Horizon Console Administration

13 DEC 2018
VMware Horizon 7 7.7

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

VMware Horizon Console Administration

1

VMware Horizon Console Administration describes how to configure and administer VMware Horizon[®] 7, create administrators, set up user authentication, configure policies, and perform management tasks in Horizon Console. This document also describes how to maintain and troubleshoot Horizon 7 components.

Intended Audience

This information is intended for anyone who wants to configure and administer VMware Horizon 7. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Using VMware Horizon Console

2

VMware Horizon Console is the latest version of the Web interface through which you can create and manage virtual desktops and published desktops and applications. Horizon Console also integrates VMware Horizon Just-in-Time Management Platform (JMP) Integrated Workflow features for managing workspaces.

Horizon Console is available after you install and configure Horizon Connection Server.

For more information about configuring Connection Server, see the *Horizon 7 Administration* guide.

For more information about JMP) Integrated Workflow features, see Chapter 7 Getting Started with JMP Integrated Workflow.

This chapter includes the following topics:

- Supported Horizon 7 Features

- Benefits of Using Horizon Console

- Installing and Configuring Horizon Console

- Log In to Horizon Console

Supported Horizon 7 Features

Horizon Console includes a partial implementation of Horizon 7 features. You can use Horizon Administrator, the classic Web interface to access those features that are not yet available in Horizon Console.

For information about Horizon 7 that are supported with Horizon Administrator, see the *Horizon 7 Administration* document.

The following features are supported:

- Entitlements

  - User and group entitlements

  - Desktop entitlements

  - Application entitlements

- Authentication
  - Remote access authentication
  - Unauthenticated access for published applications
- Virtual desktops
  - Automated, dedicated-assignment pools of full virtual machines
  - Automated, instant-clone dedicated-assignment and floating-assignment pools
  - Automated linked-clone desktop pools
  - Automated, floating-assignment pools of full virtual machines
  - Manual desktop pools
- Published desktops
  - Manual farms
  - Automated instant-clone farms
  - RDS desktop pools
- Published Applications
  - Manual application pools
  - Application pools from existing applications
- Virtual Machines
  - Virtual Machines available in vCenter Server
  - Registered machines that are not available in vCenter Server

The following features are not supported:

- Automated linked-clone farms
- Cloning an automated desktop pool
- Cloud Pod Architecture
- ThinApp applications

Benefits of Using Horizon Console

The benefits of using Horizon Console include an easier desktop and application deployment process, just-in-time desktop delivery, and a more secure Web interface that eliminates security risks.

The Horizon Console Web interface is updated to include easy-to-use workflows for deploying and troubleshooting desktops and applications.

Horizon Console also includes the JMP Integrated Workflow features, which incorporate instant clone, VMware App Volumes, and VMware User Environment Manager technologies into an integrated workflow to deliver on-demand desktops that deploy and scale quickly. For more information, see About JMP Integrated Workflow.

Horizon Console has an HTML5-based Web interface, which is more secure and updated to eliminate many security risks and vulnerabilities.

Installing and Configuring Horizon Console

The Horizon Console URL is available from the Horizon Administrator Web interface after you use the Horizon Connection Server installer to install and configure Connection Server. The JMP Integrated Workflow is available in Horizon Console after you use the JMP Server installer to install and configure JMP Server.

For more information about installing Connection Server, see the *Horizon 7 Installation* document.

For more information about configuring Connection Server, see the *Horizon 7 Administration* document.

For more information about installing and configuring JMP Server, see the *VMware Horizon JMP Server Installation and Setup Guide* document.

Log In to Horizon Console

To perform desktop or application pool deployment tasks, troubleshooting tasks, or manage JMP workflows, you must log in to Horizon Console. You access Horizon Console through the Horizon Administrator Web interface by using a secure (TLS) connection.

Prerequisites

- Verify that Horizon Connection Server is installed on a dedicated computer.

- A user must be assigned any predefined role or a combination of predefined roles to view the Horizon Console link in Horizon Administrator and to login to Horizon Console. However, the Horizon Console link does not appear in Horizon Administrator when the user is assigned a custom role or a combination of predefined and custom roles. For more information on configuring role-based access, see the *Horizon 7 Administration* document.

- Verify that you are using a Web browser supported by Horizon Console. For more information about supported Web browsers, see the *Horizon 7 Installation* document.

Procedure

1 Log in to the Horizon Administrator interface.

Open your Web browser and enter the following URL, where *server* is the host name of the Connection Server instance. **https://*server*/admin**

Note You can use the IP address if you have to access a Connection Server instance when the host name is not resolvable. However, the contacted host will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security.

Your access to Horizon Administrator depends on the type of certificate that is configured on the Connection Server computer.

If you open your Web browser on the Connection Server host, use **https://127.0.0.1** to connect, not **https://localhost**. This method improves security by avoiding potential DNS attacks on the `localhost` resolution.

Option	Description
You configured a certificate signed by a CA for Connection Server.	When you first connect, your Web browser displays Horizon Console.
The default, self-signed certificate supplied with Connection Server is configured.	When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click **Ignore** to continue using the current TLS certificate.

2 Log in as a user with credentials to access the Administrators account.

You make an initial assignment to the Administrators role when you install a standalone Connection Server instance or the first Connection Server instance in a replicated group. By default, the account that you use to install Connection Server is selected, but you can change this account to the Administrators local group or to a domain global group.

If you chose the Administrators local group, then you can use any domain user added to this group directly or through global group membership. You cannot use local users added to this group.

3 In Horizon Administrator, click **Horizon Console**.

The Horizon Console Web interface opens in a new tab. You are logged in with Single Sign-On to Horizon Console.

Authenticating Users and Groups

3

After you log in to Horizon Console, you can set up authentication for users and groups to control access to applications and desktops.

You can configure remote access to restrict users and groups from accessing desktops from outside the network. You can set up the configuration for unauthenticated users to access their published applications from a Horizon Client without requiring AD credentials.

This chapter includes the following topics:

- Restricting Remote Desktop Access Outside the Network
- Configuring Unauthenticated Access
- Using Access Groups to Delegate Administration of Pools and Farms in Horizon Console

Restricting Remote Desktop Access Outside the Network

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

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

Configure Remote Access

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

Prerequisites

- A Unified Access Gateway appliance, security server, or load balancer must be deployed outside the network as a gateway to the Connection Server instance to which the user is entitled. For more information about deploying a Unified Access Gateway appliance, see the *Deploying and Configuring Unified Access Gateway* document.

- The users who get remote access must be entitled to desktop or application pools.

Procedure

1. In Horizon Console, select **Users and Groups**.

2. Click the **Remote Access** tab.

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

   Note Unauthenticated access users will not appear in the search results.

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

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

Configuring Unauthenticated Access

Administrators can set up the configuration for unauthenticated users to access their published applications from a Horizon Client without requiring AD credentials. Consider setting up unauthenticated access if your users require access to a seamless application that has its own security and user management.

When a user starts a published application that is configured for unauthenticated access, the RDS host creates a local user session on demand and allocates the session to the user.

This feature requires the Horizon 7 version 7.1 environment set up and Horizon Client version 4.4.

For information about the rules and guidelines for configuring users for unauthenticated access, see the *Horizon 7 Administration* document.

Create Users for Unauthenticated Access

Administrators can create users for unauthenticated access to published applications. After an administrator configures a user for unauthenticated access, the user can log in to the Connection Server instance from Horizon Client only with unauthenticated access.

Prerequisites

- Administrators can create only one user for each Active Directory account.

- Administrators cannot create unauthenticated user groups. If you create an unauthenticated access user and there is an existing client session for that AD user, you must restart the client session to make the changes take effect.

- If you select a user with desktop entitlements and make the user an unauthenticated access user, the user will not have access to the entitled desktops.

Procedure

1. In Horizon Console, select **Users and Groups**.

2   On the **Unauthenticated Access** tab, click **Add**.

3   In the **Add Unauthenticated User** wizard, select one or more search criteria and click **Find** to find users based on your search criteria.

4   Select a user and click **Next**.

5   Enter the user alias.

The default user alias is the user name that was configured for the AD account. End users can use the user alias to log in to the Connection Server instance from Horizon Client.

6   (Optional) Review the user details and add comments.

7   Click **Submit**.

Connection Server creates the unauthenticated access user and displays the user details including user alias, user name, first and last name, domain, application entitlements, and sessions.

What to do next

After you create users for unauthenticated access, you must enable unauthenticated access in Connection Server to enable users to connect and access published applications. See, "Enable Unauthenticated Access for Users" in the *Horizon 7 Administration* document.

Entitle Unauthenticated Access Users to Published Applications

After you create an unauthenticated access user, you must entitle the user to access published applications.

Prerequisites

- Create a farm based on a group of RDS hosts. See Creating Farms in Horizon Console.

- Create an application pool for published applications that run on a farm of RDS hosts. See Creating Application Pools in Horizon Console.

Procedure

1   In Horizon Console, select **Users and Groups**.

2   On the **Entitlements** tab, select **Add Application Entitlement** from the **Entitlements** drop-down menu.

3   Click **Add**, select one or more search criteria, select the **Unauthenticated Users** check box, and click **Find**, to find unauthenticated access users based on your search criteria.

4   Select the users to entitle to the applications in the pool and click **OK**.

5   Select the applications in the pool and click **Submit**.

What to do next

Use an unauthenticated access user to log in to Horizon Client. See, Unauthenticated Access From Horizon Client.

Delete an Unauthenticated Access User

When you delete an unauthenticated access user, you must also remove the application pool entitlements for the user.

You cannot delete an unauthenticated access user who is the default user. If you delete the default user, Horizon Console displays both an internal error message and a successful user removal message. However, the default user is not deleted from Horizon Console.

Note If you delete an unauthenticated access user and if there is an existing client session for that AD user, then you must restart the client session to make the changes take effect.

Procedure

1   In Horizon Console, select **Users and Groups**.

2   On the **Unauthenticated Access** tab, select the user and click **Delete**.

3   Click **OK**.

What to do next

Remove application entitlements for the user.

Unauthenticated Access From Horizon Client

Log in to Horizon Client with unauthenticated access and start the published application.

To ensure greater security, the unauthenticated access user has a user alias that you can use to log in to Horizon Client. When you select a user alias, you do not need to provide the AD credentials or UPN for the user. After you log in to Horizon Client, you can click your published applications to start the applications. For more information about installing and setting up Horizon Clients, see the Horizon Client documentation at the VMware Horizon Clients documentation Web page .

Prerequisites

■   Verify that Horizon 7 version 7.1 Connection Server is configured for unauthenticated access.

■   Verify that the unauthenticated access users are created in Horizon Administrator. If the default unauthenticated user is the only unauthenticated access user, Horizon Client connects to the Connection Server instance with the default user.

Procedure

1   Start Horizon Client.

2   In Horizon Client, select **Log in anonymously with Unauthenticated Access**.

3   Connect to the Connection Server instance.

4   Select a user alias from the drop-down menu and click **Login**.

    The default user has the "default" suffix.

5   Double-click a published application to start the application.

Using Access Groups to Delegate Administration of Pools and Farms in Horizon Console

By default, automated desktop pools, manual desktop pools, and farms are created in the root access group, which appears as / or Root(/) in Horizon Console. Published desktop pools and application pools inherit their farm's access group. You can create access groups under the root access group to delegate the administration of specific pools or farms to different administrators.

Note   You cannot change the access group of a published desktop pool or an application pool directly. You must change the access group of the farm that the published desktop pool or the application pool belongs to.

A virtual or physical machine inherits the access group from its desktop pool. An attached persistent disk inherits the access group from its machine. You can have a maximum of 100 access groups, including the root access group.

You configure administrator access to the resources in an access group by assigning a role to an administrator on that access group. Administrators can access the resources that reside only in access groups for which they have assigned roles. The role that an administrator has on an access group determines the level of access that the administrator has to the resources in that access group.

Because roles are inherited from the root access group, an administrator that has a role on the root access group has that role on all access groups. Administrators who have the Administrators role on the root access group are super administrators because they have full access to all of the objects in the system.

A role must contain at least one object-specific privilege to apply to an access group. Roles that contain only global privileges cannot be applied to access groups.

You can use Horizon Console to create access groups and to move existing desktop pools to access groups. When you create an automated desktop pool, a manual pool, or a farm, you can accept the default root access group or select a different access group.

Add an Access Group in Horizon Console

You can delegate the administration of specific machines, desktop pools, or farms to different administrators by creating access groups. By default, desktop pools, application pools, and farms reside in the root access group.

You can have a maximum of 100 access groups, including the root access group.

Procedure

1   In Horizon Console, navigate to the Access Group dialog box.

Option	Action
From Desktops	■ Select **Inventory > Desktops**.
	■ From the **Access Group** drop-down menu, select **New Access Group**.
From Farms	■ Select **Inventory > Farms**.
	■ From the **Access Groups** drop-down menu, select **New Access Group**.

2   Type a name and description for the access group and click **OK**.

The description is optional.

What to do next

Move one or more objects to the access group.

Move a Desktop Pool or Farm to a Different Access Group in Horizon Console

After you create an access group, you can move automated desktop pools, manual pools, or farms to the new access group.

Procedure

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

2   Select a pool or a farm.

3   Select **Change Access Group** from the **Access Group** drop-down menu.

4   Select the access group and click **OK**.

Horizon Console moves the pool or farm to the access group that you selected.

Review the Desktop Pools, Application Pools, or Farms in an Access Group

You can view the desktop pools, the application pools, or the farms in a particular access group in Horizon Console.

Procedure

1   In Horizon Console, navigate to the main page for the objects.

Object	Action
Desktop Pools	Select **Inventory > Desktops**.
Application Pools	Select **Inventory > Applications**.
Farms	Select **Inventory > Farms**.

By default, the objects in all access groups are displayed.

2 Select an access group from the **Access Group** drop-down menu in the main window pane.

The objects in the access group that you selected are displayed.

Review the vCenter Virtual Machines in an Access Group

You can view the vCenter virtual machines in a particular access group in Horizon Console. A vCenter virtual machine inherits the access group from its pool.

Procedure

1 In Horizon Console, navigate to **Inventory > Machines**.

2 Select the **vCenter VMs** tab.

By default, the vCenter virtual machines in all access groups are displayed.

3 Select an access group from the **Access Group** drop-down menu.

The vCenter virtual machines in the access group that you selected are displayed.

Creating Virtual Desktop Pools in Horizon Console

<div style="text-align:right">4</div>

With Horizon 7, you can create desktop pools that include thousands of virtual desktops. You can deploy desktops that run on virtual machines (VMs) and physical machines. Create one VM as a master image, and Horizon 7 can generate a pool of virtual desktops from that image. The master image is also known as a base image or a golden image.

For more information about how to create a base image or golden image or how to configure virtual machines for cloning, see the *Setting Up Virtual Desktops in Horizon 7* document.

In Horizon Console, you can create instant-clone desktop pools or automated desktop pools that contain full virtual machines.

This chapter includes the following topics:

- Creating Instant-Clone Desktop Pools
- Creating Automated Desktop Pools That Contain Full Virtual Machines
- Creating Linked-Clone Desktop Pools in Horizon Console
- Creating Manual Desktop Pools in Horizon Console
- Configuring Desktop Pools
- Managing Desktop Pools and Virtual Desktops in Horizon Console
- Troubleshooting Machines and Desktop Pools

Creating Instant-Clone Desktop Pools

To provide users access to instant-clone desktops, you must create an instant-clone desktop pool.

An instant-clone desktop pool is based on a parent VM in vCenter Server, known as the master image. For instant-clone desktops, a parent VM is an internal VM that Horizon 7 creates and maintains, which is based on the master image. You cannot modify this internal parent VM. However, you can make changes to the master image.

For more information about the configuration information required for creating and maintaining instant-clone desktop pools, see the *Setting Up Virtual Desktops in Horizon 7* document.

Worksheet for Creating an Instant-Clone Desktop Pool in Horizon Console

When you create an instant-clone desktop pool, you can configure certain options. You can use this worksheet to record your configuration options before you create the pool.

Before creating an instant-clone desktop pool, take a snapshot of the parent VM in vCenter Server. You must shut down the parent VM in vCenter Server before taking the snapshot. The snapshot is the master image for the clones in vCenter Server.

Note You cannot create an instant-clone desktop pool from a VM template.

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Select **Floating** or **Dedicated**. In a floating user assignment, users are assigned random desktops from the pool. In a dedicated user assignment, each user is assigned a particular remote desktop and returns to the same desktop at each login. Between each login and logout, the computer name and MAC address is retained for the same desktop. Any other changes that the user makes to the desktop are not preserved.	
vCenter Server	Select **Instant clones** and select the vCenter Server that manages the instant-clone VMs.	
Desktop Pool ID	The unique name that identifies the pool. If you have multiple Connection Server configurations, make sure that another Connection Server configuration does not use the same pool ID. A Connection Server configuration can consist of a single Connection Server or multiple Connection Servers	
Display name	The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.	
Access group	Select an access group for the pool, or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. **Note** Access groups are different from vCenter Server folders that store desktop VMs. You select a vCenter Server folder later in the wizard.	
State	If set to **Enabled**, the pool is ready for use after provisioning. If set to **Disabled**, the pool is not available to users. During provisioning, if you disable the pool, provisioning stops.	
Connection Server restrictions	You can restrict access to the 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 app might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices.	
Automatically logoff after disconnect	■ **Immediately**. Users are logged off when they disconnect. ■ **Never**. Users are never logged off. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The logoff time applies to future disconnections. If a desktop session is already disconnected when you set a logoff time, the logoff duration for that user starts when you set the logoff time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, Horizon 7 will log off that session 5 minutes after you set the value.	
Allow users to reset/restart their machines	Specify whether users can reset the virtual machine or restart the virtual desktop. A reset operation resets the virtual machine without a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines. A restart operation restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.	
Allow user to initiate separate sessions from different client devices	With this option selected, a user connecting to the same desktop pool from different client devices gets different desktop sessions. The user can only reconnect to an existing session from the same client device. When this setting is not selected, users are always reconnected to their existing session no matter which client device is used.	
Default display protocol	Select the default display protocol. The choices are **Microsoft RDP**, **PCoIP**, and **VMware Blast**.	
Allow users to choose protocol	Specify whether users can choose display protocols other than the default. Do not allow users to choose a display protocol.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
3D Renderer	Select 3D graphics rendering for desktops.	
	3D rendering is supported on Windows 7 or later guests running on VMs with virtual hardware version 8 or later. The hardware-based renderer is supported (at minimum) on virtual hardware version 9 in a vSphere 5.1 environment. The software renderer is supported (at minimum) on virtual hardware version 8 in a vSphere 5.0 environment.	
	On ESXi 5.0 hosts, the renderer allows a maximum VRAM size of 128MB. On ESXi 5.1 and later hosts, the maximum VRAM size is 512MB. On hardware version 11 (HWv11) virtual machines in vSphere 6.0, the VRAM value (video memory) has changed. Select the Manage Using vSphere Client option and configure video memory for these machines in vSphere Web Client. For details, see "Configuring 3D Graphics" in the vSphere Virtual Machine Administration guide.	
	3D rendering is disabled if you select Microsoft RDP as the default display protocol and do not allow users to choose a display protocol.	
	■ **NVIDIA GRID vGPU**. 3D rendering is enabled for NVIDIA GRID vGPU. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. You cannot use vSphere Distributed Resource Scheduler (DRS) when you select this option.	
	You can select either PCoIP or VMware Blast as a display protocol with NVIDIA GRID vGPU for an instant-clone desktop pool.	
	■ **Manage using vSphere Client**. The 3D Renderer option that is set in vSphere Web Client (or vSphere Client in vSphere 5.1 or later) for a virtual machine determines the type of 3D graphics rendering that takes place. Horizon 7 does not control 3D rendering. In the vSphere Web Client, you can configure the **Automatic**, **Software**, or **Hardware** options. These options have the same effect as they do when you set them in Horizon Console. Use this setting when configuring vDGA and AMD Multiuser GPU Using vDGA. This setting is also an option for vSGA. When you select the **Manage using vSphere Client** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution** of any one monitor settings are inactive in Horizon Console. You can configure the amount of memory in vSphere Web Client.	
	■ **Disabled**. 3D rendering is inactive. Default is disabled.	
HTML Access	Select **Enabled** to allow users to connect to remote desktops from a Web browser. For more information about this feature, see the *VMware Horizon HTML Access Installation and Setup Guide*.	
	To use HTML Access with VMware Identity Manager, you must pair Connection Server with a SAML authentication server, as described in the *Horizon 7 Administration* document. VMware Identity Manager must be installed and configured for use with Connection Server.	
Allow Session Collaboration	Select **Enabled** to allow users of the desktop pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast protocol.	
Stop provisioning on error	Specify whether Horizon 7 stops provisioning desktop VMs if an error occurs and prevents the error from affecting multiple VMs.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Naming pattern	Specify a pattern that Horizon 7 uses as a prefix in all the desktop VM names, followed by a unique number.	
Max number of machines	Specify the total number of desktop VMs in the pool.	
Number of spare (powered on) machines	Specify the number of desktop VMs to keep available to users.	
Provision machines on demand Min number of machines Provision all machines up front	Specify whether to provision all desktop VMs when the pool is created or to provision the VMs when they are needed. ■ **Provision all machines up front**. When the pool is created, Horizon 7 provisions the number of VMs you specify in **Max number of machines**. ■ **Provision machines on demand**. When the pool is created, Horizon 7 creates the number of VMs based on the **Min number of machines** value or the **Number of spare (powered on) machines** value, whichever is higher. Additional VMs are created to maintain this minimum number of available VMs as users connect to desktops.	
Select separate datastores for replica and OS disks	Specify whether to store the replica and OS disks on a datastore that is different from the datastores that the instant clones are on. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.	
Parent VM in vCenter	Select the parent VM in vCenter Server for the pool.	
Snapshot (default image)	You can specify the number of monitors and resolution for your instant-clone desktop pool by setting those parameters in the parent VM and taking a snapshot. The required vRAM size is calculated based on your specifications. Select the snapshot of the parent VM to use as the master image for the pool. The instant-clone desktop pool that is created is based on the snapshot and inherits those memory settings. For more information about configuring video memory settings in vSphere Client, see the *vSphere Single Host Management* guide in the vSphere documentation. For more information about changing the resolution for your instant-clone desktop pool, see the VMware Knowledge Base (KB) article http://kb.vmware.com/kb/2151745. The snapshot lists the following details: ■ Number of monitors ■ VRAM size ■ Resolution	
VM folder location	Select the folder in vCenter Server for the desktop VMs.	
Cluster	Select the vCenter Server cluster for the desktop VMs.	
Resource pool	Select the vCenter Server resource pool for the desktop VMs.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Datastores	Select one or more datastores for the desktop VMs. The **Select Instant Clone Datastores** window provides high-level guidelines for estimating the pool's storage requirements. These guidelines help you determine which datastores are large enough to store the clones. The Storage Overcommit value is always set to Unbounded and is not configurable. **Note** Instant clones and Storage vMotion are compatible. When you create an instant-clone desktop pool on a Storage DRS datastore, the Storage DRS cluster does not appear in the list of datastores. However, you can select individual Storage DRS datastores.	
Replica disk datastores	Select one or more replica disk datastores on which to store the instant-clones. This option appears if you select separate datastores for replica and OS disks. A table on the **Select Replica Disk Datastores** page of the Add Farm wizard provides high-level guidelines for estimate the farm's storage requirements. These guidelines can help you determine which replica disk datastores are enough to store the instant-clones.	
Networks	Select the networks to use for the instant-clone desktop pool. You can select multiple vLAN networks to create a larger instant-clone desktop pool. The default setting uses the network from the current master image. A table on the **Select Networks** wizard provides the networks, ports, and port bindings that are available to use. To use multiple networks, you must unselect **Use network from current parent VM** and then select the networks to use with the instant-clone farm.	
vGPU Profile	The vGPU profile for the pool is the vGPU profile of the snapshot you selected. The pool inherits this profile. This profile cannot be edited during the pool creation process. After a pool is provisioned, you can publish the image to change the vGPU profile. Mixed vGPU profiles on a single vSphere cluster (containing any number of ESXi hosts) are supported. For vCenter Server version 6.0, only single vGPU profiles with performance mode are supported. For vCenter Server version 6.5 and later, use the following guidelines for multiple vGPU profiles: ■ You can use multiple vGPU profiles with the **GPU consolidation** assignment policy for all GPU hosts within a cluster. ■ A mixed cluster of GPU enabled and non-GPU enabled hosts is supported. ■ Using a mixed cluster of some hosts with **GPU consolidation** assignment policy and some hosts with **GPU Performance** assignment policy is not recommended. To get better performance from a single profile for all vGPU desktops, you need to set GPU assignment policy of all GPU hosts within a cluster to **best performance**.	
Domain	Select an Active Directory domain. The drop-down list shows the domains that you specify when you configure instant-clone domain administrators.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
AD container	Specify the Active Directory container's relative distinguished name. For example: `CN=Computers` In the **Add Desktop Pool** window, you can browse the Active Directory tree for the container. You can also copy, paste, or enter the path for the AD tree for the container.	
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 7 uses the existing computer account after resetting the password. Otherwise, a new computer account is created. When the instant clone is deleted, Horizon 7 does not delete the corresponding computer accounts. 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 7 creates an instant clone. If an existing computer account is found, Horizon 7 uses the existing computer account after resetting the password. When the instant clone is deleted, Horizon 7 deletes the corresponding computer account. This option is disabled by default.	
Power-off script	Specify the path name of a script to run on the desktop VMs and the script parameters before the VMs are powered off.	
Post-synchronization script	Specify the path name of a script to run on the desktop VMs and the script parameters after the VMs are created.	

Create an Instant-Clone Desktop Pool

An instant-clone desktop pool is an automated desktop pool. vCenter Server creates the desktop VMs based on the settings that you specify when you create the pool.

Prerequisites

- 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 have the master image ready. For more information, see "Creating and Preparing Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document.

- Gather the configuration information for the pool. See Worksheet for Creating an Instant-Clone Desktop Pool in Horizon Console.

- Verify that you added an instant-clone domain administrator in Horizon Administrator. See "Add an Instant-Clone Domain Administrator" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

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

2 Click **Add**.

3 Select **Automated Desktop Pool** and click **Next**.

4 Select **Instant Clones**, select the vCenter Server instance, and click **Next**.

5 Follow the prompts to create the pool.

   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.

What to do next

Entitle users to access the pool. See, Add Entitlements to a Desktop or Application Pool in Horizon Console.

Change the Image of an Instant-Clone Desktop Pool in Horizon Console

You can change the image of an instant-clone desktop pool to push out changes or to revert to a previous image. You can select any snapshot from any virtual machine to be the new image.

Once a pool is provisioned, you cannot edit the vGPU profile by editing the pool or changing the image of the pool. When you push a new image to an instant clone pool, you must verify that the new image has the same vGPU profile as the previous image, or your push image operation might fail. To change the vGPU profile of an instant clone pool, you must delete the pool and create a new pool with the desired vGPU profile.

Procedure

1 In Horizon Console, select **Inventory > Desktops**

2 Click the pool ID.

3 On the **Summary** tab, click **Maintain > Schedule**.

   The **Schedule Push Image** window opens.

4 Follow the prompts.

   You can schedule the task to start immediately or sometime in the future. For clones with user sessions, you can specify whether to force the users to log out or to wait. When the users log out, Horizon 7 recreates the clones.

5 Click **Finish**.

After you initiate this operation, publishing of the new image starts immediately. Recreating the clones starts at the time that you specify in the **Schedule Push Image** wizard.

Monitor a Push-Image Operation in Horizon Console

You can monitor the progress of a push-image operation on an instant-clone desktop pool.

Procedure

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

2   Click the pool ID.

The **Summary** tab shows the current image and pending image information.

3   Click the **Tasks** tab.

The list of tasks that are associated with the push-image operation appears.

Reschedule or Cancel a Push-Image Operation in Horizon Console

You can reschedule or cancel a push-image operation on an instant-clone desktop pool.

Procedure

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

2   Click the pool ID.

The **Summary** tab shows the current image and pending image information.

3   Select **Maintain > Reschedule** or **Maintain > Cancel**.

4   Follow the prompts.

If you cancel the push-image operation while clone creation is in progress, the clones that have the new image remain in the pool and the pool has a mix of clones, some with the new image and the others with the old image. To ensure that all the clones have the same image, you can remove all the clones. Horizon 7 recreates the clones with the same image.

Creating Automated Desktop Pools That Contain Full Virtual Machines

With an automated desktop pool that contains full virtual machines, you create a virtual machine template and Horizon 7 uses that template to create virtual machines for each desktop. You can optionally create customization specifications to expedite automated pool deployments.

To create an automated desktop pool, Horizon 7 dynamically provisions machines based on settings that you apply to the pool. Horizon 7 uses a virtual machine template as the basis of the pool. From the template, Horizon 7 creates a new virtual machine in vCenter Server for each desktop.

For more information about the configuration information required for creating and maintaining automated desktop pools that contain full virtual machines, see the *Setting Up Virtual Desktops in Horizon 7* document.

Worksheet for Creating an Automated Pool That Contains Full Virtual Machines in Horizon Console

When you create an automated desktop pool, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Table 4-2. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in to the pool. ■ In a floating-assignment pool, users receive different machines each time they log in.	
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. You can assign machines manually even when automatic assignment is enabled.	
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
Desktop Pool ID	The unique name that identifies the pool in Horizon Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID. A Connection Server configuration can be a standalone Connection Server instance or a pod of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
Access group	Select an access group in which to place the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. **Note** Access groups are different from vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	

Table 4-2. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Delete machine after logoff	If you select floating user assignment, choose whether to delete machines after users log off. **Note** You set this option on the Desktop Pool Settings page.	
Desktop Pool Settings	Settings that determine the desktop state, power status when a virtual machine is not in use such as display protocol and so on.	
Stop provisioning on error	You can direct Horizon 7 to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines.	
Specify names manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	
Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine.	
Maximum number of machines	If you use a naming pattern, specify the total number of machines in the pool. You can also specify a minimum number of machines to provision when you first create the pool.	
Number of spare (powered on) machines	If you specify names manually or use a naming pattern, specify a number of machines to keep available and powered on for new users. When you specify names manually, this option is called **# Unassigned machines kept powered on**.	
Minimum number of machines	If you use a naming pattern and provision machines on demand, specify a minimum number of machines in the pool. The minimum number of machines is created when you create the pool. If you provision machines on demand, additional machines are created as users connect to the pool for the first time or as you assign machines to users.	
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.	

Table 4-2. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Template	Select the virtual machine template to use for creating the pool.	
vCenter Server folder	Select the folder in vCenter Server in which the desktop pool resides.	
Host or cluster	Select the ESXi host or cluster on which the virtual machines run. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
Datastores	Choose the type of datastore: ■ **Individual datastore**. Select individual datastores on which to store the desktop pool. ■ **Storage DRS**. Select the Storage Distributed Resource Scheduler (DRS) cluster that contains shared or local datastores. Storage DRS is a load balancing utility that assigns and moves storage workloads to available datastores. If your desktop pool was upgraded from Horizon 7 version 7.1 to Horizon 7 version 7.2, and you want to modify the pool to use the Storage DRS cluster, you must deselect the existing datastores and select Storage DRS. **Note** If you use vSAN, select only one datastore.	
Use View Storage Accelerator	Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. **Note** Horizon Console does not save the blackout times if you add or delete blackout times and then disable View Storage Accelerator.	

Table 4-2. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Guest customization	Select a customization specification (SYSPREP) from the list to configure licensing, domain attachment, DHCP settings, and other properties on the machines. You can only select a customization specification that matches the guest operating system of the template. Alternatively, you can customize the machines manually after they are created.	

Create an Automated Pool That Contains Full Virtual Machines

You can create an automated desktop pool based on a virtual machine template that you select. Horizon 7 dynamically deploys the desktops, creating a new virtual machine in vCenter Server for each desktop.

Prerequisites

- Prepare a virtual machine template that Horizon 7 will use to create the machines. Horizon 7 must be installed on the template. See "Creating and Preparing Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document.

- If you intend to use a customization specification, make sure that the specifications are accurate. In vSphere Client, deploy and customize a virtual machine from your template using the customization specification. Fully test the resulting virtual machine, including DHCP and authentication.

- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.

- Gather the configuration information you must provide to create the pool. See Worksheet for Creating an Automated Pool That Contains Full Virtual Machines in Horizon Console.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop and Pool Setting for All Desktop Pool Types" in the *Setting Up Virtual Desktops in Horizon 7* document.

- If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in Horizon Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in Horizon 7, and you cannot configure the pool in VMware Identity Manager.

Procedure

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

2 Click **Add**.

3 Select **Automated Desktop Pool** and click **Next**.

4 Select **Full Virtual Machines**, select the vCenter Server instance, and click **Next**.

5 Follow the prompts to create the pool.

   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.

What to do next

Entitle users to access the pool.

Rebuild a Virtual Machine in a Full-Clone Desktop Pool in Horizon Console

Rebuild a virtual machine in a full-clone desktop pool if you want to replace the virtual machine with a new virtual machine and want to reuse the machine name. You can rebuild a virtual machine that is in an error state to replace the virtual machine with an error free virtual machine of the same name. When you rebuild a virtual machine, the virtual machine is deleted and then cloned with the same virtual machine name and the AD computer accounts are reused. All user data or settings from the previous virtual machine are lost and the new virtual machine is created using the desktop pool template.

Prerequisites

- Create an automated full-clone desktop pool. See Create an Automated Pool That Contains Full Virtual Machines.

Procedure

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

2   Select the desktop pool that contains the virtual machine you want to rebuild and click the **Inventory** tab.

3   Select the virtual machine that you want to rebuild and click **Rebuild**.

In vCenter Client, you can view the virtual machine as it is deleted and cloned again with the same name. In Horizon Console, the status of the rebuilt virtual machine goes through the following states: **Deleting > Provisioning > Customizing > Available**.

Creating Linked-Clone Desktop Pools in Horizon Console

With a linked-clone desktop pool, Horizon 7 creates a desktop pool based on a parent virtual machine that you select. The View Composer service dynamically creates a linked-clone virtual machine in vCenter Server for each desktop.

Horizon 7 dynamically provisions the linked-clone desktops based on settings that you apply to the pool. Because linked-clone desktops share a base system-disk image, they use less storage than full virtual machines.

Worksheet for Creating a Linked-Clone Desktop Pool in Horizon Console

When you create a linked-clone desktop pool, you can configure certain options. Use this worksheet to prepare your configuration options before you create the linked-clone desktop pool.

Before you create a linked-clone pool, you must use vCenter Server to take a snapshot of the parent virtual machine that you prepare for the pool. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

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

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool

Option	Description	Fill In Your Value Here
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user.	
Persistent disk	If you select dedicated user assignments, choose whether to store Windows user-profile data on a separate View Composer persistent disk or the same disk as the OS data. ■ **Redirect Windows profile to a persistent disk**. Select this option to store data on a separate View Composer persistent disk. Separate persistent disks let you preserve user data and settings. View Composer refresh, recompose, and rebalance operations do not affect persistent disks. You can detach a persistent disk from a linked clone and recreate the linked-clone virtual machine from the detached disk. For example, when a machine or pool is deleted, you can detach the persistent disk and recreate the desktop, preserving the original user data and settings. ■ **Disk size**. If you store user profile data on a separate View Composer persistent disk, provide the disk size in megabytes. ■ **Drive letter**. If you store user profile data on a separate View Composer persistent disk, provide the drive letter. **Note** Do not select a drive letter that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive. ■ **Do not redirect Windows profile**. Select this option if you store the Windows profile in the OS disk. The user data and settings are removed during refresh, recompose, and rebalance operations.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Disposable File Redirection	Choose whether to redirect the guest operating system's paging and temporary files to a separate, non-persistent disk. ■ **Redirect disposable files to a non-persistent disk**. Select this option to redirect the guest operating system's paging and temporary files to a separate, non-persistent disk. With this configuration, when a linked clone is powered off, the disposable-file disk is replaced with a copy of the original disk that was created with the linked-clone pool. Linked clones can increase in size as users interact with their desktops. Disposable file redirection can save storage space by slowing the growth of linked clones. ■ **Disk size**. If you redirect disposable files to a non-persistent disk, provide the disk size in megabytes. The disk size should be larger than page-file size of the guest OS. To determine the page-file size, see "Keep a Record of the Parent Virtual Machine's Paging-File Size" in the *Setting Up Virtual Desktops in Horizon 7* document. When you configure the disposable file disk size, consider that the actual size of a formatted disk partition is slightly smaller than the value you provide in Horizon Console. ■ **Drive letter**. If you redirect disposable files to a non-persistent disk, provide the drive letter. You can select a drive letter for the disposable file disk. The default value, **Auto**, directs Horizon 7 to assign the drive letter. ■ **Do not redirect disposable files**. Select this option if you do not want to redirect the guest operating systems paging and temporary files. **Note** Do not select a drive letter that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.	
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. For more information, see "Using vSAN for High-Performance Storage and Policy-Based Management" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Select separate datastores for persistent and OS disks	(Available only if you do not use vSAN) If you redirect user profiles to separate persistent disks, you can store the persistent disks and OS disks on different datastores.	

Table 4‑**3.** **Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)**

Option	Description	Fill In Your Value Here
Select separate datastores for replica and OS disks	(Available only if you do not use vSAN or Virtual Volumes) You can store the replica (master) virtual machine disk on a high performance datastore and the linked clones on separate datastores. For details, see "Storing View Composer Replicas and Linked Clones on Separate Datastores," in the *Setting Up Virtual Desktops in Horizon 7* document. If you store replicas and OS disks on separate datastores, native NFS snapshots cannot be used. Native cloning on a NAS device can only take place if the replica and OS disks are stored on the same datastores.	
Desktop Pool ID	The unique name that identifies the pool. If multiple Connection Server configurations are running in your environment, make sure that another Connection Server configuration is not using the same pool ID. A Connection Server configuration can be a standalone Connection Server instance or a pod of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
Access group	Select an access group in which to place the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. For details, see the role-based delegated administration chapter in the *Horizon 7 Administration* document. **Note** Access groups are different from vCenter Server folders that store virtual machines that are used as desktops. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	
Enable provisioning	Select this option to provision virtual machines in a desktop pool.	
Stop provisioning on error	You can direct Horizon 7 to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
Virtual machine naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console.	
Specify names manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Naming pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine. For details, see Using a Naming Pattern for Automated Desktop Pools.	
Max number of machines	If you use a naming pattern, specify the total number of machines in the pool. You can also specify a minimum number of machines to provision when you first create the pool.	
Number of spare (powered on) machines	If you specify names manually or use a naming pattern, specify a number of machines to keep available and powered on for new users. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console. When you specify names manually, this option is called **# Unassigned machines kept powered on**.	
Minimum number of ready (provisioned) machines during View Composer maintenance operations	If you specify names manually or use a naming pattern, specify a minimum number of machines that are provisioned for use in remote desktop sessions while View Composer maintenance operations take place. This setting allows users to maintain existing connections or make new connection requests while View Composer refreshes, recomposes, or rebalances the machines in the pool. The setting does not distinguish between spare machines that are ready to accept new connections and machines that are already connected in existing desktop sessions. This value must be smaller than the **Max number of machines**, which you specify if you provision machines on demand. See, "Keeping Linked-Clone Machines Provisioned for Use in Remote Desktop Sessions During View Composer Operations," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Provision machines on demand or Provision all machines up front	If you use a naming pattern, choose whether to provision all machines when the pool is created or provision machines as they are needed. ■ **Provision all machines up front**. When the pool is created, the system provisions the number of machines you specify in **Max number of machines**. ■ **Provision machines on demand**. When the pool is created, the system creates the number of machines that you specify in **Min number of machines**. Additional machines are created as users connect to the pool for the first time or as you assign machines to users.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Min number of machines	If you use a naming pattern and provision desktops on demand, specify a minimum number of machines in the pool. The system creates the minimum number of machines when you create the pool. This number is maintained even when other settings such as **Delete or refresh machine on logoff** cause machines to be deleted.	
Parent VM	Select the parent virtual machine for the pool.	
Snapshot (default image)	Select the snapshot of the parent virtual machine to use as the base image for the pool. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no linked clones in the pool use the default image, and no more linked clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new linked clones in the pool, according to pool policies. The parent virtual machine and snapshot are also required for View Composer maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the desktop pool resides.	
Host or cluster	Select the ESXi host or cluster on which the desktop virtual machines run. With vSAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts if the replicas are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts. See, "Configuring Desktop Pools on Clusters With More Than Eight Hosts," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Linked clone datastores	Select one or more datastores on which to store the desktop pool. A table on the **Select Linked Clone Datastores** page of the Add Pool wizard provides high-level guidelines for estimating the pool's storage requirements. These guidelines can help you determine which datastores are large enough to store the linked-clone disks. For details, see "Storage Sizing for Linked-Clone Desktop Pools," in the *Setting Up Virtual Desktops in Horizon 7* document. You can use shared or local datastores for an individual ESXi host or for ESXi clusters. If you use local datastores in an ESXi cluster, you must consider the vSphere infrastructure constraints that are imposed on your desktop deployment. See, "Storing Linked Clones on Local Datastores," in the *Setting Up Virtual Desktops in Horizon 7* document. With vSAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. For more information about the disks that are created for linked clones, see "Linked-Clone Data Disks," in the *Setting Up Virtual Desktops in Horizon 7* document. **Note** If you use vSAN, select only one datastore.	
Replica disk datastores	Select a replica disk datastore on which to store the replicas. In vSphere 5.1 or later, a cluster can have more than eight ESXi hosts if the replicas are stored on datastores that are VMFS5 or later or NFS. In vSphere 5.0, a cluster can have more than eight ESXi hosts only if the replicas are stored on NFS datastores. See, "Configuring Desktop Pools on Clusters With More Than Eight Hosts," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Delete or refresh machine on logoff	If you select floating user assignment, choose whether to refresh machines, delete machines, or do nothing after users log off. **Note** You set this option on the Desktop Pool Settings page.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	Settings that determine the machine state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For descriptions, see "Desktop Pool Settings for All Desktop Pool Types," in the *Setting Up Virtual Desktops in Horizon 7* document. For a list of the settings that apply to linked-clone pools, see Desktop Pool Settings for Linked-Clone Desktop Pools in Horizon Console. For more information about power policies and automated pools, see "Setting Power Policies for desktop Pools in the *Setting Up Virtual Desktops in Horizon 7* document.	
Use View Storage Accelerator	Determine whether to use View Storage Accelerator, which allows ESXi hosts to cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. For details, see "Configure View Storage Accelerator for Desktop Pools," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Storage Overcommit	Determine the storage-overcommit level at which linked-clones are created on each datastore. As the level increases, more linked clones fit on the datastore and less space is reserved to let individual clones grow. A high storage-overcommit level lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore. For details, see "Set the Storage Overcommit Level for Linked-Clone Virtual Machines," in the *Setting Up Virtual Desktops in Horizon 7* document. **Note** This setting has no effect if you use vSAN.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Use native NFS snapshots (VAAI)	(Available only if you do not use vSAN) If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can use native snapshot technology to clone virtual machines. You can use this feature only if you select datastores that reside on NAS devices that support native cloning operations through VAAI. You cannot use this feature if you store replicas and OS disks on separate datastores. You cannot use this feature on virtual machines with space-efficient disks. This feature is supported on vSphere 5.0 and later. For details, see "Using View Composer Array Integration with Native NFS Snapshot Technology," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Reclaim VM disk space	(Available only if you do not use vSAN or Virtual Volumes) Determine whether to allow ESXi hosts to reclaim unused disk space on linked clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for linked-clone desktops. This feature is supported on vSphere 5.1 and later. The linked-clone virtual machines must be virtual hardware version 9 or later. For details, see "Reclaim Disk Space on Linked-Clone Virtual Machines," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Initiate reclamation when unused space on VM exceeds:	(Available only if you do not use vSAN or Virtual Volumes) Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, View initiates the operation that directs the ESXi host to reclaim space on the OS disk. This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before View starts the space reclamation process on that machine. For example: **2** GB. The default value is 1 GB.	
Blackout Times	Configure days and times during which View Storage Accelerator regeneration and the reclamation of virtual machine disk space do not take place. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days. For details, see "Set Blackout Times for ESXi Operations on Virtual Machines," in the *Setting Up Virtual Desktops in Horizon 7* document.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Domain	Select the Active Directory domain and user name. View Composer requires certain user privileges to create a linked-clone pool. The domain and user account are used by QuickPrep or Sysprep to customize the linked-clone machines. You specify this user when you configure View Composer settings for vCenter Server. You can specify multiple domains and users when you configure View Composer settings. When you use the **Add Desktop Pool** wizard to create a pool, you must select one domain and user from the list. For information about configuring View Composer, see the *Horizon 7 Administration* document.	
AD container	Provide the Active Directory container relative distinguished name. For example: `CN=Computers` When you run the **Add Desktop Pool** wizard, you can browse your Active Directory tree for the container.	

Table 4-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Allow reuse of pre-existing computer accounts	Select this option to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This option lets you control the computer accounts that are created in Active Directory. When a linked clone is provisioned, if an existing AD computer account name matches the linked clone machine name, View Composer uses the existing computer account. Otherwise, a new computer account is created. The existing computer accounts must be located in the Active Directory container that you specify with the **Active Directory container** setting. When this option is disabled, a new AD computer account is created when View Composer provisions a linked clone. This option is disabled by default. For details, see "Use Existing Active Directory Computer Accounts for Linked Clones," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Use QuickPrep or a customization specification (Sysprep)	Choose whether to use QuickPrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines. Sysprep is supported for linked clones only on vSphere 4.1 or later software. After you use QuickPrep or Sysprep when you create a pool, you cannot switch to the other customization method later on, when you create or recompose machines in the pool. For details, see "Choosing QuickPrep or Sysprep to Customize Linked-Clone Machine," in the *Setting Up Virtual Desktops in Horizon 7* document.	
Power-off script	QuickPrep can run a customization script on linked-clone machines before they are powered off. Provide the path to the script on the parent virtual machine and the script parameters.	
Post-synchronization script	QuickPrep can run a customization script on linked-clone machines after they are created, recomposed, and refreshed. Provide the path to the script on the parent virtual machine and the script parameters.	

Desktop Pool Settings for Linked-Clone Desktop Pools in Horizon Console

You must specify machine and desktop pool settings when you configure automated pools that contain linked clones created by View Composer. Different settings apply to pools with dedicated user assignments and floating user assignments.

The following table lists the settings that apply to linked-clone pools with dedicated assignments and floating assignments.

For descriptions of each setting, see "Desktop Pool Settings for All Desktop Pool Types" in the *Setting Up Virtual Desktops in Horizon 7* document.

Table 4-4. Settings for Automated, Linked-Clone Desktop Pools

Setting	Linked-Clone Pool, Dedicated Assignment	Linked-Clone Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Category Folder (*Supported in Horizon Administrator)	Yes	Yes
Remote machine power policy	Yes	Yes
Automatically logoff after disconnect	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes
Allow user to initiate separate sessions from different client devices		Yes
Delete or refresh machine on logoff		Yes
Refresh OS disk after logoff	Yes	
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
3D Renderer	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Adobe Flash quality	Yes	Yes
Adobe Flash throttling	Yes	Yes
Override global Mirage settings	Yes	Yes
Mirage Server configuration	Yes	Yes

Create a Linked-Clone Desktop Pool in Horizon Console

You can create an automated, linked-clone desktop pool based on a parent virtual machine that you select. The View Composer service dynamically creates a new linked-clone virtual machine in vCenter Server for each desktop.

Prerequisites

- Verify that the View Composer service is installed, either on the same host as vCenter Server or on a separate host, and that a View Composer database is configured. See the *Horizon 7 Installation* document.

- Verify that View Composer settings for vCenter Server are configured in Horizon Administrator. See the *Horizon 7 Administration* document.

- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.

- Verify that you prepared a parent virtual machine. Horizon Agent must be installed on the parent virtual machine. See "Creating and Preparing a Virtual Machine for Cloning" in the *Setting Up Virtual Desktops in Horizon 7* document.

- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

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

- Gather the configuration information you must provide to create the pool. See Worksheet for Creating a Linked-Clone Desktop Pool in Horizon Console.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See, "Desktop and Pool Settings for All Desktop Pool Types" in the *Setting Up Virtual Desktops in Horizon 7* document.

- If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in Horizon Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in Horizon 7, and you cannot configure the pool in VMware Identity Manager.

Important   While a linked-clone pool is created, do not modify the parent virtual machine in vCenter Server. For example, do not convert the parent virtual machine to a template. The View Composer service requires that the parent virtual machine remain in a static, unaltered state during pool creation.

Procedure

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

2   Click **Add**.

3   Select **Automated Desktop Pool** and click **Next**.

4   Select **View Composer linked clones**, select the vCenter Server instance, and click **Next**.

5   Follow the prompts to create the pool.

    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.

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

The linked clones might restart one or more times while they are provisioned. If a linked clone is in an error state, the automatic recovery mechanism attempts to power on, or shut down and restart, the linked clone. If repeated recovery attempts fail, the linked clone is deleted.

View Composer also creates a replica virtual machine that serves as the master image for provisioning the linked clones. To reduce space consumption, the replica is created as a thin disk. If all the virtual machines are recomposed or deleted, and no clones are linked to the replica, the replica virtual machine is deleted from vCenter Server.

If you do not store the replica on a separate datastore, View Composer creates a replica on each datastore on which linked clones are created.

If you store the replica on a separate datastore, one replica is created for the entire pool, even when linked clones are created on multiple datastores.

What to do next

Entitle users to access the pool. See, Add Entitlements to a Desktop or Application Pool in Horizon Console.

Creating Manual Desktop Pools in Horizon Console

In a manual desktop pool, each remote desktop that is accessed by an end user is a separate machine. When you create a manual desktop pool, you select existing machines. You can create a pool that contains a single desktop by creating a manual desktop pool and selecting a single machine.

Horizon 7 can use several types of machines in manual pools:

- Virtual machines that are managed by vCenter Server

- Virtual machines that run on a virtualization platform other than vCenter Server

- Physical computers

For information about creating a manual desktop pool that uses Linux virtual machines, see the *Setting Up Horizon 7 for Linux Desktops* guide.

Worksheet for Creating a Manual Desktop Pool in Horizon Console

When you create a manual desktop pool, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Note   In a manual pool, you must prepare each machine to deliver remote desktop access. Horizon Agent must be installed and running on each machine.

Table 4-5. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see User Assignment in Desktop Pools in Horizon Console.	
vCenter Server	The vCenter Server that manages the machines. This option appears only if the machines are virtual machines that are managed by vCenter Server.	
Machine Source	The virtual machines or physical computers that you want to include in the desktop pool. 1 Decide which type of machine you want to use. You can use either virtual machines that are managed by vCenter Server or unmanaged virtual machines and physical computers. 2 Prepare a list of the vCenter Server virtual machines or unmanaged virtual machines and physical computers that you want to include in the desktop pool. 3 Install Horizon Agent on each machine that you want to include in the desktop pool. To use PCoIP with machines that are unmanaged virtual machines or physical computers, you must use Teradici hardware. **Note** When you enable Windows Server desktops in Horizon Console, Horizon Console displays all available Windows Server machines, including machines on which Connection Server and other Horizon 7 servers are installed, as potential machine sources. You cannot select machines for the desktop pool if Horizon 7 server software is installed on the machines. Horizon Agent cannot coexist on the same virtual or physical machine with any other Horizon 7 software component, including Connection Server, security server, View Composer, or Horizon Client.	
Desktop Pool ID	The pool name that users see when they log in and that identifies the pool in Horizon Console. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.	

Table 4-5. Worksheet: Configuration Options for Creating a Manual Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	Settings that determine the machine state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For details, see Desktop Pool Settings for All Desktop Pool Types in Horizon Console. For a list of the settings that apply to manual pools, see Desktop Pool Settings for Manual Pools in Horizon Console.	
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	

Create a Manual Desktop Pool in Horizon Console

You can create a manual desktop pool that provisions desktops from existing virtual machines or physical computers. You must select the machines that will be included in the desktop pool.

For manual pools with virtual machines that are managed by vCenter Server, Horizon 7 ensures that a spare machine is powered on so that users can connect to it. The spare machine is powered on no matter which power policy is in effect.

Prerequisites

- Prepare the machines to deliver remote desktop access. In a manual pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine.

To prepare virtual machines managed by vCenter Server, see "Creating and Preparing Virtual Machines," in the *Setting Up Virtual Desktops in Horizon 7* document.

To prepare unmanaged virtual machines and physical computers, see "Preparing Unmanaged Machines," in the *Setting Up Virtual Desktops in Horizon 7* document.

- Gather the configuration information that you must provide to create the pool. See Worksheet for Creating a Manual Desktop Pool in Horizon Console.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See Desktop Pool Settings for All Desktop Pool Types in Horizon Console.

Procedure

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

2   Click **Add**.

3   Select **Manual Desktop Pool**.

4   Choose virtual machines managed by vCenter Server or unmanaged virtual machines that are not managed by vCenter Server and click **Next**.

Option	Description
vCenter virtual machines	Virtual machines that are managed by vCenter Server. Select the vCenter Server on which the virtual machines reside.
Other Sources	Physical computers or virtual machines that are not managed by vCenter Server

5   Select the type of user assignment.

Option	Description
Dedicated	The machine is assigned to one user. Only that user can log in to the desktop.
Floating	The machine is shared by all users who are entitled to the pool. Any entitled user can log in to the desktop as long as another user is not logged in.

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

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

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See Add Entitlements to a Desktop or Application Pool in Horizon Console.

Desktop Pool Settings for Manual Pools in Horizon Console

You must specify machine and pool settings when you configure manual desktop pools. Not all settings apply to all types of manual pools.

The settings for manual desktop pools lists the settings that apply to manual desktop pools that are configured with these properties:

- Dedicated user assignments

- Floating user assignments

- Managed machines (vCenter Server virtual machines)

- Unmanaged machines

These settings also apply to a manual pool that contains a single machine.

For descriptions of each desktop pool setting, see Desktop Pool Settings for All Desktop Pool Types in Horizon Console.

Table 4-6. Settings for Manual Desktop Pools

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
State	Yes	Yes	Yes	Yes
Connection Server restrictions	Yes	Yes	Yes	Yes
Remote machine power policy	Yes	Yes		
Automatically logoff after disconnect	Yes	Yes	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes		
Allow user to initiate separate sessions from different client devices		Yes		Yes
Default display protocol	Yes	Yes	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.
Allow users to choose protocol	Yes	Yes	Yes	Yes
3D Renderer	Yes	Yes		
Max number of monitors	Yes	Yes		

Table 4-6. Settings for Manual Desktop Pools (Continued)

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
Max resolution of any one monitor	Yes	Yes		
Adobe Flash quality	Yes	Yes	Yes	Yes
Adobe Flash throttling	Yes	Yes	Yes	Yes
Override global Mirage settings	Yes	Yes	Yes	Yes
Mirage Server configuration	Yes	Yes	Yes	Yes

Configuring Desktop Pools

When you create a desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

These tasks apply to desktop pools that are deployed on single-user machines. They do not apply to RDS desktop pools. However, the Adobe Flash quality and throttling settings apply to all types of desktop pools, including RDS.

User Assignment in Desktop Pools in Horizon Console

You can choose floating or dedicated user assignment for the desktops in a desktop pool.

With a dedicated assignment, each desktop is assigned to a specific user. A user logging in for the first time gets a desktop that is not assigned to another user. Thereafter, this user will always get this desktop after logging in, and this desktop is not available to any other user. Between each login and logout, the computer name and MAC address is retained for the same desktop. Any other changes that the user makes to the desktop are not preserved.

With a floating assignment, users get a random desktop every time they log in. When a user logs off, the desktop is returned to the pool.

With floating instant clones, the desktop is always deleted and recreated from the current image when a user logs out.

With floating-assignment, you might be able to reduce software licensing costs.

Naming Machines Manually or Providing a Naming Pattern in Horizon Console

With an automated desktop pool of full virtual machines or View Composer linked clones, you can specify a list of names for the desktop machines or provide a naming pattern. With an instant-clone desktop pool, you can only specify a naming pattern when provisioning the pool.

If you name machines by specifying a list, you can use your company's naming scheme, and you can associate each machine name with a user.

If you provide a naming pattern, Horizon 7 can dynamically create and assign machines as users need them.

The following table compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 4-7. Naming machines Manually or Providing a machine-Naming Pattern

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Machine names	The machine names are generated by appending a number to the naming pattern. For details, see Using a Naming Pattern for Automated Desktop Pools.	You specify a list of machine names. In a dedicated-assignment pool, you can pair users with machines by listing user names with the machine names. For details, see Specify a List of Machine Names in Horizon Console.
Pool size	You specify a maximum number of machines.	Your list of machine names determines the number of machines.
To add machines to the pool	You can increase the maximum pool size.	You can add machine names to the list. For details, see Add Machines to an Automated Pool Provisioned by a List of Names.
On-demand provisioning	Available. Horizon 7 dynamically creates and provisions the specified minimum and spare number of machines as users first log in or as you assign machines to users. Horizon 7 can also create and provision all the machines when you create the pool.	Not available. Horizon 7 creates and provisions all the machines that you specify in your list when the pool is created.
Initial customization	Available. When a machine is provisioned, Horizon 7 can run a customization specification that you select.	Available. When a machine is provisioned, Horizon 7 can run a customization specification that you select.
Manual customization of dedicated machines	Not available to instant clones. To customize machines and return desktop access to your users, you must remove and reassign the ownership of each machine. Depending on whether you assign machines on first log in, you might have to perform these steps twice. You cannot start machines in maintenance mode. After the pool is created, you can manually put the machines into maintenance mode.	You can customize and test machines without having to reassign ownership. When you create the pool, you can start all machines in maintenance mode to prevent users from accessing them. You can customize the machines and exit maintenance mode to return access to your users. For details, see Manually Customizing Machines.

Table 4-7. Naming machines Manually or Providing a machine-Naming Pattern (Continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Dynamic or fixed pool size	Dynamic. If you remove a user assignment from a machine in a dedicated-assignment pool, the machine is returned to the pool of available machines. If you choose to delete machines on logoff in a floating-assignment pool, the pool size can grow or shrink depending on the number of active user sessions. **Note** Instant-clone pools can only be floating-assignment pools. The machines are always deleted on logoff.	Fixed. The pool contains the number of machines you provide in the list of machine names. You cannot select the **Delete machine on logoff** setting if you name machines manually.
Spare machines	You can specify a number of spare machines that Horizon 7 keeps powered on for new users. Horizon 7 creates new machines to maintain the specified number. Horizon 7 stops creating spare machines when it reaches the maximum pool size. Horizon 7 keeps the spare machines powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy. **Note** Instant-clone pools do not have a power policy.	You can specify a number of spare machines that Horizon 7 keeps powered on for new users. Horizon 7 does not create new spare machines to maintain the specified number. Horizon 7 keeps the spare machines powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy.
User assignment	You can use a naming pattern for dedicated-assignment and floating-assignment pools.	You can specify machine names for dedicated-assignment and floating-assignment pools. **Note** In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Specify a List of Machine Names in Horizon Console

You can provision an automated desktop pool by manually specifying a list of machine names. This naming method lets you use your company's naming conventions to identify the machines in a pool.

When you explicitly specify machine names, users can see familiar names based on their company's organization when they log in to their remote desktops.

Follow these guidelines for manually specifying machine names:

- Type each machine name on a separate line.

- A machine name can have up to 15 alphanumeric characters.

- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are specified. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Make sure that each machine name is unique. You cannot use the names of existing virtual machines in vCenter Server.

Procedure

1   Create a text file that contains the list of machine names.

    If you intend to create a desktop pool with only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.

2   In Horizon Console start the **Add Pool** wizard to begin creating an automated desktop pool that contains full virtual machines.

3   On the Provisioning Settings page, select **Specify names manually** and click **Enter names**.

4   Copy your list of machine names in the **Enter Machine Names** page and click **Next**.

5   Click **Submit**.

6   (Optional) Select **Start machines in maintenance mode**.

    This option lets you customize the machines before users can log in and use them.

7   Follow the prompts in the wizard to finish creating the desktop pool.

Horizon 7 creates a machine for each name in the list. When an entry includes a machine and user name, Horizon 7 assigns the machine to that user.

After the desktop pool is created, you can add machines by importing another list file that contains additional machine names and users. See Add Machines to an Automated Pool Provisioned by a List of Names."

Using a Naming Pattern for Automated Desktop Pools

You can provision the machines in a pool by providing a naming pattern and the total number of machines you want in the pool. By default, Horizon 7 uses your pattern as a prefix in all the machine names and appends a unique number to identify each machine.

Length of the Naming Pattern in a Machine Name

Machine names have a 15-character limit, including your naming pattern and the automatically generated number.

Table 4-8. Maximum Length of the Naming Pattern in a Machine Name

If You Set This Number of Machines in the Pool	This Is the Maximum Prefix Length
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Names that contain fixed-length tokens have different length limits. See Length of the Naming Pattern When You Use a Fixed-Length Token.

Using a Token in a Machine Name

You can place the automatically generated number anywhere else in the name by using a token. When you type the pool name, type **n** surrounded by curly brackets to designate the token.

For example: **amber-{n}-desktop**

When a machine is created, Horizon 7 replaces **{n}** with a unique number.

You can generate a fixed-length token by typing **{n:fixed=*number of digits*}**.

Horizon 7 replaces the token with numbers containing the specified number of digits.

For example, if you type **amber-{n:fixed=3}**, Horizon 7 replaces **{n:fixed=3}** with a three-digit number and creates these machine names: **amber-001**, **amber-002**, **amber-003**, and so on.

Length of the Naming Pattern When You Use a Fixed-Length Token

Names that contain fixed-length tokens have a 15-character limit, including your naming pattern and the number of digits in the token.

Table 4-9. Maximum Length of the Naming Pattern When You Use a Fixed-Length Token

Fixed-Length Token	Maximum Length of the Naming Pattern
{n:fixed=1}	14 characters
{n:fixed=2}	13 characters
{n:fixed=3}	12 characters

Machine-Naming Example

This example shows how to create two automated desktop pools that use the same machine names, but different sets of numbers. The strategies that are used in this example achieve a specific user objective and show the flexibility of the machine-naming methods.

The objective is to create two pools with the same naming convention such as VDIABC-*XX*, where *XX* represents a number. Each pool has a different set of sequential numbers. For example, the first pool might contain machines VDIABC-01 through VDIABC-10. The second pool contains machines VDIABC-11 through VDIABC-20.

You can use either machine-naming method to satisfy this objective.

- To create fixed sets of machines at one time, specify machine names manually.

- To create machines dynamically when users log in for the first time, provide a naming pattern and use a token to designate the sequential numbers.

Specifying the Names Manually

1 Prepare a text file for the first pool that contains a list of machine names from VDIABC-01 through VDIABC-10.

2 In Horizon Console, create the pool and specify machine names manually.

3 Click **Enter Names** and copy your list into the **Enter Machine Names** list box.

4 Repeat these steps for the second pool, using the names VDIABC-11 through VDIABC-20.

For detailed instructions, see Specify a List of Machine Names in Horizon Console.

You can add machines to each pool after it is created. For example, you can add machines VDIABC-21 through VDIABC-30 to the first pool, and VDIABC-31 through VDIABC-40 to the second pool. See Add Machines to an Automated Pool Provisioned by a List of Names.

Providing a Naming Pattern With a Token

1 In Horizon Console, create the first pool and use a naming pattern to provision the machine names.

2 In the naming-pattern text box, type **`VDIABC-0{n}`**.

3 Limit the pool's maximum size to 9.

4 Repeat these steps for the second pool, but in the naming-pattern text box, type **`VDIABC-1{n}`**.

The first pool contains machines VDIABC-01 through VDIABC-09. The second pool contains machines VDIABC-11 through VDIABC-19.

Alternatively, you can configure the pools to contain up to 99 machines each by using a fixed-length token of 2 digits:

- For the first pool, type **`VDIABC-0{n:fixed=2}`**.

- For the second pool, type **`VDIABC-1{n:fixed=2}`**.

Limit each pool's maximum size to 99. This configuration produces machines that contain a 3-digit sequential naming pattern.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

For details about naming patterns and tokens, see Using a Naming Pattern for Automated Desktop Pools.

Add Machines to an Automated Pool Provisioned by a List of Names

To add machines to an automated desktop pool provisioned by manually specifying machine names, you provide another list of new machine names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

Follow these guidelines for manually adding machine names:

- Type each machine name on a separate line.

- A machine name can have up to 15 alphanumeric characters.

- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are added. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Note   In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Verify that you created the automated desktop pool of full virtual machines by manually specifying machine names. You cannot add machines by providing new machine names if you created the pool by providing a naming pattern.

Procedure

1   Create a text file that contains the list of additional machine names.

    If you intend to add only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.

2   In Horizon Console, select **Inventory > Desktops**.

3   Select the desktop pool to be expanded.

4   Click **Edit**.

5   Click the **Provisioning Settings** tab.

6   Click **Add Machines**.

7   Copy your list of machine names in the **Enter Machine Names** page and click **Next**.

8   Click **Submit**.

9   Click **OK**.

In vCenter Server, you can monitor the creation of the new virtual machines.

In Horizon Console, you can view the machines as they are added to the desktop pool by selecting **Inventory > Desktops**.

Change the Size of an Automated Pool Provisioned by a Naming Pattern in Horizon Console

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of machines.

Prerequisites

- Verify that you provisioned the desktop pool by using a naming pattern.

- Verify that the desktop pool is automated.

Procedure

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

2   Click the desktop pool ID and click **Edit**.

3   On the **Provisioning Settings** tab, type the new number of machines in the desktop pool in the **Max number of machines** text box.

If you increase the desktop pool size, new machines can be added to the pool up to the maximum number.

If you decrease the size of a floating-assignment pool, unused machines are deleted. If more users are logged into the pool than the new maximum, the pool size decreases after users log off.

If you decrease the size of a dedicated-assignment pool, unassigned machines are deleted. If more users are assigned to machines than the new maximum, the pool size decreases after you unassign users.

Note   When you decrease the size of a desktop pool, the actual number of machines might be larger than **Max number of machines** if more users are currently logged in or assigned to machines than the value that is specified in **Max number of machines**.

Manually Customizing Machines

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Note   This feature is not available to an instant-clone desktop pool.

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, Horizon 7 places each machine in maintenance mode when the machine is created. In a dedicated-assignment pool of full virtual machines, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template or parent. Horizon 7 deploys your customization to all the machines.

Note   You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Existing Machines in Maintenance Mode in Horizon Console

After a desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual-machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually.

Procedure

1   In Horizon Console, select **Inventory > Desktops**, double-click a pool ID, and select the **Inventory** tab.

2   Select a machine.

3   Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.

4   Customize, modify, or test the virtual-machine desktop.

5   Repeat Step 2 through Step 4

6   Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

The modified virtual-machine desktops are available to users.

Customize Individual Machines in Horizon Console

You can customize individual machines after a pool is created by starting the machines in maintenance mode.

Procedure

1   In Horizon Console, begin creating an automated desktop pool by starting the **Add Pool** wizard.

2   On the Provisioning Settings page, select **Specify names manually**.

3   Select **Start machines in maintenance mode**.

4   Complete the **Add Pool** wizard to finish creating the desktop pool.

5   In vCenter Server, log in, customize, and test the individual virtual machines.

You can customize the machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.

6   In Horizon Console, select **Inventory > Machines**.

7   Select specific machines to release to your users.

8   Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Desktop Pool Settings for All Desktop Pool Types in Horizon Console

You must specify machine and desktop pool settings when you configure automated pools that contain full virtual machines, linked-clone desktop pools, manual desktop pools, and instant-clone desktop pools. Not all settings apply to all types of desktop pools.

Table 4-10. Desktop Pool Setting Descriptions

Setting	Options
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.
Connection Server restrictions	■ **None**. The desktop pool can be accessed by any Connection Server instance. ■ **With tags**. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. If you intend to provide access to your desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager app might display desktops to users when those desktops are actually restricted. 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 desktop pool entitlement on Windows client devices. For more information, see "Configuring Start Menu Shortcuts for Desktop and Application Pools," in the *Setting Up Published Desktops and Applications in Horizon 7* document. This feature is available with Horizon Administrator.
Remote machine power policy	Determines how a virtual machine behaves when the user logs off of the associated desktop. For descriptions of the power-policy options, see "Power Policies for Desktop Pools," in the *Setting Up Virtual Desktops in Horizon 7* document. For more information about how power policies affect automated pools, see "setting Power Policies for Desktop Pools," in the *Setting Up Virtual Desktops in Horizon 7* document. Not applicable to instant-clone desktop pools. Instant clones are always powered on.

Table 4-10. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Automatically logoff after disconnect	■ **Immediately**. Users are logged off as soon as they disconnect. ■ **Never**. Users are never logged off. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The log off time applies to future disconnections. If a desktop session was already disconnected when you set a log off time, the log off duration for that user starts when you set the log off time, not when the session was originally disconnected. For example, if you set this value to five minutes, and a session was disconnected 10 minutes earlier, View will log off that session five minutes after you set the value.
Allow users to reset/restart their machines	Allow users to reset or restart their own desktops.
Allow user to initiate separate sessions from different client devices	When this setting is selected, a user connecting to the same desktop pool from different client devices will get different desktop sessions. The user can only reconnect to an existing session from the client device where that session was initiated. When this setting is not selected, the user will be reconnected to his or her existing session no matter which client device is used.
Delete machine after logoff	Select whether to delete floating-assignment, full virtual machines. ■ **No**. Virtual machines remain in the desktop pool after users log off. ■ **Yes**. Virtual machines are powered off and deleted as soon as users log off. For instant-clone desktops, the machine is always deleted and recreated after logoff.
Delete or refresh machine on logoff	Select whether to delete, refresh, or leave alone floating-assignment, linked-clone virtual machines. ■ **Never**. Virtual machines remain in the pool and are not refreshed after users log off. ■ **Delete immediately**. Virtual machines are powered off and deleted as soon as users log off. When users log off, virtual machines immediately go into a `Deleting` state. ■ **Refresh immediately**. Virtual machines are refreshed as soon as users log off. When users log off, virtual machines immediately go into maintenance mode to prevent other users from logging in as the refresh operation begins. For instant-clone desktops, the machine is always deleted and recreated after logoff.
Refresh OS disk after logoff	Select whether and when to refresh the OS disks for dedicated-assignment, linked-clone virtual machines. ■ **Never**. The OS disk is never refreshed. ■ **Always**. The OS disk is refreshed every time the user logs off. ■ **Every**. The OS disk is refreshed at regular intervals of a specified number of days. Type the number of days. The number of days is counted from the last refresh, or from the initial provisioning if no refresh has occurred yet. For example, if the specified value is **3** days, and three days have passed since the last refresh, the machine is refreshed after the user logs off. ■ **At**. The OS disk is refreshed when its current size reaches a specified percentage of its maximum allowable size. The maximum size of a linked clone's OS disk is the size of the replica's OS disk. Type the percentage at which refresh operations occur. With the **At** option, the size of the linked clone's OS disk in the datastore is compared to its maximum allowable size. This disk-utilization percentage does not reflect disk usage that you might see inside the machine's guest operating system. When you refresh the OS disks in a linked-clone pool with dedicated assignment, the View Composer persistent disks are not affected. For instant-clone desktops, the machine is always deleted and recreated after logoff.

Table 4-10. Desktop Pool Setting Descriptions (Continued)

Setting	Options	
Default display protocol	Select the display protocol that you want Connection Server to use to communicate with clients.	
	VMware Blast	The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network. This protocol consumes the least CPU resources and so provides longer battery life on mobile devices.
	PCoIP	PCoIP is supported as the display protocol for virtual and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN.
	Microsoft RDP	Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.
Allow users to choose protocol	Allow users to override the default display protocol for their desktops by using Horizon Client.	
3D Renderer	You can select whether to enable 3D graphics rendering if your pool comprises Windows 7 or later desktops. You can configure the **3D Renderer** to use software rendering or hardware rendering based on physical GPU graphics cards installed on ESXi 5.1 or later hosts.	
	To enable this feature, you must select PCoIP or VMware Blast as the protocol and disable the **Allow users to choose protocol** setting (select **No**).	
	With the hardware-based **3D Renderer** options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software **3D Renderer** option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For system requirements, see "Configuring 3D Rendering for Desktops," in the *Setting Up Virtual Desktops in Horizon 7* document.	
	If your View deployment does not run on vSphere 5.0 or later, this setting is not available and is inactive in View Administrator.	
	When you select this feature, if you select the **Automatic**, **Software**, or **Hardware** option, you can configure the amount of VRAM that is assigned to machines in the pool. The maximum number of monitors is 2 and the maximum resolution is 1920 x 1200.	
	If you select **Manage using vSphere Client**, or **NVIDIA GRID vGPU**, you must configure the amount of 3D memory and the number of monitors in vCenter Server. You can select at most four monitors for your machines that are used as remote desktops, depending on the monitor resolution.	
	Note When you configure or edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.	
	For instant-clone desktop pools, NVIDIA GRID vGPU is the only 3D Renderer option available.	

Table 4-10. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Max number of monitors	If you select PCoIP or VMware Blast as the display protocol, you can select the **Maximum number of monitors** on which users can display the desktop. You can select up to four monitors. When the **3D Renderer** setting is not selected, the **Max number of monitors** setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts. When the **3D Renderer** setting is not selected, up to three monitors are supported at 3840 x 2160 resolution on a Windows 7 guest operating system with Aero disabled. For other operating systems, or for Windows 7 with Aero enabled, one monitor is supported at 3840 x 2160 resolution. When the **3D Renderer** setting is selected, one monitor is supported at 3840 x 2160 resolution. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. **Note** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.
Max resolution of any one monitor	If you select PCoIP or VMware Blast as the display protocol, you should specify the **Maximum resolution of any one monitor**. The **Maximum resolution of any one monitor** is set to 1920 x 1200 pixels by default, but you can configure this value. When the **3D Renderer** setting is not selected, the **Max resolution of any one monitor** setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts. When the **3D Renderer** setting is not selected, up to three monitors are supported at 3840 x 2160 resolution on a Windows 7 guest operating system with Aero disabled. For other operating systems, or for Windows 7 with Aero enabled, one monitor is supported at 3840 x 2160 resolution. When the **3D Renderer** setting is selected, one monitor is supported at 3840 x 2160 resolution. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. **Note** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.
HTML Access	Select **Enabled** to allow users to connect to remote desktops from within their Web browsers. When a user logs in through the VMware Horizon Web portal page or the VMware Identity Manager app and selects a remote desktop, the HTML Access agent enables the user to connect to the desktop over HTTPS. The desktop is displayed in the user's browser. Other display protocols, such as PCoIP or RDP, are not used. Horizon Client software does not have to be installed on the client devices. To use HTML Access, you must install HTML Access in your View deployment. For more information, see *Using HTML Access*, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html. To use HTML Access with VMware Identity Manager, you must pair Connection Server with a SAML Authentication server, as described in the *Horizon 7 Administration* document. VMware Identity Manager must be installed and configured for use with Connection Server.
Allow Session Collaboration	Select **Enabled** to allow users of the pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.

Table 4-10. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Adobe Flash quality	Determines the quality of Adobe Flash content that is displayed on Web pages. ■ **Do not control**. Quality is determined by Web page settings. ■ **Low**. This setting results in the most bandwidth savings. If no quality level is specified, the system defaults to Low. ■ **Medium**. This setting results in moderate bandwidth savings. ■ **High**. This setting results in the least bandwidth savings. For more information, see "Adobe Flash Quality and Throttling," in the *Setting Up Virtual Desktops in Horizon 7* document.
Adobe Flash throttling	Determines the frame rate of Adobe Flash movies. If you enable this setting, you can reduce or increase the number of frames displayed per second by selecting an aggressiveness level. ■ **Disabled**. No throttling is performed. The timer interval is not modified. ■ **Conservative**. Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames. ■ **Moderate**. Timer interval is 500 milliseconds. ■ **Aggressive**. Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames. For more information, see "Adobe Flash Quality and Throttling," in the *Setting Up Virtual Desktops in Horizon 7* document.
Override global Mirage settings	To specify the same Mirage server for all desktop pools, use the global Horizon 7 configuration setting rather than this pool-specific setting. Not available to instant-clone desktop pools.
Mirage Server configuration	Allows you to specify the URL of a Mirage server, using the format `mirage://server-name:port` or `mirages://server-name:port`. Here *server-name* is the fully qualified domain name. If you do not specify the port number, the default port number 8000 is used. Specifying the Mirage server in Horizon Administrator is an alternative to specifying the Mirage server when installing the Mirage client. To find out which versions of Mirage support having the server specified in View Administrator, see the Mirage documentation, at https://www.vmware.com/support/pubs/mirage_pubs.html. Not available to instant-clone desktop pools.

Managing Desktop Pools and Virtual Desktops in Horizon Console

In Horizon Console, you can manage desktop pools, virtual machine-based desktops, physical machine-based desktops, and desktop sessions.

Managing Desktop Pools

You can perform administrative tasks on a desktop pool such as editing its properties, enabling, disabling, or deleting the pool.

Edit a Desktop Pool

You can edit an existing desktop pool to configure settings such as the number of spare machines, datastores, and customization specifications.

Prerequisites

Familiarize yourself with the desktop pool settings that you can and cannot change after a desktop pool is created. See "Modifying Settings in an Existing Desktop Pool" and "Fixed Settings in an Existing Desktop Pool" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

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

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

3   Click a tab in the Edit dialog box and reconfigure desktop pool options.

4   Click **OK**.

If you change the image of an instant-clone desktop pool, the image publishing operation starts immediately. In Horizon Administrator, the summary page for the desktop pool shows the state for the pending image as `Publishing`.

If you change the cluster of an instant-clone desktop pool, new replica and parent VMs are created in the new cluster. You can initiate a push image using the same image to have new clones created in the new cluster. However, the template VM, which is used in the cloning process, remains in the old cluster. You can put the ESXi host that the template VM is on in maintenance mode but you cannot migrate the template VM. To completely remove all infrastructure VMs, including the template VM, from the old cluster, you can initiate a push image using a new image.

Delete a Desktop Pool

When you delete a desktop pool, users can no longer launch new remote desktops in the pool.

Depending on the type of desktop pool, you have various options regarding how Horizon 7 handles persistent disks, vCenter Server full virtual machines, and users' active sessions.

By default, you can delete a desktop pool even if desktop machines exist in the pool. For details, see "Configure Desktop Pool Deletion Setting" in the *Setting Up Virtual Desktops in Horizon 7* document. If you configure the setting, you must delete all the machines in a desktop pool before you can delete the pool.

With an automated desktop pool of instant clones, Horizon 7 always deletes the virtual machines from disk.

Important   Do not delete the virtual machines in vCenter Server before you delete a desktop pool with Horizon Console. This action could put Horizon 7 components into an inconsistent state.

Procedure

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

2   Select a desktop pool and click **Delete**.

3   Choose how to delete the desktop pool.

Pool	Options
Automated desktop pool of instant clones without persistent disks.	No available options. Horizon 7 deletes all virtual machines from disk. Users' sessions to their remote desktops are terminated.
Automated desktop pool of full virtual machines.	Choose whether to keep or delete the virtual machines in vCenter Server.
RDS desktop pool. **Automated desktop pool of full virtual machines.**	If there are users who are connected to their remote desktops, choose whether to keep users' sessions active or terminate them. Note that Connection Server does not keep track of sessions that are kept active.

When you delete a desktop pool, full virtual machines' computer accounts remain in Active Directory. To remove these accounts, you must manually delete them from Active Directory.

If you delete an instant-clone desktop pool, it can take some time for Horizon 7 to delete the internal VMs from vCenter Server. Do not remove vCenter Server from Horizon Console until you verify that all the internal VMs are deleted.

Disable or Enable a Desktop Pool

When you disable a desktop pool, the pool is no longer presented to users and pool provisioning is stopped. Users have no access to the pool. After you disable a pool, you can enable it again.

Prerequisites

You can disable a desktop pool to prevent users from accessing their remote desktops while you prepare the desktops for use. If a desktop pool is no longer needed, you can use the disable feature to withdraw the pool from active use without having to delete the desktop pool definition from Horizon 7.

Procedure

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

2   Select a desktop pool and change the status of the pool.

Option	Action
Disable the pool	Select **Disable Desktop Pool** from the **Status** drop-down menu.
Enable the pool	Select **Enable Desktop Pool** from the **Status** drop-down menu.

3   Click **OK**.

Disable or Enable Provisioning in a Desktop Pool

When you disable provisioning in an automated desktop pool, Horizon 7 stops provisioning new virtual machines for the pool. After you disable provisioning, you can enable provisioning again.

Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You also can disable provisioning to prevent Horizon 7 from using additional storage when a pool is close to filling up the available space.

Procedure

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

2 Select a desktop pool and change the status of the pool.

Option	Action
Disable provisioning	Select **Disable Provisioning** from the **Status** drop-down menu.
Enable provisioning	Select **Enable Provisioning** from the **Status** drop-down menu.

3 Click **OK**.

Managing Virtual Machine-Based Desktops

A virtual machine-based desktop is a desktop that is from an automated desktop pool or a manual desktop pool that contains vCenter Server virtual machines.

Assign a Machine to a user in Horizon Console

In a dedicated-assignment pool, you can assign a user to be the owner of the virtual machine that hosts a remote desktop. Only the assigned user can log in and connect to the remote desktop.

Horizon Console assigns machines to users in these situations.

▪ When you create a desktop pool and select the **Allow automatic assignment** setting.

> **Note** If you select the **Allow automatic assignment** setting, you can still manually assign machines to users.

▪ When you create an automated pool, select the **Specify names manually** setting, and provide user names with the machine names.

If you do not select either setting in a dedicated-assignment pool, users do not have access to virtual desktops. You must manually assign a machine to each user.

You can also use the `vdmadmin` command to assign machines to users. For more information about the `vdmadmin` command, see the *Horizon 7 Administration* guide.

Prerequisites

▪ Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.

Procedure

1 In Horizon Console, select **Inventory > Desktops**, double-click a pool ID, and click the **Inventory** tab.

2 Select the machine.

3 Select **Assign User** from the **More Commands** drop-down menu.

4 Choose whether to find users or groups, select a domain, and type a search string in the **Name** or **Description** text box.

5 Select the user or group name and click **OK**.

Unassign a User from a Dedicated Machine in Horizon Console

In a dedicated-assignment pool, you can remove a machine assignment to a user.

You can also use the vdmadmin command to remove a machine assignment to a user. For more information about the vdmadmin command, see the *Horizon 7 Administration* guide.

Procedure

1 In Horizon Console, select **Inventory > Desktops**, double-click a pool ID, and click the **Inventory** tab.

2 Select the machine.

3 Select **Unassign User** from the **More Commands** drop-down menu.

4 Click **OK**.

The machine is available and can be assigned to another user.

Delete Virtual-Machine Desktops in Horizon Console

When you delete a virtual-machine desktop, users can no longer access the desktop.

Users in currently active sessions can continue to use full virtual-machine desktops if you keep the virtual machines in vCenter Server. After the users log off, they cannot access the deleted virtual-machine desktops.

With instant clones, vCenter Server always deletes the virtual machines from disk.

Note Do not delete the virtual machines in vCenter Server before you delete virtual-machine desktops with Horizon Console. This action could put Horizon 7 components into an inconsistent state.

Procedure

1 In Horizon Console, select **Inventory > Machines**

2 Select the **vCenter VMs** tab.

3 Select one or more machines and click **Remove**.

4 Choose how to delete the virtual-machine desktop.

Option	Description
Pool that contains full virtual-machine desktops	Choose whether to keep or delete the virtual machines in vCenter Server.
	If you delete the virtual machines from disk, users in active sessions are disconnected from their desktops.
	If you keep the virtual machines in vCenter Server, choose whether to let users in active sessions stay connected to their desktops or disconnect them.
Instant-clone pool without persistent disks	vCenter Server deletes the instant-clone virtual machines from disk. Users in currently active sessions are disconnected from their remote desktops.

Export Horizon 7 Information to External Files in Horizon Console

In Horizon Console, you can export Horizon 7 table information to external files. You can export the tables that list users and groups, pools, machines, View Composer persistent disks, ThinApp applications, events, and VDI sessions. You can view and manage the information in a spreadsheet or another tool.

For example, you might collect information about machines that are managed by more than one Connection Server instance or group of replicated Connection Server instances. You can export the Machines table from each Horizon Console interface and view it in a spreadsheet.

When you export a Horizon Console table, it is saved as a Microsoft Excel Open XML Format Spreadsheet (XLSX) file. This feature exports the entire table, not individual pages.

Procedure

1 In Horizon Console, display the table you want to export.

For example, click **Inventory > Machines** to display the machines table.

2 Click the export icon in the upper right corner of the table.

When you point to the icon, the `Export table contents` tooltip appears.

3 Type a filename for the XLSX file in the Select location for download dialog box.

4 Browse to a location to store the file.

5 Click **Save**.

What to do next

Open a spreadsheet or another tool to view the XLSX format file.

Managing View Composer Linked-Clone Desktop Virtual Machines

You can update View Composer linked-clone desktop machines, reduce the size of their operating system data, and rebalance the machines among datastores. You also can manage the persistent disks associated with linked clones.

Reduce Linked-Clone Size with Machine Refresh in Horizon Console

A machine refresh operation restores the operating system disk of each linked clone to its original state and size, reducing storage costs.

If possible, schedule refresh operations during off-peak hours.

For guidelines, see Machine Refresh Operations.

Prerequisites

- Decide when to schedule the refresh operation. By default, View Composer starts the operation immediately.

  You can schedule only one refresh operation at a time for a given set of linked clones. You can schedule multiple refresh operations if they affect different linked clones.

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

  If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

  If you force users to log off, the maximum number of concurrent refresh operations on remote desktops that require logoffs is half the value of the **Max concurrent View Composer maintenance operations** setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent refresh operations on remote desktops that require logoffs is 12.

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

Procedure

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

2   Select a linked-clone virtual machine.

3   On the **Inventory** tab, choose to refresh one virtual machine or multiple virtual machines.

   - To refresh one virtual machine, select the virtual machine, and select **Refresh** from the **View Composer** drop-down menu.

   - To refresh multiple virtual machines, select multiple virtual machines, and select **Refresh** from the **View Composer** drop-down menu.

4   Follow the wizard instructions.

The OS disks are reduced to their original size.

In vCenter Server, you can monitor the progress of the refresh operation on the linked-clone virtual machines.

In Horizon Console, you can monitor the operation by selecting **Inventory > Desktops**, clicking the pool ID, and clicking the **Tasks** tab. You can click **Pause task**, or **Resume task** to suspend a task, or resume a suspended task.

Machine Refresh Operations

As users interact with linked clones, the clones' OS disks grow. A machine refresh operation restores the OS disks to their original state and size, reducing storage costs.

A refresh operation does not affect View Composer persistent disks.

A linked clone uses less storage space than the parent virtual machine, which contains the complete OS data. However, a clone's OS disk expands each time data is written to it from within the guest operating system.

When View Composer creates a linked clone, it takes a snapshot of the clone's OS disk. The snapshot uniquely identifies the linked-clone virtual machine. A refresh operation reverts the OS disk to the snapshot.

View Composer can refresh a linked clone in as little as half the time it takes to delete and recreate the clone.

Apply these guidelines to refresh operations:

- You can refresh a desktop pool on demand, as a scheduled event, or when the OS data reaches a specified size.

  You can schedule only one refresh operation at a time for a given set of linked clones. If you start a refresh operation immediately, the operation overwrites any previously scheduled task.

  You can schedule multiple refresh operations if they affect different linked clones.

  Before you schedule a new refresh operation, you must cancel any previously scheduled task.

- You can refresh dedicated-assignment and floating-assignment pools.

- A refresh can only occur when users are disconnected from their linked-clone desktops.

- A refresh preserves the unique computer information set up by QuickPrep or Sysprep. You do not need to rerun Sysprep after a refresh to restore the SID or the GUIDs of third-party software installed in the system drive.

- After you recompose a linked clone, Horizon 7 takes a new snapshot of the linked clone's OS disk. Future refresh operations restore the OS data to that snapshot, not the one originally taken when the linked clone was first created.

  If you use native NFS snapshot (VAAI) technology to generate linked clones, certain vendors' NAS devices take snapshots of the replica disk when they refresh the linked clones' OS disks. These NAS devices do not support taking direct snapshots of each clone's OS disk.

- You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the refresh operation.

Note   You can slow the growth of linked clones by redirecting their paging files and system temp files to a temporary disk. When a linked clone is powered off, Horizon 7 replaces the temporary disk with a copy of the original temporary disk that View Composer created with the linked-clone pool. This operation shrinks the temporary disk to its original size.

You can configure this option when you create a linked-clone desktop pool.

Update Linked-Clone Desktops

You can update linked-clone virtual machines by creating a new base image on the parent virtual machine and using the recompose feature to distribute the updated image to the linked clones.

Prepare a Parent Virtual Machine to Recompose Linked Clones

Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones.

View Composer does not support recomposing linked clones that use one operating system to a parent virtual machine that uses a different operating system. For example, you cannot use a snapshot of a Windows 8 parent virtual machine to recompose a Windows 7 linked clone.

Procedure

1 In vCenter Server, update the parent virtual machine for the recomposition.

- Install OS patches or service packs, new applications, application updates, or make other changes in the parent virtual machine.

- Alternatively, prepare another virtual machine to be selected as the new parent during the recomposition.

2 In vCenter Server, power off the updated or new parent virtual machine.

3 In vCenter Server, take a snapshot of the parent virtual machine.

What to do next

Recompose the linked-clone desktop pool.

Recompose Linked-Clone Virtual Machines in Horizon Console

Machine recomposition simultaneously updates all the linked-clone virtual machines anchored to a parent virtual machine.

If possible, schedule recompositions during off-peak hours.

Prerequisites

- Verify that you have a snapshot of the parent virtual machine. See Prepare a Parent Virtual Machine to Recompose Linked Clones.

- Familiarize yourself with the recomposition guidelines. See Updating Linked Clones with Recomposition.

- Decide when to schedule the recomposition. By default, View Composer starts the recomposition immediately.

  You can schedule only one recomposition at a time for a given set of linked clones. You can schedule multiple recompositions if they affect different linked clones.

- Decide whether to force all users to log off as soon as the recomposition begins or wait for each user to log off before recomposing that user's linked-clone desktop.

  If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when View Composer provisions a linked clone, provisioning stops for all clones in the desktop pool. 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 a linked clone, other clones continue to be provisioned and customized.

- Verify that provisioning for the desktop pool is enabled. When desktop pool provisioning is disabled, Horizon 7 stops the desktops from being customized after they are recomposed.

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

Procedure

1 Choose whether to recompose the whole desktop pool or a single machine.

Option	Action
Recompose all virtual machines in the desktop pool	a In Horizon Console, select **Inventory > Desktops**. b Select the desktop pool to recompose by clicking the pool ID. c On the **Inventory** tab, click **Machines**. d Select all the machine IDs in the left column. e Select **Recompose** from the **View Composer** drop-down menu.
Recompose selected virtual machines	a In Horizon Console, select **Inventory > Machines**. b Select the machine to recompose by clicking the machine ID in the left column. c On the **Summary** tab, select **Recompose** from the **View Composer** drop-down menu.

2 Follow the wizard instructions.

  You can select a new virtual machine to be used as the parent virtual machine for the desktop pool.

  On the Ready to Complete page, you can click **Show Details** to display the recomposed linked-clone desktops.

The linked-clone virtual machines are refreshed and updated. The OS disks are reduced to their original size.

In a dedicated-assignment pool, unassigned linked clones are deleted and recreated. The specified number of spare virtual machines is maintained.

In a floating-assignment pool, all selected linked clones are recomposed.

In vCenter Server, you can monitor the progress of the recomposition on the linked-clone virtual machines.

In Horizon Console, you can monitor the operation by selecting **Inventory > Desktops**, clicking the pool ID, and clicking the **Tasks** tab. You can click **Pause task**, or **Resume task** to suspend a task, or resume a suspended task.

Note If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines.

Updating Linked Clones with Recomposition

In a recomposition, you can provide operating system patches, install or update applications, or modify the virtual machine hardware settings in all the linked clones in a desktop pool.

To recompose linked-clone virtual machines, you update the parent virtual machine in vCenter Server or select a different virtual machine to become the new parent. Next, you take a snapshot of the new parent virtual machine configuration.

You can change the parent virtual machine without affecting the linked clones because they are linked to the replica, not directly to the parent.

You then initiate the recomposition, selecting the snapshot to be used as the new base image for the desktop pool. View Composer creates a new replica, copies the reconfigured OS disk to the linked clones, and anchors the linked clones to the new replica.

The recomposition also refreshes the linked clones, reducing the size of their OS disks.

Desktop recompositions do not affect View Composer persistent disks.

Apply these guidelines to recompositions:

- You can recompose dedicated-assignment and floating-assignment desktop pools.

- You can recompose a desktop pool on demand or as a scheduled event.

  You can schedule only one recomposition at a time for a given set of linked clones. Before you can schedule a new recomposition, you must cancel any previously scheduled task or wait until the previous operation is completed. Before you can start a new recomposition immediately, you must cancel any previously scheduled task.

  You can schedule multiple recompositions if they affect different linked clones.

- You can recompose selected linked clones or all linked clones in a desktop pool.

- When different linked clones in a desktop pool are derived from different snapshots of the base image or from different base images, the desktop pool includes more than one replica.

- A recomposition can only occur when users are logged off of their linked-clone desktops.

- You cannot recompose linked clones that use one operating system to a new or updated parent virtual machine that uses a different operating system.

- You cannot recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.

- You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the recompose operation.

Note If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines.

Correcting an Unsuccessful Recomposition

You can correct a recomposition that failed. You can also take action if you accidentally recompose linked clones using a different base image than the one you intended to use.

Problem

The virtual machines are in an erroneous or outdated state as a result of an unsuccessful recomposition.

Cause

A system failure or problem might have occurred on the vCenter Server host, in vCenter Server, or on a datastore during the recomposition.

Alternatively, the recomposition might have used a virtual-machine snapshot with a different operating system than the operating system of the original parent virtual machine. For example, you might have used a Windows 8 snapshot to recompose Windows 7 linked clones.

Solution

1   Select the snapshot that was used in the last successful recomposition.

    You can also select a new snapshot to update the linked clones to a new state.

    The snapshot must use the same operating system as the original parent virtual machine's snapshot.

2   Recompose the desktop pool again.

    View Composer creates a base image from the snapshot and recreates the linked-clone OS disks.

    View Composer persistent disks that contain user data and settings are preserved during the recomposition.

    Depending on the conditions of the incorrect recomposition, you might refresh or rebalance the linked clones instead of or in addition to recomposing them.

    Note If you do not configure View Composer persistent disks, all recompositions delete user-generated changes in the linked-clone virtual machines.

Rebalance Linked-Clone Virtual Machines in Horizon Console

A rebalance operation evenly redistributes linked-clone virtual machines among available datastores.

If possible, schedule rebalance operations during off-peak hours.

Prerequisites

- Familiarize yourself with the rebalance operation. See Rebalancing Linked Clones Among Logical Drives.

- Decide when to schedule the rebalance operation. By default, View Composer starts the operation immediately.

  You can schedule only one rebalance operation at a time for a given set of linked clones. You can schedule multiple rebalance operations if they affect different linked clones.

- Decide whether to force all users to log off as soon as the operation begins or wait for each user to log off before rebalancing that user's linked-clone desktop.

  If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

  If you force users to log off, the maximum number of concurrent rebalance operations on remote desktops that require logoffs is half the value of the **Max concurrent View Composer maintenance operations** setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent rebalance operations on remote desktops that require logoffs is 12.

- Verify that provisioning for the desktop pool is enabled. When pool provisioning is disabled, Horizon 7 stops the virtual machines from being customized after they are rebalanced.

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

Procedure

1 Choose whether to rebalance the whole desktop pool or a single machine.

Option	Action
Rebalance all virtual machines in the desktop pool	a In Horizon Console, select **Inventory > Desktops**.
	b Select the desktop pool to rebalance by clicking the pool ID.
	c On the **Inventory** tab, click **Machines**.
	d Select all the machine IDs in the left column.
	e Select **Rebalance** from the **View Composer** drop-down menu.
Rebalance selected virtual machines	a In Horizon Console, select **Inventory > Machines**.
	b Select the machine to rebalance by clicking the machine ID in the left column.
	c On the **Summary** tab, select **Rebalance** from the **View Composer** drop-down menu.

2 Follow the wizard instructions.

The linked-clone virtual machines are refreshed and rebalanced. The OS disks are reduced to their original size.

In View Administrator, you can monitor the operation by selecting **Catalog > Desktop Pools**, double-clicking the pool ID, and clicking the **Tasks** tab. You can click **Pause task**, or **Resume task** to suspend a task, or resume a suspended task.

Rebalancing Linked Clones Among Logical Drives

A rebalance operation evenly redistributes linked-clone virtual machines among available logical drives. It saves storage space on overloaded drives and ensures that no drives are underused.

When you create large linked-clone desktop pools and use multiple Logical Unit Numbers (LUNs), the space might not be used efficiently if the initial sizing was inaccurate. If you set an aggressive storage overcommit level, the linked clones can grow quickly and consume all the free space on the datastore.

When the virtual machines use 95% of the space on the datastore, Horizon 7 generates a warning log entry.

The rebalance also refreshes the linked clones, reducing the size of their OS disks. It does not affect View Composer persistent disks.

Apply these guidelines to rebalances:

- You can rebalance dedicated-assignment and floating-assignment desktop pools.

- You can rebalance selected linked clones or all clones in a pool.

- You can rebalance a desktop pool on demand or as a scheduled event.

   You can schedule only one rebalance operation at a time for a given set of linked clones. If you start a rebalance operation immediately, the operation overwrites any previously scheduled task.

   You can schedule multiple rebalance operations if they affect different linked clones.

   Before you schedule a new rebalance operation, you must cancel any previously scheduled task.

- You can only rebalance virtual machines in the Available, Error, or Customizing state with no schedules or pending cancellations.

- As a best practice, do not mix linked-clone virtual machines with other types of virtual machines on the same datastore. This way View Composer can rebalance all the virtual machines on the datastore.

- If you edit a pool and change the host or cluster and the datastores on which linked clones are stored, you can only rebalance the linked clones if the newly selected host or cluster has full access to both the original and the new datastores. All hosts in the new cluster must have access to the original and new datastores.

   For example, you might create a linked-clone desktop pool on a standalone host and select a local datastore to store the clones. If you edit the desktop pool and select a cluster and a shared datastore, a rebalance operation will fail because the hosts in the cluster cannot access the original, local datastore.

- You can set a minimum number of ready, provisioned virtual machines that remain available for users to connect to during the rebalance operation.

Important   If you use a vSAN datastore, you can use the rebalance operation only to migrate all the virtual machines in a desktop pool from a vSAN datastore to some other type of datastore, or the reverse. If a desktop pool uses a vSAN datastore, vSAN provides the load balancing functionality and optimizes the use of resources across the ESXi cluster.

Filenames of Linked-Clone Disks After a Rebalance Operation

When you rebalance linked-clone virtual machines, vCenter Server changes the filenames of View Composer persistent disks and disposable-data disks in linked clones that are moved to a new datastore.

The original filenames identify the disk type. The renamed disks do not include the identifying labels.

An original persistent disk has a filename with a `user-disk` label: *desktop_name*`-vdm-user-disk-D-`*ID*`.vmdk`.

An original disposable-data disk has a filename with a `disposable` label: *desktop_name*`-vdm-disposable-`*ID*`.vmdk`.

After a rebalance operation moves a linked clone to a new datastore, vCenter Server uses a common filename syntax for both types of disks: *desktop_name_n*`.vmdk`.

Manage View Composer Persistent Disks

You can detach a View Composer persistent disk from a linked-clone virtual machine and attach it to another linked clone. This feature lets you manage user information separately from linked-clone virtual machines.

View Composer Persistent Disks

With View Composer, you can configure OS data and user information on separate disks in linked-clone virtual machines. View Composer preserves the user information on the persistent disk when the OS data is updated, refreshed, or rebalanced.

A View Composer persistent disk contains user settings and other user-generated data. You create persistent disks when you create a linked-clone desktop pool.

You can detach a persistent disk from its linked-clone virtual machine and store the disk on its original datastore or another datastore. After you detach the disk, the linked-clone virtual machine is deleted. A detached persistent disk is no longer associated with any virtual machine.

You can use several methods to attach a detached persistent disk to another linked-clone virtual machine. This flexibility has several uses:

- When a linked clone is deleted, you can preserve the user data.

- When an employee leaves the company, another employee can access the departing employee's user data.

- A user who has multiple remote desktops can consolidate the user data on a single remote desktop.

- If a virtual machine becomes inaccessible in vCenter Server, but the persistent disk is intact, you can import the persistent disk and create a new linked clone using the disk.

Note Persistent disks must be reconnected to the operating system that was used when they were created. For example, you cannot detach a persistent disk from a Windows 7 linked clone and recreate or attach the persistent disk to a Windows 8 linked clone.

Detach a View Composer Persistent Disk in Horizon Console

When you detach a View Composer persistent disk from a linked-clone virtual machine, the disk is stored and the linked clone is deleted. By detaching a persistent disk, you can store and reuse user-specific information with another virtual machine.

Procedure

1   In Horizon Console, select **Inventory > Persistent Disks**.

2   Select the persistent disk to detach and click **Detach.**

3   Choose where to store the persistent disk.

Option	Description
Use current datastore	Store the persistent disk on the datastore where it is currently located.
Use the following datastore	Select a new datastore on which to store the persistent disk. Click **Browse**, click the down arrow, and select a new datastore from the **Choose a Datastore** menu.
	From the filtered results, you can select a compatible non-vSAN datastore to store the detached persistent disk. Or, select **Show all datastores (including local datastores)** to view all datastores including shared and vSAN datastores. You cannot use a vSAN datastore.

The View Composer persistent disk is saved on the datastore. The linked-clone virtual machine is deleted and does not appear in Horizon Console.

Attach a View Composer Persistent Disk to Another Linked Clone in Horizon Console

You can attach a detached persistent disk to another linked-clone virtual machine. Attaching a persistent disk makes the user settings and information in the disk available to the user of the other virtual machine.

You attach a detached persistent disk as a secondary disk on the selected linked-clone virtual machine. The new user of the linked clone has access to the secondary disk and to the existing user information and settings.

You cannot attach a persistent disk that is stored on a non-vSAN datastore to a virtual machine that is stored on a vSAN datastore. Similarly, you cannot attach a disk that is stored on vSAN to a virtual machine that is stored on non-vSAN. Horizon Console prevents you from selecting virtual machines that span vSAN and non-vSAN datastores.

If you attach a persistent disk to a linked-cloned desktop pool that does not have persistent disk datastores, the persistent disk information appears under the **Machines (View Composer Details)** tab and on the **Persistent Disks** tab for the desktop pool.

Prerequisites

■ Verify that the selected virtual machine uses the same operating system as the linked clone in which the persistent disk was created.

Procedure

1 In Horizon Console, select **Inventory > Persistent Disks**.

2 On the **Detached** tab, select the persistent disk and click **Attach**.

3 Select a linked-clone virtual machine to which to attach the persistent disk.

4 Select the machine that the persistent disk will be attached to.

5 Click **OK**.

What to do next

Verify that the user of the linked clone has sufficient privileges to use the attached disk. For example, if the original user had certain access permissions on the persistent disk, and the persistent disk is attached as drive D on the new linked clone, the new user of the linked clone must have the original user's access permissions on drive D.

Log in to the linked clone's guest operating system as an administrator and assign appropriate privileges to the new user.

Edit a View Composer Persistent Disk's Pool or User in Horizon Console

You can assign a detached View Composer persistent disk to a new desktop pool or user if the original desktop pool or user was deleted from Horizon 7.

A detached persistent disk is still associated with its original desktop pool and user. If the desktop pool or user is deleted from Horizon 7, you cannot use the persistent disk to recreate a linked-clone virtual machine.

By editing the desktop pool and user, you can use the detached persistent disk to recreate a virtual machine in the new desktop pool. The virtual machine is assigned to the new user.

You can select a new desktop pool, a new user, or both.

Prerequisites

■ Verify that the persistent disk's desktop pool or user was deleted from Horizon 7.

■ Verify that the new desktop pool uses the same operating system as the desktop pool in which persistent disk was created.

Procedure

1 In Horizon Console, select **Inventory > Persistent Disks**.

2 Select the persistent disk for which the user or desktop pool has been deleted and click **Edit**.

3 (Optional) Select a linked-cloned desktop pool from the list.

4   (Optional) Select a user for the persistent disk.

You can browse your Active Directory for the domain and user name.

What to do next

Recreate a linked-clone virtual machine with the detached persistent disk.

Delete a Detached View Composer Persistent Disk in Horizon Console

When you delete a detached persistent disk, you can remove the disk from Horizon 7 and leave it on the datastore or delete the disk from Horizon 7 and the datastore.

Procedure

1   In Horizon Console, select **Inventory > Persistent Disks**.

2   On the **Detached** tab, select the persistent disk and click **Delete**.

3   Choose whether to delete the disk from the datastore or let it remain on the datastore after it is removed from Horizon Console.

Option	Description
Delete from View Manager only	After the deletion, the persistent disk is no longer accessible in Horizon 7 but remains on the datastore.
Delete from disk	After the deletion, the persistent disk no longer exists.

4   Click **OK**.

Managing Unmanaged and Registered Machines in Horizon Console

In Horizon Console, you can remove unmanaged machines and remove registered machines from Horizon 7.

Unmanaged machines include physical computers, RDS hosts, and virtual machines that are not managed by vCenter Server. These unmanaged machines must therefore be registered with the Connection Server instance before they can be added to a desktop pool.

There are two types of registered machines in Horizon 7: RDS Hosts and Others. Unmanaged machines are in the Others category. Use unmanaged machines to form desktop pools that do not contain vCenter Server virtual machines.

When you reconfigure a setting that affects an unmanaged machine, it can take up to 10 minutes for the new setting to take effect. For example, if you change the **Automatically logoff after disconnect** setting for a pool, Horizon 7 might take up to 10 minutes to reconfigure the affected unmanaged machines.

Remove an Unmanaged Machine from a Desktop Pool in Horizon Console

You can reduce the size of a desktop pool by removing unmanaged machines from the pool.

Procedure

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

2 Select the **Others** tab.

3 Select the unmanaged machines to remove.

4 Click **Remove**.

5 Click **OK**.

The unmanaged machines are removed from the pool.

Remove Registered Machines in Horizon Console

If you do not plan to use a registered machine again, you can remove it from Horizon 7.

After you remove a registered machine, it becomes unavailable in Horizon 7. To make the machine available again, you must reinstall Horizon Agent.

Prerequisites

Verify that the registered machines that you want to remove are not being used in any desktop pool.

Procedure

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

2 Click the **RDS Hosts** tab.

3 Select one or more machines and click **Remove**.

You can select only machines that are not being used by a desktop pool.

4 Click **OK** to confirm.

Troubleshooting Machines and Desktop Pools

You can use a variety of procedures to diagnose and fix problems that you encounter when you create and use machines and desktop pools.

Users might experience difficulty when they use Horizon Client to access desktops and applications. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

Display Problem Machines in Horizon Console

You can display a list of the machines whose operation Horizon 7 has detected as being suspect.

Horizon Console displays machines that exhibit the following problems:

- Are powered on, but which are not responding.

- Remain in the provisioning state for a long time.

- Are ready, but which report that they are not accepting connections.

- Appear to be missing from a vCenter Server.

- Have active logins on the console, logins by users who are not entitled, or logins not made from a Connection Server instance.

Procedure

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

2 On the **vCenter** tab, click **Problem Machines** from the Machines drop-down menu.

What to do next

The action that you should take depends on the problem that Horizon Console reports for a machine.

- If a machine is powered on, but does not respond, restart its virtual machine. If the machine still does not respond, verify that the version of the Horizon Agent is supported for the machine operating system. You can use the `vdmadmin` command with the `-A` option to display the Horizon Agent version. For more information, see the *View Administration* document.

- If a machine remains in the provisioning state for a long time, delete its virtual machine, and clone it again. Verify that there is sufficient disk space to provision the machine.

- If a machine reports that it is ready, but does not accept connections, check the firewall configuration to make sure that the display protocol is not blocked.

- If a machine appears to be missing from a vCenter Server, verify whether its virtual machine is configured on the expected vCenter Server, or if it has been moved to another vCenter Server.

- If a machine has an active login, but this is not on the console, the session must be remote. If you cannot contact the logged-in users, you might need to restart the virtual machine to forcibly log out the users.

Verify User Assignment for Desktop Pools

For dedicated user assignments, you can verify if the user that is assigned to the virtual machine is the user that connects to the virtual desktop or not.

Prerequisites

- Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.

- Verify that you have entitled users to the desktop pool.

Procedure

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

2 On the **vCenter** tab, choose to view the assigned user or connected user.

Option	Description
Assigned User	The **Assigned User** column displays the user who is assigned to the desktop pool. **Note** The **Assigned User** column does not display any user for a floating desktop pool.
Connected User	The **Connected User** column displays the user who is connected to the virtual machine. Most of the time, the **Connected User** is the same as the **Assigned User** when the assigned user is connected to the desktop. At other times, when an administrator is connected to the virtual machine, the **Connected User** column displays the administrator.

Restart Desktops and Reset Virtual Machines in Horizon Console

You can perform a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. You can perform 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.

Table 4-11. Reset and Restart Functionality

Pool Type	Reset Functionality (Pools, Machines, Sessions, and Horizon Clients)	Restart Functionality (Pools, Machines, Sessions, and Horizon Clients)
Full-clone pool (dedicated pool and floating pool without delete on logOff option enabled)	Reset the VM (Power Off and Power On VM)	Restart the VM (Graceful OS restart)
Instant-clone pool (floating pool)	**Power Off VM > Delete VM > Create new VM > Power On**	**Graceful OS shut down > Delete VM > Create new VM > Power On**
Published desktop pools	NA (Not Supported)	NA (Not Supported)

Note The restart functionality is available for Horizon Clients 4.4 and later.

Procedure

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

2 On the **vCenter** tab, choose to restart a virtual desktop or reset a virtual machine.

Option	Description
Restart Desktop	Restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.
Reset Virtual Machine	Resets the virtual machine without a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.

3 Click **OK**.

Send Messages to Desktop Users in Horizon Console

You might sometimes need to send messages to users who are currently logged into desktops. For example, if you need to perform maintenance on machine, you can ask the users to log out temporarily, or warn them of a future interruption of service. You can send a message to multiple users.

Procedure

1   In Horizon Console, click **Inventory > Desktops**.

2   Click a pool ID and click the **Sessions** tab.

3   Select one or more machines and click **Send Message**.

4   Type the message, select the message type, and click **OK**.

    A message type can be **Info**, **Warning**, or **Error**.

The message is sent to all selected machines in active sessions.

Manage Machines and Policies for Unentitled Users in Horizon Console

You can display the machines that are allocated to users whose entitlement has been removed, and you can also display the policies that have been applied to unentitled users.

A user who is unentitled might have left the organization permanently, or you might have suspended their account for an extended period of time. These users are assigned a machine but they are no longer entitled to use the machine pool.

You can also use the `vdmadmin` command with the `-O` or `-P` option to display unentitled machines and policies. For more information, see the *Horizon 7 Administration* document.

Procedure

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

2   Select **More Commands > View Unentitled Machines**.

3   Remove the machine assignments for unentitled users.

4   Select **More Commands > View Unentitled Machines** or **More Commands > View Unentitled Policies** as appropriate.

5   Change or remove the policies that are applied to unentitled users.

Creating Published Desktops and Applications in Horizon Console

5

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

This chapter includes the following topics:

- Creating Farms in Horizon Console
- Creating Published Desktop Pools in Horizon Console
- Creating Application Pools in Horizon Console
- Managing Farms in Horizon Console
- Managing Application Pools in Horizon Console
- Managing RDS Hosts in Horizon Console
- Manage Published Desktop and Application Sessions in Horizon Console

Creating Farms in Horizon Console

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.

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

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

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 7 Administration* document.

Worksheet for Creating a Manual Farm in Horizon Console

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

Table 5-1. 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 5-1. Worksheet: Configuration Settings for Creating a Manual Farm (Continued)

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

Create a Manual Farm in Horizon Console

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 "Setting Up Remote Desktop Services Hosts," in the *Setting Up Published Desktops and Applications in Horizon 7* document.

- Verify that all the RDS hosts have the Available status. In Horizon Console, select **Inventory > 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 Console.

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.

Worksheet for Creating an Automated Instant-Clone Farm in Horizon Console

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

Table 5-2. 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**.	

Table 5-2. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
3D Renderer	Select 3D graphics rendering for desktops. 3D rendering is supported on Windows 2008, Windows 2012, and Windows 2016 guests running on VMs with virtual hardware version 11 or later. The hardware-based renderer is supported (at minimum) on virtual hardware version 11 and above in a vSphere 6.0 U1 and above environment. The software renderer is supported (at minimum) on virtual hardware version 11 in a vSphere 6.0 U1 and above environment. On ESXi 5.0 hosts, the renderer allows a maximum VRAM size of 128MB. On ESXi 5.1 and later hosts, the maximum VRAM size is 512MB. On hardware version 11 (HWv11) virtual machines in vSphere 6.0, the VRAM value (video memory) has changed. Select the Manage Using vSphere Client option and configure video memory for these machines in vSphere Web Client. For details, see "Configuring 3D Graphics" in the vSphere Virtual Machine Administration guide. 3D rendering is disabled if you select Microsoft RDP as the default display protocol and do not allow users to choose a display protocol. ■ **NVIDIA GRID vGPU**. 3D rendering is enabled for NVIDIA GRID vGPU. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. You cannot use vSphere Distributed Resource Scheduler (DRS) when you select this option. To use NVIDIA GRID vGPU for an instant-clone desktop pool, the recommendation is to select VMware Blast as a protocol and not allow the user to choose their own display protocols. ■ **Manage using vSphere Client**. The 3D Renderer option that is set in vSphere Web Client (or vSphere Client in vSphere 5.1 or later) for a virtual machine determines the type of 3D graphics rendering that takes place. Horizon 7 does not control 3D rendering. In the vSphere Web Client, you can configure the **Automatic**, **Software**, or **Hardware** options. These options have the same effect as they do when you set them in Horizon Console. Use this setting when configuring vDGA and AMD Multiuser GPU Using vDGA. This setting is also an option for vSGA. When you select the **Manage using vSphere Client** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution** of any one monitor settings are inactive in Horizon Console. You can configure the amount of memory in vSphere Web Client. ■ **Disabled**. 3D rendering is inactive. Default is disabled.	
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 5-2. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never**, **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 session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to published desktops and applications is allowed. Check the **Enabled** box to allow HTML Access to published desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	
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 server	Determines the maximum number of sessions that an RDS host can support. Select **Unlimited** or **No More Than ...**. The default is **Unlimited**.	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	

Table 5-2. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
Naming pattern	Specify a prefix or a name format. Horizon 7 will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify **{n}** anywhere in a character string and **{n}** will be replaced by the number. You can also specify **{n:fixed=<number of digits>}**, where **fixed=<number of digits>** indicates the number of digits to be used for the number. For example, specify **vm-{n:fixed=3}-sales** and the machine names will be vm-001-sales, vm-002-sales, and so on. **Note** Each machine name, including the automatically generated number, has a 15-character limit.	
Max number of machines	The number of machines to be provisioned.	
Minimum number of ready (provisioned) machines during Instant Clone maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while Connection Server performs maintenance operations on the machines in the farm. This setting is not honored if you schedule immediate maintenance.	
Use 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.	
Parent VM	Select a parent virtual machine from the list. Be aware that the list includes virtual machines that do not have View Composer Agent installed. You must not select any of those machines because View Composer Agent is required. A good practice is to use a naming convention that indicates whether a virtual machine has View Composer Agent installed.	
Snapshot	Select the snapshot of the parent virtual machine to use as the base image for the farm. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no instant clones in the farm use the default image, and no more instant clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new instant clones in the farm, according to farm policies. The parent virtual machine and snapshot are also required for Connection Server maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	

Table 5-2. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

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

Table 5-2. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (Continued)

Setting	Description	Fill in Your Value Here
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 7 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 7 creates an instant clone. This option is disabled by default.	
Use ClonePrep	Provide a ClonePrep customization specification to customize the virtual machines. ■ **Power-off script name**. Name of the customization script that ClonePrep runs on instant-clone machines before they are powered off. Provide the path to the script on the parent virtual machine. ■ **Power-off script parameters**. Provide parameters that ClonePrep can use to run a customization script on instant-clone machines before they are powered off. For example, use p1. ■ **Post-synchronization script name**. Name of the customization script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. Provide the path to the script on the parent virtual machine. ■ **Post-synchronization script parameters**. Provide parameters for the script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. For example, use p2.	
Ready to Complete	Review the settings for the automated instant-clone farm.	

Create an Automated Instant-Clone Farm in Horizon Console

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 7 Installation* document.

■ Verify that Connection Server settings for vCenter Server are configured in Horizon Administrator. See the *Horizon 7 Administration* document.

- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools.

- Verify that you prepared a parent virtual machine. Horizon Agent must be installed on the parent virtual machine. See "Preparing a Parent Virtual Machine for an Automated Farm" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. Connection Server uses the snapshot as the base image from which the clones are created.

- Gather the configuration information you must provide to create the farm. See Worksheet for Creating an Automated Instant-Clone Farm in Horizon Console.

Procedure

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

2 Click **Add**.

3 Select **Automated Farm**.

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

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

What to do next

Create a published application or desktop pool.

Creating Published Desktop Pools in Horizon Console

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.

For more information about the properties of published desktop pools, see the *Setting Up Published Desktops and Applications in Horizon 7* document.

Worksheet for Creating Published Desktop Pools

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 5-3. 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
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

Create a Published Desktop Pool in Horizon Console

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 "Setting Up Remote Desktop Services Hosts" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

- Create a farm that contains the RDS hosts. See Creating Farms in Horizon Console.

- Decide how to configure the pool settings. See "Desktop Pool Settings for RDS Desktop Pools" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

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 Administrator. The display name is the name of the RDS desktop pool that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as the pool ID.

5   Select pool settings.

6   Select or create a farm for this pool.

What to do next

Entitle users to access the pool.

Creating Application Pools in Horizon Console

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.

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

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

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

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

An application supports the PCoIP and VMware Blast display protocols. To enable HTML Access, see the *VMware Horizon HTML Access Installation and Setup Guide* document.

Worksheet for Creating an Application Pool Manually in Horizon Console

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 5-4. Worksheet: Application Properties for Creating an Application Pool Manually

Property	Description	Fill in Your Value Here
ID	Unique name that identifies the pool in Horizon Administrator. This field is required.	
Display Name	Pool name that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as **ID**.	
Version	Version of the application.	
Publisher	Publisher of the application.	
Path	Full pathname of the application. For example, `C:\Program Files\app1.exe`. This field is required.	
Start Folder	Full pathname of the starting directory for the application.	
Parameters	Parameters to pass to the application when it starts. For example, you can specify `–username user1 –loglevel 3`.	
Description	Description of this application pool.	
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. **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 5-4. 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.	
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.	

Create an Application Pool in Horizon Console

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

Prerequisites

- Set up RDS hosts. See "Setting Up Remote Desktop Services Hosts" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

- Create a farm that contains the RDS hosts. See Creating Farms in Horizon Console.

- If you plan to add the application pool manually, gather information about the application. See Worksheet for Creating an Application Pool Manually in Horizon Console

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.

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

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 in Horizon Console.

- 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 7 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.

- Aniti-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, View 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.

Managing Farms in Horizon Console

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 in Horizon Console

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 in Horizon Console

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 in Horizon Console

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.

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 Console

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 parent virtual machine.

You can make changes to the parent virtual machine without affecting the RDS host instant clones because the snapshot of the current parent VM is used for maintenance. The instant clones created in the automated farm use the information in the parent 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 7 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 7 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 parent VM image 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 parent 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**.

Managing Application Pools in Horizon Console

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

Edit an Application Pool in Horizon Console

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 in Horizon Console

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.

Managing RDS Hosts in Horizon Console

You can manage RDS hosts that you set up manually and RDS hosts that are created automatically when you add an automated farm.

When you manually set up an RDS host, it automatically registers with Horizon Connection Server. You cannot manually register an RDS host with Connection Server. For an RDS host that you set up manually, 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 RDS host that is created automatically when you add an automated farm, 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 Horizon Console

You can change the number of connections that an RDS host can support. This setting is the only one that you can change. The default value is 150. 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 **Inventory > 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 in Horizon Console

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 Farm in Horizon Console

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 7 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 an RDS Host from Horizon 7

You can remove from Horizon 7 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 **Inventory > Registered Machines**.

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

3 Click **OK**.

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

Disable or Enable an RDS Host in Horizon Console

When you disable an RDS host, Horizon 7 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**.

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.

Monitor RDS Hosts in Horizon Console

You can monitor the status and view the properties of RDS hosts in Horizon Console.

Procedure

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

Properties	Action
RDS Host, Farm, Desktop Pool, Agent Version, Sessions, Status	▪ In Horizon Console, select **Inventory > Machines**. ▪ Click the **RDS Hosts** tab. RDS hosts that are set up manually are displayed.
DNS Name, Type, RDS Farm, Max Number of Connections, Agent Version, Enabled, Status	▪ In Horizon Console, select **Inventory > Registered Machines**. ▪ Click the **RDS Hosts** tab. Only RDS hosts that are set up manually are displayed.

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.
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.

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 5-5. 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	Horizon 7 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.

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.
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.

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**.
Restart Desktop	Performs a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine.
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.

4 Click **OK**.

Entitling Users and Groups in Horizon Console

6

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

Note Adding, removing, or reviewing entitlements is not supported for manual or linked-clone desktop pools.

This chapter includes the following topics:

- Add Entitlements to a Desktop or Application Pool in Horizon Console
- Remove Entitlements from a Desktop or Application Pool in Horizon Console
- Review Desktop or Application Pool Entitlements

Add Entitlements to a Desktop or Application Pool in Horizon Console

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

Prerequisites

Create a desktop or application pool.

Procedure

1 Select the desktop or application pool.

Option	Action
Add an entitlement for a desktop pool	In Horizon Console, select **Inventory > Desktops** and click the name of the desktop pool.
Add an entitlement for an application pool	In Horizon Console, select **Inventory > Applications** and click the name of the application pool.

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

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

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

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

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

Remove Entitlements from a Desktop or Application Pool in Horizon Console

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

Procedure

1   Select the desktop or application pool.

Option	Action
Add an entitlement for a desktop pool	In Horizon Console, select **Inventory > Desktops** and click the name of the desktop pool.
Add an entitlement for an application pool	In Horizon Console, select **Inventory > Applications** and click the name of the application pool.

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

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

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

Review Desktop or Application Pool Entitlements

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

Procedure

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

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

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

Getting Started with JMP Integrated Workflow

7

Familiarize yourself with the high level JMP Integrated Workflow concepts and finish the tasks required to get started using the JMP Integrated Workflow features.

This chapter includes the following topics:

- About JMP Integrated Workflow

- Get Started with JMP Integrated Workflow

About JMP Integrated Workflow

With VMware Horizon JMP (Just-in-Time Management Platform) Integrated Workflow features, you can use a single console to define and manage desktop workspaces for users or group of users.

A desktop workspace is created by defining a JMP assignment that includes information about the VMware Horizon desktop pools, VMware App Volumes AppStacks, and VMware User Environment Manager settings. After a JMP assignment is submitted, the JMP automation engine communicates with the Horizon 7, App Volumes, and User Environment Manager systems to entitle the user to a desktop.

You can manage existing JMP assignments using the **Assignments (JMP)** tab in Horizon Console. You can also modify each component assignment using the respective JMP component console. For example, changes to the desktop pools defined in a JMP assignment can also be modified by selecting **Inventory > Desktops** from Horizon Console.

When a JMP assignment is opened in the Horizon Console, the current state of each component of the JMP assignment is validated to ensure that it is at the expected state. When differences are identified, the affected areas are highlighted in the console and you can either accept the current state, or modify the assignment to achieve the desired state and re-entitle the user.

The JMP Integrated Workflow features become available in Horizon Console after you install and configure the VMware Horizon JMP Server. See Get Started with JMP Integrated Workflow and *VMware Horizon JMP Server Installation and Setup Guide* for information.

Note   The JMP Integrated Workflow features do not support VMware Cloud® on AWS since App Volumes does not support VMware Cloud

Get Started with JMP Integrated Workflow

To begin using the JMP Integrated Workflow features, you must install and set up JMP Server, and configure the JMP settings.

Prerequisites

Review the prerequisites and the system requirements for all the technology components that you plan to install.

Procedure

1   If necessary, set up the required administrator users and groups in Active Directory.

    See "Preparing Active Directory" in the *Horizon 7 Installation* document. The Active Directory information is required when configuring the JMP settings.

2   Set up the Microsoft SQL Server and ensure that the login credentials you plan to use during the JMP Server installation process have been created. See "Database Requirements for JMP Server" in the *VMware Horizon JMP Server Installation and Setup Guide* document for more information.

3   Install and set up VMware Horizon 7 version 7.5 or later.

    See the *Horizon 7 Installation* document.

4   (Optional) Install and set up VMware App Volumes 2.14 or later, which provides features for real-time application delivery.

    See the *VMware App Volumes Installation Guide* document for details.

5   (Optional) To provide contextual policy management, install and set up VMware User Environment Manager 9.2.1 or later.

    See the *Installing and Configuring VMware User Environment Manager* document.

6   Obtain the CA-signed SSL certificates that must be used for JMP Server to communicate securely with other servers within your organization's network.

7   Install JMP Server and configure the SSL certificates for the JMP Server to communicate with the other servers that are required for the JMP Integrated Workflow features.

    See *VMware Horizon JMP Server Installation and Setup Guide* for more information.

8   Configure the JMP settings for the first time. See Configure JMP Settings for the First Time for details.

What to do next

After successfully finishing the preceding tasks, you can now create a JMP assignment. See Creating a JMP Assignment for information.

Administering JMP Settings

<div align="right" style="font-size:3em">8</div>

After installing JMP Server, you must configure the JMP settings with the necessary credentials before you can create any JMP assignments and can get started using the JMP Integrated Workflow features. You can edit the initial JMP settings and when applicable, add new settings information.

This chapter includes the following topics:

- Configure JMP Settings for the First Time
- Managing JMP Settings

Configure JMP Settings for the First Time

Before you can create any JMP assignments, you must configure the JMP settings using Horizon Console. You must provide credentials for the Active Directory domain that you use to assign desktop workspaces for users or group of users. You can optionally include the credentials information to use App Volumes AppStacks and User Environment Manager configuration share when creating JMP assignments.

Prerequisites

- Verify that the VMware Horizon JMP Server has been successfully installed and that you have its URL. See *VMware Horizon JMP Server Installation and Setup Guide* for more information.

- Obtain the administrator account credentials for Horizon 7 version 7.5 or later that you plan to use with JMP Server.

- Obtain the Active Directory credentials that must be used with the JMP Server.

- If you are assigning applications to JMP assignments, ensure that you have the URL and administrator account credentials for the VMware App Volumes Manager instance to be used. If a load balancer manages your App Volumes Manager instances that you plan to use, obtain the URL for the load balancer and use it when configuring the App Volumes Manager information.

- If you choose to use a VMware User Environment Manager configuration share, obtain its UNC path and the administrator account credentials required to access it.

Procedure

1   In the Horizon Console, click **Settings (JMP)**.

2 Enter the JMP Server information.

    a   In the **JMP Server** tab, click **Add JMP Server**.

    b   Enter the JMP Server URL in the format of `https://jmp.yourcompany.com`.

    c   Click **Save**.

The JMP Server URL is validated. If you receive the `JMP Server is unreachable` message, verify that you had entered the correct URL, that the JMP Server is configured correctly, and that the JMP Server is reachable.

3 Enter the account information for the Horizon 7 Connection Server version 7.5 or later that you plan to use with JMP Server.

    a   Click the **Horizon 7** tab.

    b   If not auto-filled, enter the **Connection Server URL** value. This URL is the same URL as the Horizon 7 Connection Server URL to which the Horizon Console is connected.

    c   Enter your Horizon 7 service account user name and password.

    d   In the **Service Account Domain** text box, enter a valid name to be used with the JMP assignments that you are creating and press **Enter**.

    e   Click **Save**.

4 Enter the information for the Active Directory that you are going to use with the JMP assignments.

    a   Click the **Active Directory** tab.

    b   Click **New**.

    c   In the **NETBIOS Name** text box, select from the list of available NetBIOS domain names.

        The DNS Domain Name and Context text boxes are updated with default values.

    d   Verify that the default value that was added in the **DNS Domain Name** text box is the correct value to use. Optionally, enter another fully qualified Active Directory domain name. For example, `mycompany.com`.

    e   In the **Protocol** section, select the protocol used by your Active Directory.

    f   In the **Bind Username** and **Bind Password** text boxes, enter the credentials for the Bind Distinguished Name (DN) user account. For example, `administrator`.

    g   Modify the value in the **Context** text box, if you want to use a value different from the default.

        The value is used as the root for the Active Directory data search.

    h   (Optional) Click **Advanced Properties** and modify the default Port number value.

        The default Port value is based on the protocol you selected earlier. You can modify the Port value or leave the text box blank.

i   In the **Domain Controller** text box, optionally enter one or more host names or IP addresses to use for handling the Active Directory traffic.

For example, `adserver.mycompany.com, 10.111.XXX.XXX`. If the text box is left blank, the value in the **DNS Domain Name** text box is used.

j   Click **Save**.

5   If you plan to use App Volumes AppStacks when creating JMP assignments, configure the App Volumes Manager that you plan to use.

a   Click the **App Volumes** tab.

b   Click **New**.

c   In the **Name** text box, enter a name to assign to the App Volumes instance. If you leave the text box blank, the value you enter in the **App Volumes Server URL** text box is used.

d   Enter a valid URL for the App Volumes Manager that you want the JMP Server pod to be associated.

Important   If a load balancer manages the App Volumes Manager that you plan to use, enter the URL for that load balancer.

e   Enter the App Volumes Manager or load balancer administrator account credentials that your JMP Server can use to access your App Volumes Manager.

f   Enter the domain name for the App Volumes Manager service account that is to be used for the JMP assignments.

g   (Optional) If you are registering more than one App Volumes Manager, use the toggle button to indicate if the App Volumes Manager you are adding is the default server to use when creating JMP assignments. You can change the instance you want to use at the time a JMP assignment is being created.

h   Click **Save**.

6   If you are going to use a User Environment Manager configuration share when you create JMP assignments, add the information for it to the JMP settings.

a   Click the **UEM** tab.

b   Click **New**.

c   Enter a value in the **File Share UNC Path** text box in the format of `\\fileserver-name\UEM-configuration-share-pathname`. For example, `\\FileServer\UEMConfig`.

Important   Do not include `General` in the file share UNC path that you enter.

d   Enter the User Environment Manager administrator account credentials to be used to connect to the User Environment Manager configuration share.

    e   Select from the **Active Directory** list the domain name to be used with the User Environment Manager configuration share.

> **Note** An Active Directory can be associated with only one User Environment Manager configuration share.

    f   Click **Save**.

What to do next

After successfully configuring the initial JMP settings, you can now create JMP assignments. See Creating a JMP Assignment for more information.

Managing JMP Settings

You can use the Horizon Console to modify, add, or delete information for a JMP setting.

- Have the necessary information to modify the specific JMP setting.
- To modify the JMP Settings, ensure that you have the proper administrative privileges.

Edit JMP Server Settings

You can use the Horizon Console to make changes to existing JMP Server settings.

Prerequisites

- Have the necessary information to modify the specific JMP Server settings.
- Ensure you have the proper administrative privileges to log in to Horizon Console and modify the JMP Server settings

Procedure

1. In Horizon Console, select **Settings (JMP)**.
2. In the JMP Settings pane, click the **JMP Server** tab.
3. Click **Edit**.
4. Enter a new **JMP Server URL**.
5. Click **Save**.

The new JMP Server URL is validated and if it is invalid, an error message appears.

Edit Horizon 7 Credentials

Use the Horizon Console to make changes to the existing Horizon 7 Connection Server credentials.

Procedure

1. In Horizon Console, click **Settings (JMP)**.

2 Click the **Horizon 7** tab.

3 Click **Edit Credentials**.

4 Enter a new user name in the **Service Account User Name**, if necessary.

5 Enter a new password in the **Service Account Password**, if necessary.

6 Change the value in the **Service Account Domain**, if necessary.

7 Click **Save**.

Edit the Horizon Connection Server URL

If you want to associate existing JMP assignments to a different Horizon Connection Server, you must modify the Horizon Connection Server URL that is registered with the JMP Server settings that is associated with those JMP assignments.

There is no user interface in Horizon Console that allows you to modify the Horizon Connection Server information. You must use the SQL Server Management Studio to modify the existing Horizon Connection Server host URL in the JMP settings.

Prerequisites

- Ensure that you have the proper system administrator privileges to log in to a SQL Server Management Studio session and access to the SQL Server database that you created for JMP Server.

- Back up your SQL Server database before proceeding with the database modifications.

Procedure

1 If you are currently logged in to a Horizon Console session, log out.

2 Log in to a SQL Server Management Studio session as the sysadmin (SA) or using a user account with SA privileges.

3 Verify that the replacement Horizon Connection Server host URL that you plan to use is not already registered to another JMP Server instance.

For example, if the replacement Horizon Connection Server host URL is `new-horizon-host.com`, use the following SQL statement to verify it is not already registered.

```
SELECT * from  xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

4 If the previous SQL statement did not return any results, proceed to the next step. Otherwise, use the following statement to delete the information for the existing Horizon Connection Server host.

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

5   Update the existing JMP Server settings using the following statements, where `new-horizon-server-host.com` is the URL of the replacement Horizon Connection Server host and the `old-horizon-host.com` is the URL of currently registered Horizon Connection Server host.

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
    AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

6   Log in to Horizon Console using the new Horizon Connection Server URL and verify that the new Horizon Connection Server host is now associated with your existing JMP assignments that were previously associated with the old Horizon Connection Server host.

Add Active Directory Domains

If you need to add another Active Directory domain after setting the initial one, use the Horizon Console.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **Active Directory** tab and click **Add**.

3   In the **NETBIOS Name** text box, select from the list of available NetBIOS domain names.

    The DNS Domain Name and Context text boxes are updated with default values.

4   In the **DNS Domain Name** text field, verify the default value added after the NETBIOS Name was updated. Optionally, enter another fully qualified Active Directory domain name. For example, `mycompany.com`.

5   In the **Protocol** section, select the protocol used by your Active Directory.

6   In the **Bind Username** and **Bind Password** text fields, enter the credentials for the Bind Distinguished Name (DN) user account, such as Administrator.

7   Modify the value in the **Context** text field, if you want to use a value different from the default.

8   (Optional) Click **Advanced Properties** and modify the default Port number value.

    The default Port value is based on the protocol you selected earlier. You can modify the Port value or leave the text field blank.

9   In the **Domain Controller** text field, optionally enter one or more host names or IP addresses to use for handling the Active Directory traffic.

10 Click **Save**.

Information about the newly added Active Directory domain appears in the Active Directory table.

Edit Active Directory Domain Information

If certain information has changed since you initially configured the JMP settings, use the Horizon Console to modify the Active Directory domain settings information.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **Active Directory** tab.

3   Select one of the rows in the table of Active Directory domains and click **Edit**.

4   Modify the Active Directory information that has to be updated.

5   Click **Save**.

Delete Active Directory Domain Information

Use Horizon Console if you must delete an existing Active Directory (AD) domain settings information.

You can only delete information about a registered Active Directory domain from a JMP setting if that domain is not in use by any existing JMP assignments.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **Active Directory** tab.

3   Select the table row for the Active Directory domain that you want to delete from JMP Settings.

4   In the delete confirmation dialog box appears, read the message and click **Delete** to confirm that you do want to delete this Active Directory domain information.

If there are no JMP assignments that use the Active Directory domain, it is removed.

If the Active Directory domain is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the Active Directory domain. You can delete the domain information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Add App Volumes Information

Use Horizon Console to add information for any additional App Volumes Managers that can be used when creating JMP assignments.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **App Volumes** tab and click **Add**.

The **Add App Volumes Instance** dialog box appears.

3   In the **Name** text box, enter a unique name to assign to the App Volumes instance. If you leave the text box blank, the value you enter in the **App Volumes Server URL** text box is used.

4   In the **App Volumes Server URL** text box, enter a valid URL for the App Volumes Manager that you want to associate with your JMP Server. If a load balancer manages the App Volumes Manager that you are adding, enter the URL for that load balancer.

> **Note**   If the App Volumes Managers you have added are connected to different SQL databases, information about the App Volumes Manager that you add appears in the App Volumes tab. If the App Volumes Managers are connected to the same SQL database, only the information about the previously registered App Volumes Manager appears on the App Volumes tab.

5   Enter the App Volumes administrator user name and password that your JMP Server can use to access your App Volumes Manager.

6   Enter the domain name for the App Volumes service account that is used for the JMP assignments.

7   To make the App Volumes Manager that you are currently adding as the default App Volumes Manager server to use when JMP assignments are created, click the toggle button. You can change the server you want to use at the time a JMP assignment is being created.

The toggle button changes to the blue color with a **Yes** label.

8   Click **Save**.

Edit the App Volumes Instance Information

If you must modify existing information about the App Volumes instance that is being used by the JMP assignments, use the Horizon Console to modify the information.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **App Volumes** tab and select the table row for the App Volumes instance that you want to modify.

3   Click **Edit**.

The **Add App Volumes Instance** dialog box appears.

4   Modify the App Volumes instance information that has to be updated.

5   Click **Save**.

Delete App Volumes Instance Information

Use Horizon Console if you must delete existing settings information about an App Volumes instance.

You can only delete information about a registered App Volumes instance from a JMP setting if that instance is not being used by any JMP assignments.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **App Volumes** tab.

3   Select the row for the App Volumes instance information that you want to delete from the JMP Settings.

4   Click **Delete** to confirm that you do want to delete this App Volumes instance information.

If there are no JMP assignments that use the App Volumes instance, it is removed.

If the App Volumes instance is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the App Volumes instance. You can delete the App Volumes instance information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Add User Environment Manager Configuration Share Information

Use the Horizon Console if you must add another User Environment Manager configuration share information after setting the initial one.

You can add only one User Environment Manager configuration share per AD domain. So, the configuration share that you are about to add cannot have the same IP or DNS address as the configuration shares that are already included in your JMP server settings.

Procedure

1   In Horizon Console, click **Settings (JMP)**.

2   Click the **UEM** tab and click **Add**.

The **Add UEM File Share** dialog box appears.

3   Enter a value in the **File Share UNC Path** text box in the format of *server-name\UEM-configuration-share-pathname*.

For example, if the configuration share location is \\<IP-address>\uemshare\config\general\FlexRepository\.., the path you need to enter in the **File Share UNC Path** text box is **\\<IP-address>\uemshare\config**.

4   Enter the User Environment Manager user name and password that must be used to connect to the User Environment Manager configuration file share.

5   From the **Active Directory** list, select the domain name to use with the User Environment Manager configuration file share.

Note   An Active Directory can be associated with only one User Environment Manager configuration file share.

6 Click **Save**.

The information about the User Environment Manager configuration file share is added to the JMP settings and a new row is added to the table in the **UEM** tab.

Edit the User Environment Manager Configuration File Share Information

Use the Horizon Console if you must modify existing information about the User Environment Manager configuration file share that is being used by the JMP assignments.

Procedure

1 In Horizon Console, click **Settings (JMP)**.

2 Click the **UEM** tab and from the table of existing information, select the row for the User Environment Manager configuration file share that you want to modify.

3 Click **Edit**.

The **Edit UEM File Share** dialog box appears.

4 Modify the User Environment Manager configuration file share information that has to be updated.

5 Click **Save**.

Delete User Environment Manager Configuration Share Information

Use Horizon Console if you must delete existing settings information about a User Environment Manager configuration share.

You can only delete information about a registered User Environment Manager configuration share from a JMP setting if that configuration share is not being used by any JMP assignments.

Procedure

1 In Horizon Console, click **Settings (JMP)**.

2 Click the **UEM** tab.

3 Select the row for the User Environment Manager configuration share information that you want to delete from JMP Settings.

4 Click **Delete** to confirm that you do want to delete this User Environment Manager configuration share information.

If there are no JMP assignments that use the User Environment Manager configuration share, it is removed.

If the User Environment Manager configuration share is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the User Environment Manager configuration share. You can delete the User Environment Manager configuration share information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Administering JMP Assignments 9

After you install theJMP Server and configure the JMP settings, you can begin using the JMP Integrated Workflow features to create, modify, duplicate, or delete JMP assignments.

You must first install JMP Server and configure the JMP settings before you can start creating JMP assignments. See *VMware Horizon JMP Server Installation and Setup Guide* and Configure JMP Settings for the First Time for more information.

Ensure that the following pre-requisites are met before you create, edit, duplicate, or delete JMP assignments.

- Verify that the Horizon 7 instance that is registered with the JMP setting is up and running.

- Ensure that there is at least one Active Directory domain registered with the JMP setting.

- Verify that the App Volumes instance that you registered with the JMP setting is up and running.

- Verify that the User Environment Manager configuration share defined in the JMP setting is up and running.

Note   Global entitlements are not supported.

When you are attempting to create, edit, duplicate, or delete a JMP assignment, you might receive a message saying that the attempted action did not complete successfully. For example, some problems might be encountered while attempting to reach one of the underlying JMP technology components and the assignment validation fails to complete successfully. On the JMP Assignment summary screen, you can try to correct the problem by selecting one of the following options.

- Click **Edit** to correct the issues manually.

- Click **Repair** to have the JMP Server attempt to fix the issues found on the current JMP assignment.

- Click **Force Delete** to remove the JMP assignment completely.

This chapter includes the following topics:

- Creating a JMP Assignment

- Editing a JMP Assignment

- Duplicating a JMP Assignment

- Deleting a JMP Assignment

Creating a JMP Assignment

Using Horizon Console, you can create JMP assignments, which you use to create desktop workspaces for users or group of users.

You select the Horizon desktops pools, App Volumes AppStacks, and User Environment Manager settings to define a JMP assignment.

Prerequisites

Ensure that the pre-requisites listed in Chapter 9 Administering JMP Assignments have been met.

Procedure

1 In Horizon Console, click **Assignments (JMP)**.

2 Click **New**.

3 In the **Users** tab of the New Assignment wizard, enter a couple of characters next to the Active Directory drop list and select the users or group of users to include in the new JMP assignment .

   Your selection is added in the Selected Users/Groups section.

4 Click **Next**.

5 In the **Desktops** tab, select the desktop pool you want to include in the JMP assignment, and click **Next**.

6 In the **Applications** tab, click the check box next to the name of the application that you want to include in the JMP assignment. When done with your selection, click **Next**.

7 In the **User Environment** tab, decide whether you are going to configure the JMP assignment with any of the available user environment settings.

   ■ With **Disable UEM Settings?** set to **No**, clicking **Skip** means that the User Environment Manager assignment file is not going to be saved to the User Environment Manager configuration share. All the User Environment Manager settings are going to be applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.

   ■ With **Disable UEM Settings?** set to **No**, select the user environment settings that you want applied to the JMP assignment being created. Clicking **Next** creates the User Environment Manager assignment file with the selected user environment settings. The selected settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.

   ■ With **Disable UEM settings?** set to **Yes**, the list of available user environment settings are removed from view. When you click **Next**, an empty assignment file is written to the User Environment Manager configuration share. Disabling User Environment Manager settings ensures that no user environment settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.

8 In the **Definitions** tab, accept the default name for the JMP assignment or replace the name with another, and optionally add a description.

9 In the **AppStack Attach** drop list, select when the AppStack is to be attached to the JMP assignment and click **Next**.

10 In the **Summary** tab, review the details for the new assignment. If they are acceptable, click **Submit**. If changes must be made, click **Back** to make the adjustments.

The new JMP assignment is queued for storage into the JMP database and is added to the list of assignments in the JMP Assignments pane. After the JMP assignment is successfully added to the JMP database, the status changes from the Pending state. It becomes selectable from the JMP assignment list so you can edit, duplicate, or delete it.

You can also verify the assignments or entitlements that were created for the new JMP assignment using the following information.

- To verify information about the Horizon desktop pool created for the JMP assignment, use Horizon Console. Select **Inventory > Desktops** and locate the desktop pool created by JMP Server.

- To view the AppStacks information created by JMP Server for the new JMP assignment, use the App Volumes Manager console. Select **Volumes > AppStacks** and locate the AppStacks created by JMP Server.

- To verify the user environment settings you configured for the JMP assignment, use the User Environment Manager Management Console and click the **User Environment** tab. From the left-side pane, select the user environment setting used by the JMP assignment and click the **Assignments** tab from the resulting dialog box to view the JMP assignment information for that user environment setting.

Editing a JMP Assignment

You might need to modify an existing JMP assignment due to changes with the components that were used to define it. You can use Horizon Console to make the necessary changes to the JMP assignment.

Prerequisites

- Ensure that the pre-requisites listed in Chapter 9 Administering JMP Assignments have been met.

- The JMP assignment you plan to edit must not be in a "Pending" state.

Procedure

1 In Horizon Console, click **Assignments (JMP)**.

2 Select the JMP assignment you want to edit either by clicking the check box or the JMP assignment's name in the list.

3 Click **Edit**.

4　In the Edit Assignment wizard, modify the current settings.

Click **Cancel** if you want to discontinue at any point during the editing process.

a　If you want to remove any of the currently selected users or groups, click the delete icon (**X**).

b　Click **Next**.

c　In the **Desktops** tab, select a desktop pool that you want included in the JMP assignment. Click **Next**.

d　In the **Applications** tab, select the available applications that you want added to the JMP assignment or deselect the ones that were previously selected. Click **Next**.

e　In the **User Environment** tab, decide whether you are going to configure the JMP assignment with any of the available user environment settings.

- With **Disable UEM Settings?** set to **No**, clicking **Skip** means that the User Environment Manager assignment file is not going to be saved to the User Environment Manager configuration share. All the User Environment Manager settings are going to be applied on the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.

- With **Disable UEM Settings?** set to **No**, select the user environment settings that you want applied to the JMP assignment being created. Clicking **Next** creates the User Environment Manager assignment file with the selected user environment settings. The selected settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.

- With **Disable UEM settings?** set to **Yes**, the list of available user environment settings are removed from view. When you click **Next**, an empty assignment file is written to the User Environment Manager configuration share. Disabling User Environment Manager settings ensures that no user environment settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.

f　In the **Definitions** tab, if applicable, modify the current values in the **Name**, **Description**, or when to attach the AppStack to the JMP assignment.

g　Click **Next**.

h　Review the summary of the changes you made and click **Submit** to save the modifications.

If successful, the changes are saved. If there are any problems encountered, additional information is provided and any possible action that you can take are displayed.

Duplicating a JMP Assignment

You can create JMP assignments more quickly by duplicating existing JMP assignments that are similar to what you want to create.

Prerequisites

- Ensure that the pre-requisites listed in Chapter 9 Administering JMP Assignments have been met.

- The JMP assignment you plan to duplicate must not be in a "Pending" or "Error" state.

Procedure

1 From Horizon Console, select **Assignments (JMP)**.

2 Select the JMP assignment you want to duplicate and click **Duplicate**.

3 In the New Assignment wizard, modify the duplicated JMP assignment as needed.

  a Select new users or groups, or remove any of the currently selected users or groups. Click **Next**.

  b In the Desktops pane, select a new desktop pool or remove any of the desktop pools that was included in the duplicated JMP assignment. Click **Next**.

  c Select additional applications to include in the new JMP assignment and deselect ones that are currently selected. Click **Next**.

  d In the User Environment pane, select the User Environment Manager setting you want to apply to the new JMP assignment. Click **Next**.

  e In the Definitions name, replace the default name created, if you want. Add a description and specify when you want the AppStack to be attached to the new JMP assignment.

  f Click **Next** and review the summary of the details of the new JMP assignment.

  g If the information is satisfactory, click **Submit**. Otherwise, click **Back** to make any corrections.

The new JMP assignment is validated, which can take some time. After it is successfully validated, the newly created JMP assignment is added to the list on the JMP Assignments pane. When you point over its name, you see that it is in a pending state until it is successfully saved to the JMP database. After the JMP assignment is no longer in a pending state, you can take any additional action on the assignment.

Deleting a JMP Assignment

Use the Horizon Console to delete a JMP assignment.

When a JMP assignment is deleted, the Horizon pool entitlement, AppStack assignment, and UEM entitlement associated with the JMP assignment are deleted. However, if the Horizon pool entitlement or AppStack assignment used by the JMP assignment existed before the JMP assignment creation, they are not deleted. After you delete a JMP assignment, it no longer applies to users or desktops.

Prerequisites

- Verify that the pre-requisites listed in Chapter 9 Administering JMP Assignments have been met.

- The JMP assignment you plan to delete must not be in a "Pending" state.

Procedure

1 In Horizon Console, click **Assignments (JMP)**.

2   In the JMP Assignments pane, select one or more of the JMP assignments and click **Delete**.

3   In the confirmation dialog box, click **Delete** to confirm that you want to delete the assignment permanently.

If successful, the Horizon pool entitlement is removed from the JMP database and removed from the list in the JMP Assignments pane.

If a part of the delete operation fails, the JMP assignment is not deleted. Clicking the status indicators can provide more information on why the delete operation failed.

Using Horizon Help Desk Tool in Horizon Console

10

Horizon Help Desk Tool is a Web application that you can use to get the status of Horizon 7 user sessions and to perform troubleshooting and maintenance operations.

In Horizon Help Desk Tool, you can look up user sessions to troubleshoot problems and perform desktop maintenance operations such as restart or reset desktops.

To configure Horizon Help Desk Tool, you must meet the following requirements:

■ Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon 7. To verify that you have the correct license, see the *Horizon 7 Administration* document.

■ An event database to store information about Horizon 7 components. For more information about configuring an event database, see the *Horizon 7 Installation* document.

■ The Help Desk Administrator role or the Help Desk Administrator (Read Only) role to log in to Horizon Help Desk Tool. For more information on these roles, see the *Horizon 7 Administration* document.

■ Enable the timing profiler on each Connection Server instance to view logon segments.

   Use the following `vdmadmin` command to enable the timing profiler on each Connection Server instance:

   ```
   vdmadmin -I -timingProfiler -enable
   ```

   Use the following `vdmadmin` command to enable the timing profiler on a Connection Server instance that uses a management port:

   ```
   vdmadmin -I -timingProfiler -enable -server {ip/server}
   ```

This chapter includes the following topics:

■ Start Horizon Help Desk Tool in Horizon Console

■ Troubleshooting Users in Horizon Help Desk Tool

■ Session Details for Horizon Help Desk Tool

■ Session Processes for Horizon Help Desk Tool

■ Application Status for Horizon Help Desk Tool

■   Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool

Start Horizon Help Desk Tool in Horizon Console

Horizon Help Desk Tool is integrated into Horizon Console. You can search for a user that you want to troubleshoot problems for in Horizon Help Desk Tool.

Procedure

1   In Horizon Console, enter a user name in the User Search field.

   Horizon Console displays a list of users in the search results. The search can return up to 100 matching results.

2   Select a user name.

   The user information appears in a user card.

What to do next

To troubleshoot problems, click the related tabs in the user card.

Troubleshooting Users in Horizon Help Desk Tool

In Horizon Help Desk Tool, you can view basic user information in a user card. You can click tabs in the user card to get more details about specific components.

The user details can sometimes appear in tables. You can sort these user details by table columns.

■   To sort a column by ascending order, click the column once.

■   To sort a column by descending order, click the column twice.

■   To not sort the column, click the column thrice.

Basic User Information

Displays basic user information such as user name, phone number, and email address of the user and the connected or disconnected status of the user. If the user has a desktop or application session, the status of the user is connected. If the user does not have any desktop or application sessions, the status of the user is disconnected.

You can click the email address to send a message to the user.

You can also click the phone number to open a Skype for Business session to call the user to collaborate with the user on a troubleshooting task.

Note   The Skype for Business information is not displayed for Linux desktop users.

Sessions

The **Sessions** tab displays information about desktop or application sessions that the user is connected to.

You can use the **Filter** text box to filter desktop or application sessions.

Note The **Sessions** tab does not display session information for sessions that use the Microsoft RDP display protocol or sessions that access VMs from vSphere Client or ESXi.

The **Sessions** tab includes the following information:

Table 10‑1. Sessions tab

Option	Description
State	Displays information about the state of the desktop or application session. ■ Appears green, if the session is connected. ■ L, if the session is a local session or a session running in the local pod.
Computer Name	Name of the desktop or application session. Click the name to open the session information in a card. You can click the tabs in the session card to view additional information: ■ The **Details** tab displays the user information such as the VM information, CPU, or memory usage. ■ The **Processes** tab displays information about CPU and memory related processes. ■ The **Applications** tab displays the details about the applications that are running. **Note** You cannot access the **Applications** tab for Linux desktop sessions.
Protocol	Display protocol for the desktop or application session.
Type	Displays whether the desktop is a published desktop, virtual machine desktop, or an application.
Connection Time	The time the session connected to Connection Server.
Session Duration	The duration of time the session remained connected to Connection Server.

Desktops

The **Desktops** tab displays information about the published desktops or virtual desktops that the user is entitled to use.

Table 10‑2. Desktops

Option	Description
State	Displays information about the state of the desktop session. ■ Appears green, if the session is connected.
Desktop Pool Name	Name of the desktop pool for the session. Displays Linux as the desktop pool for a Linux desktop session.

Table 10-2. Desktops (Continued)

Option	Description
Desktop Type	Displays whether the desktop is a published desktop or virtual machine desktop.
	Note Does not display any information if the session is running in a different pod in the pod federation.
Type	Displays information about the type of desktop entitlement. ■ Local, for a local entitlement.
vCenter	Displays the name of the virtual machine in vCenter Server.
	Note Does not display any information if the session is running in a different pod in the pod federation.
Default Protocol	Default display protocol for the desktop or application session.

Applications

The **Applications** tab displays information about the published applications that the user is entitled to use.

Note You cannot access the **Applications** tab for Linux desktop sessions.

Table 10-3. Applications

Option	Description
State	Displays information about the state of the application session. ■ Appears green, if the session is connected.
Applications	Displays the names of published applications in the application pool.
Farm	Name of the farm that contains the RDS host that the session connects to.
	Note If there is a global application entitlement, this column shows the number of farms in the global application entitlement.
Type	Displays information about the type of application entitlement. ■ Local, for a local entitlement.
Publisher	Software manufacturer name of the published application.

Activities

The **Activities** tab displays the event log information about the user's activities. You can filter activities by a time range such as the Last 12 hours or Last 30 Days or by administrator name. Click **Help Desk Event Only** to filter only by Horizon Help Desk Tool activities. Click the refresh icon to refresh the event log. Click the export icon to export the event log as a file.

Note The event log information is not displayed for users in a Cloud Pod Architecture environment.

Table 10-4. Activities

Option	Description
Time	Select a time range. Default is the last 12 hours. ■ **Last 12 Hours** ■ **Last 24 Hours** ■ **Last 7 Days** ■ **Last 30 Days** ■ **All**
Admins	Name of the administrator user.
Message	Displays messages for a user or administrator that are specific to the activities that the user or administrator performed.
Resource Name	Displays information about the desktop pool or virtual machine name on which the activity was performed.

Session Details for Horizon Help Desk Tool

The session details appear on the **Details** tab when you click a user name in the **Computer Name** option on the **Sessions** tab. You can view details for Horizon Client, the virtual or published desktop, and CPU and memory details.

Horizon Client

Displays information that depends on the type of Horizon Client and includes details such as user name, version of Horizon Client, IP address of the client machine, and the operating system of the client machine.

Note If you upgraded Horizon Agent, you must also upgrade Horizon Client to the latest version. Else, no version is displayed for Horizon Client. For more information about upgrading Horizon Client, see the *Horizon 7 Upgrades* document.

VM

Displays information about virtual desktops or published desktops.

Table 10-5. VM Details

Option	Description
Computer Name	Name of the desktop or application session.
Agent Version	Horizon Agent version.
OS Version	Operating System version.
Connection Server	The Connection Server that the session connects to.
Pool	Name of the desktop or application pool. Displays Linux for a Linux desktop pool.
vCenter	IP address of vCenter Server.
Session State	State of the desktop or application session. The session states can be idle, active, or disconnected. If the user is not active for one minute, the session status turns idle. The status icon appears as green outline for idle, solid green for active, and gray for disconnected. **Note** Linux desktop sessions do not display the idle status.
Session Duration	The time the session remained connected to Connection Server.
State Duration	The time the session remained in the same state.
Logon Time	The logon time of the user who logged in to the session.
Logon Duration	The time the user remained logged in to the session.
Gateway/Proxy Name	Name of the security server, Unified Access Gateway appliance, or load balancer. This information might take from 30 seconds through 60 seconds to display after connecting to the session.
Gateway/Proxy IP	IP address of the security server, Unified Access Gateway appliance, or load balancer. This information might take from 30 seconds through 60 seconds to display after connecting to the session.
Farm	The farm of RDS hosts for the published desktop or application session.

User Experience Metrics

Displays performance details for a virtual or published desktop session that uses the PCoIP or VMware Blast display protocol. To view these performance details, click **More**. To refresh these details, click the refresh icon.

Table 10-6. PCoIP Display Protocol Details

Option	Description
Tx Bandwidth	The transmission bandwidth, in kilobits per second, in a PCoIP session.
Frame Rate	The frame rate, in frames per second, in a PCoIP session.

Table 10-6. PCoIP Display Protocol Details (Continued)

Option	Description
Packet Loss	Percentage of packet loss in a PCoIP session.
Skype Status	The Skype for Business status in a PCoIP session. ■ Optimized ■ Fallback ■ Optimized (version-mismatch) ■ Fallback (version-mismatch) ■ Connecting ■ Disconnected ■ Undefined This option appears as N/A for Linux desktop sessions.

Table 10-7. Blast Display Protocol Details

Option	Description
Frame Rate	The frame rate, in frames per second, in a Blast session.
Skype Status	The Skype for Business status in a Blast session. ■ Optimized ■ Fallback ■ Optimized (version-mismatch) ■ Fallback (version-mismatch) ■ Connecting ■ Disconnected ■ Undefined This option appears as N/A for Linux desktop sessions.
Blast Session Counters	■ **Estimated Bandwidth (Uplink)**. Estimated bandwidth for an uplink signal. ■ **Packet Loss (Uplink)**. Percentage of packet loss for an uplink signal.
Blast Imaging Counters	■ **Transmitted Bytes**. Total number of bytes for imaging data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for imaging data that have been received for a Blast session.
Blast Audio Counters	■ **Transmitted Bytes**. Total number of bytes for audio data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for audio data that have been received for a Blast session.
Blast CDR Counters	■ **Transmitted Bytes**. Total number of bytes for Client Drive Redirection data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for Client Drive Redirection data that have been received for a Blast session.

CPU and Memory Usage and Network and Disk Performance

Displays charts for CPU and memory usage of the virtual or published desktop or application and the network or disk performance for the PCoIP or Blast display protocol.

Note Following a start or a restart of Horizon Agent on the desktop, the performance charts might not display the timeline immediately. The timeline appears after a few minutes.

Table 10-8. CPU Usage

Option	Description
Session CPU	CPU usage of the current session.
Host CPU	CPU usage of the virtual machine to which the session is assigned.

Table 10-9. Memory Usage

Option	Description
Session Memory	Memory usage of the current session.
Host Memory	Memory usage of the virtual machine to which the session is assigned.

Table 10-10. Network Performance

Option	Description
Latency	Displays a chart for the latency for the PCoIP or Blast session.
	For the Blast display protocol, the latency time is the Round-Trip Time in milliseconds. The performance counter that tracks this latency time is **VMware Blast Session Counters > RTT**.
	For the PCoIP display protocol, the latency time is the Round-Trip Latency time in milliseconds. The performance counter that tracks this latency time is **PCoIP Session Network Statistics > Round Trip Latency**.

Table 10-11. Disk Performance

Option	Description
Read	The number of read Input/Output (I/O) operations per second.
Write	The number of write I/O operations per second.
Disk Latency	Displays a chart for the disk latency. The disk latency is the time in milliseconds from the Input/Output Operations Per Second (IOPS) data retrieved from the Windows performance counters.
Average Read	Average number of random read I/O operations per second.
Average Write	Average number of random write I/O operations per second.
Average Latency	Average latency time in milliseconds from the IOPS data retrieved from the Windows performance counters.

Session Logon Segments

Displays the logon duration and usage segments that are created during logon.

Table 10-12. Session Logon Segments

Option	Description
Logon duration	The length of time calculated from the time the user clicks the desktop or application pool to the time when Windows Explorer starts.
Session Logon Time	The length of time that the user was logged in to the session.
Logon Segments	Displays the segments that are created during logon. ■ **Brokering**. Total time for Connection Server to process a session connect or reconnect. Calculated from the time the user clicks the desktop pool to the time when the tunnel connection is set up. Includes the times for Connection Server tasks such as user authentication, machine selection, and machine preparation for setting up the tunnel connection. ■ **GPO load**. Total time for Windows group policy processing. Displays 0 if there is no global policy configured. ■ **Profile load**. Total time for Windows user profile processing. ■ **Interactive**. Total time for Horizon Agent to process a session connect or reconnect. Calculated from the time when PCoIP or Blast Extreme uses the tunnel connection to the time when Windows Explorer starts. ■ **Protocol Connection**. Total time taken for the PCoIP or Blast protocol connection to complete during the logon process. ■ **Logon Script**. Total time taken for a logon script to execute from start to completion. ■ **Authentication**. Total time for Connection Server to authenticate the session. ■ **VM Start**. Total time taken to start a VM. This time includes the time for booting the operating system, resuming a suspended machine, and the time it takes Horizon Agent to signal that it is ready for a connection.

Use the following guidelines when you use the information in logon segments for troubleshooting:

■ If the session is a new virtual desktop session, all the logon segments appear. If no global policy is configured, the **GPO Load** logon segment time is 0.

■ If the virtual desktop session is a reconnected session from a disconnected session, the **Logon Duration**, **Interactive**, and **Brokering** logon segments appear.

■ If the session is a published desktop session, the **Logon Duration**, **GPO Load**, or the **Profile load** logon segments appear. The **GPO Load** and **Profile load** logon segment appear for new sessions. If these logon segments do not appear for new sessions, you must restart the RDS host.

- If the session is a Linux desktop session, the **GPO Load** and **Profile load** segments do not appear.

- Logon data might not be immediately available when the desktop session connects. The logon data appears after a few minutes.

Session Processes for Horizon Help Desk Tool

The session processes appear on the **Processes** tab when you click a user name in the **Computer Name** option on the **Sessions** tab.

Processes

For each session, you can view additional details about CPU and memory related processes. For example, if you notice that the CPU and memory usage for a session is abnormally high, you can view the details for the process on the **Processes** tab.

For RDS host sessions, the **Processes** tab displays the current RDS host session processes started by the current user or current system process.

Table 10-13. Session Process Details

Option	Description
Process Name	Name of the session process. For example, chrome.exe.
CPU	CPU usage of the process in percent.
Memory	Memory usage of the process in KB.
Disk	Memory disk IOPs. Calculated using the following formula: (Total I/O bytes of current time) - (Total I/O bytes one second before the current time). This calculation can display a value of 0 KB per second if the Task Manager displays a positive value.
Username	User name of the user who owns the process.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Processes	Count of processes in the virtual machine
Refresh	The refresh icon refreshes the list of processes.
End Process	Ends a process that is running. **Note** You must have the Help Desk Administrator role to end a process. To end a process, select a process and click the **End Process** button. You cannot end critical processes such as Windows core processes that might be listed in the **Processes** tab. If you end a critical process, Horizon Help Desk Tool displays a message that states it cannot end the system process.

Application Status for Horizon Help Desk Tool

You can view the status and details of an application on the **Applications** tab when you click a user name in the **Computer Name** option on the **Sessions** tab. You cannot access the **Applications** tab for Linux desktop sessions.

Applications

For each application, you can view the current status and other details.

You can end an application process for the end user. To end an application process, click **End Application** and click **OK** to confirm the change.

Note The end application process can fail if the application is pending a user interaction such as unsaved data or because of other exceptions. However, Horizon Help Desk Tool does not display any success or failure message when you end an application.

Table 10-14. Application Details

Option	Description
Application	Name of the application.
Description	Description of the application.
Status	Status of the application. Displays whether the application is running or not.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Applications	List of applications that are running.
Refresh	The refresh icon refreshes the list of applications.

Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool

In Horizon Help Desk Tool, you can troubleshoot desktop or application sessions based on a user's connection status.

Prerequisites

■ Start Horizon Help Desk Tool.

Procedure

1 On the user card, click the **Sessions** tab.

A performance card appears that displays CPU and memory usage and includes information about Horizon Client, and the virtual or published desktop.

2 Choose a troubleshooting option.

Option	Action
Send Message	Sends a message to the user on the published desktop or virtual desktop. You can choose the severity of the message to include Warning, Info, or Error. Click **Send Message** and enter the type of severity and the message details, and then click **Submit**.
Remote Assistance	You can generate remote assistance tickets for connected desktop or application sessions. Administrators can use the remote assistance ticket to take control of a user's desktop and troubleshoot problems. **Note** This feature is not available for Linux desktop users. Click **Remote Assistance** and download the Help Desk ticket file. Open the ticket and wait for the ticket to be accepted by the user on the remote desktop. You can open the ticket only on a Windows desktop. After the user accepts the ticket, you can chat with the user and request control of the user's desktop. **Note** The Help Desk remote assistance feature is based on Microsoft Remote Assistance. You must install Microsoft Remote Assistance and enable the Remote Assistance feature on the published desktop. Help Desk remote assistance might not start if Microsoft Remote Assistance has connection or upgrade issues. For more information, see the Microsoft Remote Assistance documentation on the Microsoft Web site.
Restart	Initiates the Windows Restart process on the virtual desktop. This feature is not available for a published desktop or application session. Click **Restart VDI**.
Disconnect	Disconnect the desktop or application session. Click **More > Disconnect**.
Log Off	Initiates the log off process for a published desktop or virtual desktop, or the log off process for an application session. Click **More > Log Off**.
Reset	Initiates a reset of the virtual machine. This feature is not available for a published desktop or application session. Click **More > Reset VM**. **Note** The user can lose unsaved work.