multi-session mode affects how HTML Access behaves when it is started from Workspace ONE. For more information, see the Workspace ONE documentation. For more information about using the **Multi-Launch** setting, see the Horizon Client documentation. **Note** This setting is not supported for applications based on a desktop 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 or a desktop pool.

Prerequisites

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

Procedure

1 In Horizon Console, select **Inventory > Applications**.

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 Horizon Console displays, you can select multiple applications. A separate pool is created for each application.

What to do next

Entitle users to access the pool. You can also view the number of entitled users that are using a published application in the **User Count** column in the application pools page.

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

If you need to ensure that 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.

Note For applications running on desktop pools, the anti-affinity rule is supported only for applications created from floating desktop pools, and not from dedicated desktop pools.

See Configure an Anti-Affinity Rule for an Application Pool in Horizon Console.

Managing Application Pools

You can add, edit, delete, or entitle application pools in Horizon Console.

Edit an Application Pool

You can edit an existing application pool to configure settings such as display name, version, publisher, path, start folder, parameters, and description. You cannot change the ID or access group of an application pool.

Prerequisites

- Familiarize yourself with the settings of an application pool.
- You might need to configure an anti-affinity rule to ensure that Connection Server launches the application only on RDS hosts that have sufficient resources to run the application.

Procedure

1 In Horizon Console, select **Inventory** > **Applications**.

2 Select a pool and click **Edit**.

3 Make changes to the pool settings.

4 Click **OK**.

Delete an Application Pool

When you delete an application pool, users can no longer launch the application in the pool.

You can delete an application pool even if users are currently accessing the application. After the users close the application, they can no longer access the application.

Procedure

1 In Horizon Console, select **Inventory** > **Applications**.

2 Select one or more application pools and click **Delete**.

3 Click **OK** to confirm.

Duplicate an Application Pool

You can duplicate an application pool to create multiple applications that are similar to each other.

When you duplicate an application pool, you can change the application pool ID and description to create a new application pool.

Note If there is an icon for the original application pool, the icon does not get associated with the duplicate application pool. However, you can assign the original icon to the duplicate application pool.

Note If there are user entitlements for the original application pool, the duplicate application pool does not get these entitlements and you must entitle users to the duplicate application pool again.

Procedure

1 In Horizon Console, select **Inventory** > **Applications**.

2 Select an application pools and click **Duplicate**.

3 Enter an application pool ID.

4 (Optional) Enter a display name and a description.

5 Click **OK**.

What to do next

Entitle users to the duplicate application pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Change the Icon of a Published Application

You can customize the icons for published applications for end users. When you change the icon for a published application, the new application icon is available for the end user to view on the published desktop.

Prerequisites

- Verify that the icon is available in the .PNG file format.

Procedure

1 In Horizon Console, select **Inventory** > **Applications**.

2 Select an application pool or multiple application pools and click **Application Icon** > **Associate Application Icon**.

3 To upload an icon, click **Upload Icon File** and browse for an icon in the .PNG format.

The icon file must be between 16x16 pixels and 256x256 pixels.

4 Click **OK**.

Results

The icon appears for the published application on the published desktop.

Remove the Icon of a Published Application

You can remove the icon of a published application to replace it with another icon. When you remove the icon for a published application, the published application is replaced with the default icon on the published desktop. You can remove icons from multiple published applications only if all published applications have the same icon. You cannot select multiple published applications that have different icons to remove an icon.

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Select an application pool or multiple application pools and click **Application Icon > Remove Application Icon**.

Results

The published application is replaced with the default icon on the published desktop.

Enable or Disable an Application Pool

When you enable an application pool, entitled users have access to the application pool. When you disable an application pool, entitled users no longer have access to the application pool. You can enable or disable one or multiple application pools.

Prerequisites

- Verify that you have the **Enable Farms, Desktops and Applications Pools** privilege.

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Select one or more application pools.

3 Choose to enable or disable an application pool or pools.

   - To enable an application pool or pools, click **More > Enable Pool**.
   - To disable an application pool or pools, click **More > Disable Pool**.

4 Click **OK** to confirm.

Configure an Anti-Affinity Rule for an Application Pool in Horizon Console

When you configure an anti-affinity rule for an application pool, Horizon Connection Server attempts to launch the application only on RDS hosts that have sufficient resources to run the application. This feature can be useful for controlling applications that consume large amounts of CPU or memory resources.

An anti-affinity rule consists of an application matching pattern and a maximum count. For example, the application matching pattern might be `autocad.exe` and the maximum count might be 2.

Connection Server sends the anti-affinity rule to Horizon Agent on an RDS host. If any applications running on the RDS host have process names that match the application matching pattern, Horizon Agent counts the current number of instances of those applications and compares the number to the maximum count. If the maximum count is exceeded, Connection Server skips that RDS host when it selects an RDS host to run new sessions of the application.

Prerequisites

- Create the application pool. See Create an Application Pool.
- Become familiar with the constraints of the anti-affinity feature. See Anti-Affinity Feature Constraints.

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Select the pool to modify and click **Edit**.

3 In the **Anti-Affinity Patterns** text box, type a comma-separated list of patterns to match against the process names of other applications running on RDS hosts.

   The pattern string can include the asterisk (*) and question mark (?) wildcard characters. An asterisk matches zero or more characters and a question mark matches any single character.

   For example, **`*pad.exe,*notepad.???`** matches `wordpad.exe`, `notepad.exe`, and `notepad.bat`, but it does not match `wordpad.bat` or `notepad.script`.

   Note Horizon counts multiple patterns that match for an application in a single session as a single match.

4 In the **Anti-Affinity Count** text box, type the maximum number of other applications that can be running on the RDS host before the RDS host is rejected for new application sessions.

   The maximum count can be an integer from 1 to 20.

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

Anti-Affinity Feature Constraints

The anti-affinity feature has certain constraints.

- Anti-affinity rules affect new application sessions only. An RDS host that contains sessions in which a user has previously run an application is always reused for the same application. This behavior overrides reported load preferences and anti-affinity rules.
- Anti-affinity rules do not affect application launches from within an RDS desktop session.
- RDS session limits prevent application sessions from being created, regardless of anti-affinity rules.
- In certain circumstances, the instances of applications on the RDS host might not be restricted to the maximum count that you specify. For example, Horizon cannot determine the exact instance count if other applications for other pending sessions are in the process of being launched.
- Inter-application anti-affinity rules are not supported. For example, large application classes, such as Autocad and Visual Studio instances, cannot be counted in a single rule.
- Do not use anti-affinity rules in environments where end-users use Horizon Client on mobile clients. Anti-affinity rules can result in multiple sessions in the same farm for an end user. Reconnecting to multiple sessions on mobile clients can result in indeterminate behavior.
- Anti-Affinity rules consider only the connected number of sessions for load balancing. However, load balancing for RDS hosts considers the sum of the connected, pending, and disconnected sessions for load balancing.

Managing RDS Hosts and Sessions

7

In Horizon Console, you can perform management operations such as configuring or deleting RDS hosts or manage sessions for published desktops and applications.

This chapter includes the following topics:

- Managing RDS Hosts in Horizon Console
- Monitor RDS Hosts in Horizon Console
- Manage Published Desktop and Application Sessions in Horizon Console
- Configuring Load Balancing for RDS Hosts in Horizon Console

Managing RDS Hosts in Horizon Console

You can perform certain management tasks on the manual or automated farm of RDS hosts you have created. Note that some tasks are applicable to both manual and automated farms, whereas others are only applicable to one type of farm.

When you manually set up an RDS host, it automatically registers with Horizon Connection Server. You cannot separately register an RDS host with Connection Server. For a manual farm, you can perform the following management tasks:

- Edit the RDS host.
- Add the RDS host to a manual farm.
- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

For an automated farm of RDS hosts, you can perform the following management tasks:

- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

Edit an RDS Host in a Manual Farm

You can change the number of connections that an RDS host can support. You can set it to any positive number, or to unlimited.

You can only edit an RDS host that you set up manually, but not an RDS host that is in an automated farm.

Procedure

1. In Horizon Console, select **Settings > Registered Machines**.
2. Select an RDS host and click **Edit**.
3. Specify a value for the setting **Number of connections**.
4. Click **OK**.

Add an RDS Host to a Manual Farm

You can add an RDS host that you set up manually to a manual farm to increase the scale of the farm or for other reasons. You can only add RDS hosts to a manual farm.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click the farm ID.
3. Select the **RDS Hosts** tab.
4. Click **Add**.
5. Select one or more RDS hosts.
6. Click **OK**.

Remove an RDS Host from a Manual or Automated Farm

You can remove an RDS host from a manual farm to reduce the scale of the farm, to perform maintenance on the RDS host, or for other reasons. As a best practice, disable the RDS host and ensure that users are logged off from active sessions before you remove a host from a farm.

If users have application or desktop sessions on hosts that you remove, the sessions remain active, but Horizon does not track them. A user who disconnects from a session will be unable to reconnect to it, and any unsaved data might be lost.

You can also remove an RDS host from an automated farm. One possible reason might be that the RDS host is in an unrecoverable error state.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click the farm ID.

3 Select the **RDS Hosts** tab.

4 Select one or more RDS hosts.

5 Click **Remove from farm**.

6 Click **OK**.

Remove a Registered RDS Host from Horizon

You can remove from Horizon an RDS host that you set up manually and that you no longer plan to use. The RDS host must not currently be in a manual farm.

Prerequisites

Verify that the RDS host does not belong to a farm.

Procedure

1 In Horizon Console, select **Settings > Registered Machines**.

2 Select an RDS host and click **Remove**.

3 Click **OK**.

Results

After you remove an RDS host, to use it again, you must reinstall Horizon Agent.

Disable or Enable an RDS Host in a Manual or Automated Farm

When you disable an RDS host, Horizon no longer uses it to host new published desktops or applications. Users can continue to use published desktops and applications that are currently open.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click the farm ID.

3 Select the **RDS Hosts** tab.

4 Select an RDS host and click **More Commands**.

5 Click **Enable** or **Disable**.

6 Click **OK**.

Results

If you enable the RDS host, a check mark appears in the Enabled column, and Available appears in the Status column. If you disable the RDS host, the Enabled column is empty and Disabled appears in the Status column.

Status of RDS Hosts in Horizon Console

An RDS host can be in various states from the time that it is initialized. As a best practice, check that RDS hosts are in the state that you expect them to be in before and after you perform tasks or operations on them.

Table 7-1. Status of an RDS Host

Status	Description
Startup	Horizon Agent has started on the RDS host, but other required services such as the display protocol are still starting. The agent startup period also allows other processes such as protocol services to start up.
Disable in progress	RDS host is in the process of being disabled while sessions are still running on the host. When the sessions end, the status changes to Disabled.
Disabled	Process of disabling the RDS host is complete.
Validating	Occurs after Connection Server first becomes aware of the RDS host, typically after Connection Server is started or restarted, and before the first successful communication with Horizon Agent on the RDS host. Typically, this state is transient. This state is not the same as the Agent unreachable state, which indicates a communication problem.
Agent disabled	Occurs if Connection Server disables Horizon Agent. This state ensures that a new desktop or application session cannot be started on the RDS host.
Agent unreachable	Connection Server cannot establish communication with Horizon Agent on an RDS host.
Invalid IP	Subnet mask registry setting is configured on the RDS host, and no active network adapters have an IP address within the configured range.
Agent needs reboot	component was upgraded, and the RDS host must be restarted to allow Horizon Agent to operate with the upgraded component.
Protocol failure	The RDP display protocol is not running correctly. If RDP is not running and PCoIP is running, clients cannot connect using either RDP or PCoIP. However, if RDP is running and PCoIP is not running, clients can connect using RDP.
Domain failure	RDS host encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	RDS role is not enabled on the server.
Unknown	RDS host is in an unknown state.
Available	RDS host is available. If the host is in a farm, and the farm is associated with a published desktop or application pool, it will be used to deliver published desktops or applications to users.

Monitor RDS Hosts in Horizon Console

You can monitor the status and view the properties of RDS hosts in both manual and automated farms in Horizon Console.

Procedure

- In Horizon Console, navigate to the page that displays the properties that you want to view.

Properties	Action
DNS Name, Type, Image, Pending Image, Task, Max Number of Connections, Sessions, Agent Version, Enabled, Status	■ In Horizon Console, select **Inventory > Farms**. ■ Select a farm and click the **RDS Hosts** tab.
RDS Host, Farm, Desktop Pool, Agent Version, Sessions, Status	■ In Horizon Console, select **Inventory > Machines**. ■ Click the **RDS Hosts** tab.
DNS Name, Type, RDS Farm, Max Number of Connections, Sessions, Agent Version, Enabled, Status	■ In Horizon Console, select **Settings > Registered Machines**. ■ Click the **RDS Hosts** tab.

Results

The properties are displayed and have the following meanings:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	Published desktop pool associated with the farm.
Agent Version	Version ofHorizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
RDS Farm	Farm to which the RDS host belongs.
Image	Image of the RDS host on the farm.
Pending Image	Pending image of the RDS host on the farm.
Task	Task being performed on the RDS host of the farm.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Manage Published Desktop and Application Sessions in Horizon Console

When a user launches a published desktop or application, a session is created. You can disconnect and log off sessions, send messages to clients, reset, and restart virtual machines.

Procedure

1 In Horizon Console, navigate to where session information is displayed.

Session Type	Navigation
Remote desktop sessions	Select **Inventory > Desktops**, click a pool's ID, and click the **Sessions** tab. The **Sessions** column also appears on the **Desktop Pools** page for all desktops. Select **Inventory > Farms**, click a farm's ID, and click the **Sessions** tab. You can also view the published applications associated with a session. The **Application Names** column displays the published applications associated with a session. The **Sessions** column also appears on the **Farms** page for all farms. Select **Settings > Registered Machines**, and view the **Sessions** column.
Remote desktop and application sessions	Select **Monitor > Sessions**.
Sessions associated with a user or user group	■ Select **Users and Groups**. ■ Click a user's name or a user group's name. ■ Click on the **Sessions** tab.

2 Select a session.

To send a message to users, you can select multiple sessions. You can perform the other operations on only one session at a time. You can perform a log off operation only on a session that is not connected from a vSphere console.

3 Choose whether to disconnect, log off, send a message, restart a desktop, or reset a virtual machine.

Option	Description
Disconnect Session	Disconnects the user from the session.
Logoff Session	Logs the user off the session. Data that is not saved is lost.
Send Message	Send a message to Horizon Client. You can label the message as **Info**, **Warning**, or **Error**.

Option	Description
Restart Desktop	Performs a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. **Note** This option is not available for instant-clone farms.
Reset Virtual Machine	Performs a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine. **Note** This option is not available for instant-clone farms.

4 Click **OK**.

Results

The session properties have the following descriptions:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	RDS desktop pool associated with the farm.
Agent Version	Version of Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
Client ID	Name or the MAC address of the client.
Client Version	Version of Horizon Client for the user's session.
RDS Farm	Farm to which the RDS host belongs.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Configuring Load Balancing for RDS Hosts in Horizon Console

You can configure load balancing for RDS hosts by configuring load balancing settings in Horizon Console or by creating and configuring load balancing scripts.

By default, Connection Server uses the following formula to balance the placement of published desktop and application sessions on RDS hosts:

```
(connected sessions + pending sessions + disconnected sessions)/(maximum session count)
```

If the maximum session count is configured as unlimited, load balancing falls back to using the absolute number of the total session count which includes connected, pending and disconnected sessions.

Load Balancing Settings in Horizon Console

You can configure load balancing settings for a farm in Horizon Console to control the placement of published desktop and application sessions. See, Load Balancing Settings.

Load Balancing Scripts

You can also override the default behavior of the load balancing settings and control the placement of new published desktop and application sessions by writing and configuring load balancing scripts.

You can write your own custom load balancing scripts, or you can use one of the sample load balancing scripts provided with Horizon Agent. To use custom load balancing scripts, you must select the **Use Custom Script** load balancing setting in Horizon Console.

You can run these scripts on your own schedule or run these scripts with Horizon. For more information on configuring load balancing scripts in Horizon, see Configure a Load Balancing Script on an RDS Host.

Configuring load balancing scripts involves enabling the VMware Horizon View Script Host service and setting a registry key on each RDS host in a farm.

Load balancing scripts must write the load index to the `CustomLoadValue` registry key with the `REG_DWORD` registry setting in the following location:

```
HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue
```

The value must be between 0-100.

Horizon calculates the raw performance metrics that are written to the `Performance Stats` registry key in the following location:

```
HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats
```

You can use the raw performance metrics and combine these with your custom index factor for writing custom scripts.

Configure Load Balancing Settings on an RDS Host in Horizon Console

You can configure load balancing settings in Connection Server to control the placement of published desktop and application sessions on RDS hosts.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click **Add** and follow the prompts to the **Load Balancing Settings** page.

3 Configure the load balancing settings. See, Load Balancing Settings.

4 Follow the prompts to complete the wizard and click **Submit**.

Load Balancing Settings

Horizon calculates the Server Load Index based on the load balancing settings you configure in Horizon Console. The Server Load Index indicates the load on the server. The Server Load Index can range from 0 to 100, where 0 represents no load and 100 represents full load. A Server Load Index of -1 indicates that load balancing is disabled. You can view the Server Load Index in the Horizon Console dashboard.

Follow the best practice of including the session count with other metrics when you configure load balancing settings. If the session count is not included, then, during load balancing, one of the RDS hosts gets considerably more session requests than other RDS hosts when a large number of users logon to the farm within 30 seconds. This occurs because the sampling interval is 30 seconds and the CPU, Memory, or Disk statistics are not collected in the last 30 seconds. As a result, all session requests in the last 30 seconds go to the RDS host that reports the lowest load index even though this RDS host, after a few sessions, gets a higher load than the other hosts.

To mitigate this issue, you can also reduce the sampling interval to collect the CPU, Memory, and Disk statistics more frequently than every 30 seconds. You can reduce the sampling interval to a minimum of 5 seconds however, this can affect performance on the RDS host. You can alter the sampling interval by configuring the **CPU and Memory Sampling Interval in Seconds** global policy setting. For more information on configuring global policy settings, see the *Horizon Administration* document.

Table 7-2. Load Balancing Settings in Horizon Console

Option	Description
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon does not consider other load balancing settings and reads the `CustomLoadValue` registry key in the following location to get the server load index: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. See, Writing a Load Balancing Script for an RDS Host.
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.

Table 7-2. Load Balancing Settings in Horizon Console (continued)

Option	Description
Memory usage threshold	Threshold value for the memory in percentage. Horizon uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.

Writing a Load Balancing Script for an RDS Host

You can write a load balancing script to generate a load value based on any RDS host metric that you want to use for load balancing.

Your load balancing script must write the load index value to the `CustomLoadValue` registry key in the following location: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. This value must be between 0-100.

If at least one RDS host in the farm returns a valid load value, the Connection Server assumes a load value of 25 for the other RDS hosts in farm until their load balancing scripts return valid values. If no RDS host in the farm returns a valid load value, the load balancing feature is disabled for the farm.

Note The Horizon Console dashboard shows -1 for those RDS hosts that do not report a load index. Connection Server only uses the value of 25 for internal load balancing logic.

If your load balancing script writes an invalid load value to the `CustomLoadValue` registry key, the value is capped at 100 and returned as the load index to the Connection Server. If the script is unable to create the `CustomLoadValue` registry key, the default value of 0 is sent as the load index to the Connection Server. If the custom script does not finish running within 10 seconds, Horizon terminates the script after 10 seconds and uses stale values from the `CustomLoadValue` registry key as the load index.

Copy your load balancing script to the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`) on each RDS host in the farm. You must copy the same script to every RDS host in the farm.

For an example how to write a load balancing script, see the sample scripts in the Horizon Agent `scripts` directory. For more information, see Sample Load Balancing Scripts for RDS Hosts.

Sample Load Balancing Scripts for RDS Hosts

When you install Horizon Agent on an RDS host, the installer places sample load balancing scripts in the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`).

Table 7-3. Sample Load Balancing Scripts

Name	Description
`cpuutilisation.vbs`	Reads the percentage of CPU that has been utilized from the registry and writes it to the `CustomLoadValue` registry key.
`memoryutilisation.vbs`	Reads the percentage of memory that has been utilized from the registry and writes it to the `CustomLoadValue` registry key.

Enable the VMware Horizon View Script Host Service on an RDS Host

You must enable the VMware Horizon View Script Host service on an RDS host before you configure a load balancing script. The VMware Horizon View Script Host service is disabled by default.

Procedure

1. Log in to the RDS host as an administrator.
2. Start Server Manager.
3. Select **Tools > Services** and navigate to the VMware Horizon View Script Host service.
4. Right-click **VMware Horizon View Script Host** and select **Properties**.
5. In the Properties dialog box, select **Automatic** from the **Startup type** drop-down menu and click **OK** to save your changes.
6. Right-click **VMware Horizon View Script Host** and select **Start** to start the VMware Horizon View Script Host service.

Results

The VMware Horizon View Script Host service restarts automatically each time the RDS host starts.

What to do next

Configure your load balancing script on each RDS host in the farm. See Configure a Load Balancing Script on an RDS Host.

Configure a Load Balancing Script on an RDS Host

You must configure the same load balancing script on every RDS host in the farm. Configuring a load balancing script involves setting a registry key on the RDS host.

If you are using an automated farm, you perform this procedure on the golden image virtual machine for the automated farm.

Important You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm. If you configure a load balancing script on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to red.

Prerequisites

- Write a load balancing script and copy the same script to the Horizon Agent `scripts` directory on each RDS host in the farm. See Writing a Load Balancing Script for an RDS Host.
- Enable the VMware Horizon View Script Host service on the RDS host. See Enable the VMware Horizon View Script Host Service on an RDS Host.

Procedure

1. Log in to the RDS host as an administrator.
2. Start Server Manager.
3. Select **Tools > System Configuration**, click the **Tools** tab, and launch the Registry Editor.
4. In the registry, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
5. In the navigation area, select the **RdshLoad** key.

   The values for the **RdshLoad** key, if any, appear in the topic area (the right pane).
6. Right-click in the topic area for the **RdshLoad** key, select **New > String Value**, and create a new string value.

   As a best practice, use a name that represents the load balancing script to be run, for example, **`cpuutilisationScript`** for the `cpuutilisation.vbs` script.
7. Right-click the entry for the new string value you created and select **Modify**.
8. In the **Value data** text box, type the command line that invokes your load balancing script and click **OK**.

   Type the full path to your load balancing script.

   For example: `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`
9. Restart the Horizon Agent service on the RDS host to make your changes take effect.

Results

Your load balancing script begins to run on the RDS host.

What to do next

Repeat this procedure on each RDS host in the farm. If you performed this procedure on the golden image virtual machine for an automated farm, provision the automated farm.

To verify that your load balancing script is working correctly, see Verify a Load Balancing Script.

Verify a Load Balancing Script

You can verify that your load balancing script is working correctly by viewing RDS farm and RDS host information in Horizon Console.

Procedure

1 In Horizon Console, navigate to **Monitor > Dashboard**.

2 In the **Issues** pane, click **View**.

3 Click **RDS Farms** and click the name of each RDS host to view its load index.

   The Server load field in the details dialog box shows the server load index reported by Horizon Agent. The value should be between 0-100.

   The status of the farm should be green. If a load balancing script is configured on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to yellow. You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm.

What to do next

If load balancing is not working as you expected, verify the content of your load balancing script. If the script is written correctly, it should update the `CustomLoadValue` registry key on Horizon Agent with the expected load index. The `CustomLoadValue` registry key is located in the following location: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. Verify that this registry key is updated correctly. If you use Horizon to run your scripts, verify that the VMware Horizon View Script Host service is running. Also, verify that the same load balancing script is configured on each RDS host in the farm.