Horizon Console Administration

JUL 2019

VMware Horizon 7 7.9

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.

For information about how to use Horizon Console to configure and manage a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

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 data center 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 13 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:

- Servers
  - Horizon Connection Server configuration
  - Event database
- Entitlements
  - User and group entitlements
  - Desktop entitlements

  - Application entitlements
  - Global entitlements
  - Global policies
- Authentication
  - Remote access authentication
  - Unauthenticated access for published applications
  - Smart card authentication
  - Role-based delegated administration
- 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
  - Persistent disks
- Published desktops
  - Manual farms
  - Automated instant-clone farms
  - Automated linked-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
- Cloud Pod Architecture

The following features are not supported:

- Cloning an automated desktop pool
- 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.

Configuring Horizon Connection Server in Horizon Console

3

After you install and perform initial configuration of Horizon Connection Server, you can add vCenter Server instances and Horizon Composer services to your Horizon 7 deployment, set up roles to delegate administrator responsibilities, and schedule backups of your configuration data.

This chapter includes the following topics:

Configuring vCenter Server and Horizon Composer in Horizon Console

To use virtual machines as remote desktops, you must configure Horizon 7 to communicate with vCenter Server. To create and manage linked-clone desktop pools, you must configure Horizon Composer settings in Horizon Console.

You can also configure storage settings for Horizon 7. You can allow ESXi hosts to reclaim disk space on linked-clone virtual machines. To allow ESXi hosts to cache virtual machine data, you must enable Horizon Storage Accelerator for vCenter Server.

Create a User Account for Horizon Composer AD Operations

If you use Horizon Composer, you must create a user account in Active Directory that allows Horizon Composer to perform certain operations in Active Directory. Horizon Composer requires this account to join linked-clone virtual machines to your Active Directory domain.

To ensure security, create a separate user account to use with Horizon Composer. By creating a separate account, you can guarantee that it does not have additional privileges that are defined for another purpose. You can give the account the minimum privileges that it needs to create and remove computer objects in a specified Active Directory container. For example, the Horizon Composer account does not require domain administrator privileges.

Procedure

1. In Active Directory, create a user account in the same domain as your Connection Server host or in a trusted domain.
2. Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

   The following list shows all the required permissions for the user account, including permissions that are assigned by default:

   - List Contents
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Reset Password
   - Create Computer Objects
   - Delete Computer Objects

   Note Fewer permissions are required if you select the **Allow reuse of pre-existing computer accounts** setting for a desktop pool. Make sure that the following permissions are assigned to the user account:

   - List Contents
   - Read All Properties
   - Read Permissions
   - Reset Password
3. Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

What to do next

Specify the account in Horizon Console when you configure Horizon Composer domains in the **Add vCenter Server** wizard and when you configure and deploy linked-clone desktop pools.

Install the Product License Key in Horizon Console

Before you can use Connection Server, you must enter a product license key.

Note The product license key is not required if you have a Horizon 7 subscription license. For more information about subscription licenses, see "Enabling Horizon 7 for Subscription Licenses," in the *Horizon 7 Installation* document.

The first time you log in, Horizon Console displays the Licensing and Usage page.

You do not have to configure a license key when you install a replicated Connection Server instance or a security server. Replicated instances and security servers use the common license key stored in the View LDAP configuration.

Note Connection Server requires a valid license key. The product license key is a 25-character key.

Procedure

1. In Horizon Console, select **Settings > Product Licensing and Usage**.
2. In the **Licensing Settings** panel, click **Edit License**.
3. Enter the license serial number and click **OK**.
4. Verify the license expiration date.
5. Verify that the Desktop, Application Remoting, and View Composer licenses are enabled or disabled, based on the edition of VMware Horizon 7 that your product license entitles you to use.

   Not all features and capabilities of VMware Horizon 7 are available in all editions. For a comparison of feature sets in each edition, see http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf.

Add vCenter Server Instances to Horizon 7 in Horizon Console

You must configure Horizon 7 to connect to the vCenter Server instances in your Horizon 7 deployment. vCenter Server creates and manages the virtual machines that Horizon 7 uses in desktop pools.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to Horizon 7 separately.

Horizon 7 connects to the vCenter Server instance using a secure channel (TLS).

Prerequisites

- Install the Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support Horizon 7. To use Horizon Composer, you must give the user additional privileges.

  For details about configuring a vCenter Server user for Horizon 7, see the *Horizon 7 Installation* document.

- Verify that a TLS server certificate is installed on the vCenter Server host. In a production environment, install a valid certificate that is signed by a trusted Certificate Authority (CA).

  In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to Horizon 7.

- Verify that all Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the **Trusted Root Certification Authorities > Certificates** folder in the Windows local computer certificate stores on the Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

  See "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store," in the *Horizon 7 Installation* document.

- Verify that the vCenter Server instance contains ESXi hosts. If no hosts are configured in the vCenter Server instance, you cannot add the instance to Horizon 7.

- If you upgrade to vSphere 5.5 or a later release, verify that the domain administrator account that you use as the vCenter Server user was explicitly assigned permissions to log in to vCenter Server by a vCenter Server local user.

- If you plan to use Horizon 7 in FIPS mode, verify that you have vCenter Server 6.0 or later and ESXi 6.0 or later hosts.

  For more information, see "Installing Horizon 7 in FIPS Mode," in the *Horizon 7 Installation* document.

- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server and Horizon Composer.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.

2. On the **vCenter Server** tab, click **Add**.

3. In the vCenter Server Settings **Server address** text box, type the fully qualified domain name (FQDN) of the vCenter Server instance.

   The FQDN includes the host name and domain name. For example, in the FQDN `*myserverhost*.*companydomain*.com`, `*myserverhost*` is the host name and `*companydomain*.com` is the domain.

   Note If you enter a server by using a DNS name or URL, Horizon 7 does not perform a DNS lookup to verify whether an administrator previously added this server to Horizon 7 by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4. Type the name of the vCenter Server user.

   For example: `domain\user` or `user@domain.com`

5. Type the vCenter Server user password.

6. (Optional) Type a description for this vCenter Server instance.

7. Type the TCP port number.

   The default port is 443.

8. (Optional) Select **VMware Cloud on AWS**, if the vCenter Server is deployed on VMware Cloud on AWS.

   For more information about integrating Horizon 7 with VMware Cloud on AWS, see the *Horizon 7 Integration* document.

9. Under Advanced Settings, set the concurrent operations limits for vCenter Server and Horizon Composer operations.

10. Click **Next** and follow the prompts to complete the wizard.

What to do next

Configure Horizon Composer settings.

- If the vCenter Server instance is configured with a signed TLS certificate, and Connection Server trusts the root certificate, the Add vCenter Server wizard displays the Horizon Composer Settings page.
- If the vCenter Server instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See, Accept the Thumbprint of a Default TLS Certificate.

If Horizon 7 uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Configure Horizon Composer Settings

To use Horizon Composer, you must configure settings that allow Horizon 7 to connect to the Horizon Composer service. Horizon Composer can be installed on its own separate host or on the same host as vCenter Server.

There must be a one-to-one mapping between each Horizon Composer service and vCenter Server instance. A Horizon Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one Horizon Composer service.

After the initial Horizon 7 deployment, you can migrate the Horizon Composer service to a new host to support an expanding or changing Horizon 7 deployment. You can edit the initial Horizon Composer settings in Horizon Console, but you must perform additional steps to ensure that the migration succeeds.

Prerequisites

- Verify that you created a user in Active Directory with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. See Create a User Account for Horizon Composer AD Operations.
- Verify that you configured Horizon 7 to connect to vCenter Server. To do so, you must complete the vCenter Server Information page in the Add vCenter Server wizard. See Add vCenter Server Instances to Horizon 7 in Horizon Console.

- Verify that this Horizon Composer service is not already configured to connect to a different vCenter Server instance.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **vCenter Server** tab, click **Add** and complete the vCenter Server information on the **vCenter Server Settings** page, then click **Next**.
3. On the **Horizon Composer Settings** page, if you are not using Horizon Composer, select **Do not use Horizon Composer**.

   If you select **Do not use Horizon Composer**, the other Horizon Composer settings become inactive. When you click **Next**, the Add vCenter Server wizard displays the **Storage Settings** page.
4. If you are using Horizon Composer, select the location of the Horizon Composer host.

Option	Description
Horizon Composer is installed on the same host as vCenter Server.	a Select **Horizon Composer co-installed with the vCenter Server**. b Make sure that the port number is the same as the port that you specified when you installed the Horizon Composer service on vCenter Server. The default port number is 18443.
Horizon Composer is installed on its own separate host.	a Select **Standalone Horizon Composer Server**. b In the Horizon Composer server address text box, type the fully qualified domain name (FQDN) of the Horizon Composer host. c Type the name of the Horizon Composer user. For example: `domain.com\user` or `user@domain.com` d Type the password of the Horizon Composer user. e Make sure that the port number is the same as the port that you specified when you installed the Horizon Composer service. The default port number is 18443.

5. Click **Next** to display the **Horizon Composer domains** page.

What to do next

Configure Horizon Composer domains.

- If the Horizon Composer instance is configured with a signed TLS certificate, and Connection Server trusts the root certificate, the Add vCenter Server wizard displays the Horizon Composer Domains page.
- If the Horizon Composer instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate.

Configure Horizon Composer Domains

You must configure an Active Directory domain in which Horizon Composer deploys linked-clone desktops. You can configure multiple domains for Horizon Composer. After you first add vCenter Server and Horizon Composer settings to Horizon 7, you can add more Horizon Composer domains by editing the vCenter Server instance in Horizon Console.

Prerequisites

- Your Active Directory administrator must create a Horizon Composer user for AD operations. This domain user must have permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. For information about the required permissions for this user, see Create a User Account for Horizon Composer AD Operations.
- In Horizon Console, verify that you completed the **vCenter Server Settings** and **Horizon Composer Settings** pages in the **Add vCenter Server** wizard.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **vCenter Server** tab, click **Add** and complete the vCenter Server information on the **vCenter Server Settings** page, then click **Next**.
3. On the **Horizon Composer Settings** page, if you are using Horizon Composer, select the location of the Horizon Composer host and click **Next**.

   For more information on Horizon Composer, see Configure Horizon Composer Settings.
4. On the **Horizon Composer Domains** page, click **Add** to add the Horizon Composer user for AD operations account information.
5. Type the domain name of the Active Directory domain.

   For example: `domain.com`
6. Type the domain user name, including the domain name, of the Horizon Composer user.

   For example: `domain.com\admin`
7. Type the account password.
8. Click **OK**.
9. To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.
10. Click **Next** to display the **Storage Settings** page.

What to do next

Enable virtual machine disk space reclamation and configure Horizon Storage Accelerator for Horizon 7.

Add an Instant-Clone Domain Administrator in Horizon Console

Before you create an instant-clone desktop pool, you must add an instant-clone domain administrator to Horizon 7.

Prerequisites

- Verify that the instant-clone domain administrator has the required Active Directory domain privileges. For more information, see "Create a User Account for Instant-Clone Operations" in the *Horizon 7 Installation* document.

Procedure

1. In Horizon Console, select **Settings > Instant Clone Domain Accounts**.
2. Click **Add**.
3. Select the domain for the instant-clone domain administrator.
4. Enter the user name and password.

What to do next

In Horizon Console, you can add or remove an instant-clone domain administrator or export the list of instant-clone administrators to Microsoft Excel. Navigate to **Settings > Instant Clone Domain Accounts** and select an instant-clone domain administrator. Click **Edit** to edit the domain and login information for the administrator. Click **Remove** to remove an administrator. Click the export icon to export the list of instant-clone administrators to a Microsoft Excel file.

Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines

In vSphere version 5.1 or later, you can enable the disk space reclamation feature for Horizon 7. Horizon 7 creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones, reducing the total storage space required for linked clones.

As users interact with linked-clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with their remote desktops.

Disk space reclamation is especially useful for deployments that cannot take advantage of storage-saving strategies such as refresh on logoff. For example, knowledge workers who install user applications on dedicated remote desktops might lose their personal applications if the remote desktops were refreshed or recomposed. With disk space reclamation, Horizon 7 can maintain linked clones at close to the reduced size they start out with when they are first provisioned.

This feature has two components: space-efficient disk format and space reclamation operations.

In a vSphere version 5.1 or later, when a parent virtual machine is virtual hardware version 9 or later, Horizon 7 creates linked clones with space-efficient OS disks, whether or not space reclamation operations are enabled.

To enable space reclamation operations, you must use Horizon Console to enable space reclamation for vCenter Server and reclaim VM disk space for individual desktop pools. The space reclamation setting for vCenter Server gives you the option to disable this feature on all desktop pools that are managed by the vCenter Server instance. Disabling the feature for vCenter Server overrides the setting at the desktop pool level.

The following guidelines apply to the space reclamation feature:

- It operates only on space-efficient OS disks in linked clones.
- It does not affect Horizon Composer persistent disks.

- It works only with vSphere version 5.1 or later on virtual machines that are virtual hardware version 9 or later.
- It does not operate on full-clone desktops.
- It operates on virtual machines with SCSI controllers. IDE controllers are not supported.

Native NFS snapshot technology (VAAI) is not supported in pools that contain virtual machines with space-efficient disks.

Prerequisites

- Verify that your vCenter Server and ESXi hosts, including all ESXi hosts in a cluster, are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.

Procedure

1 In Horizon Console, navigate to **Settings > Servers**.

2 On the **vCenter Server** tab, click **Add** and complete the **Add vCenter Server** wizard pages that precede the **Storage Settings** page.

3 On the **Storage Settings** page, select **Reclaim VM Disk Space**.

This option is selected by default if you are performing a fresh installation of Horizon 7. You must select **Reclaim VM Disk Space** if you are upgrading to a later release of Horizon 7.

What to do next

On the **Storage Settings** page, configure Horizon Storage Accelerator.

To finish configuring disk space reclamation in Horizon 7, set up space reclamation for desktop pools.

Configure Horizon Storage Accelerator for vCenter Server

In vSphere, you can configure ESXi hosts to cache virtual machine disk data. This feature, called Horizon Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. Horizon Storage Accelerator improves Horizon 7 performance during I/O storms, which can take place when many virtual machines start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. Instead of reading the entire OS or application from the storage system over and over, a host can read common data blocks from cache.

By reducing the number of IOPS during boot storms, Horizon Storage Accelerator lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your Horizon 7 deployment.

You enable caching on your ESXi hosts by selecting the Horizon Storage Accelerator setting in the **Add vCenter Server** wizard in Horizon Console, as described in this procedure.

Make sure that Horizon Storage Accelerator is also configured for individual desktop pools. To operate on a desktop pool, Horizon Storage Accelerator must be enabled for vCenter Server and for the individual desktop pool.

Horizon Storage Accelerator is enabled for desktop pools by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool. If you enable the feature by editing an existing pool, you must ensure that a new replica and its digest disks are created before linked clones are provisioned. You can create a new replica by recomposing the pool to a new snapshot or rebalancing the pool to a new datastore. Digest files can only be configured for the virtual machines in a desktop pool when they are powered off.

You can enable Horizon Storage Accelerator on desktop pools that contain linked clones and pools that contain full virtual machines.

Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for Horizon Storage Accelerator.

Horizon Storage Accelerator is now qualified to work in configurations that use Horizon 7 replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using Horizon Storage Accelerator with Horizon 7 replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. Hence, this combination is tested and supported.

Important If you plan to use this feature and you are using multiple Horizon 7 pods that share some ESXi hosts, you must enable the Horizon Storage Accelerator feature for all pools that are on the shared ESXi hosts. Having inconsistent settings in multiple pods can cause instability of the virtual machines on the shared ESXi hosts.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.1 or later.

  In an ESXi cluster, verify that all the hosts are version 5.1 or later.

- Verify that the vCenter Server user was assigned the **Host > Configuration > Advanced settings** privilege in vCenter Server.

  See the topics in the *Horizon 7 Installation* document that describe Horizon 7 and Horizon Composer privileges required for the vCenter Server user.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **vCenter Server** tab, click **Add** and complete the **Add vCenter Server** wizard pages that precede the **Storage Settings** page.
3. On the **Storage Settings** page, select **Enable Horizon Storage Accelerator**.

   This option is selected by default.
4. Specify a default host cache size.

   The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.

   The default value is 1,024MB. The cache size must be between 100MB and 2,048MB.

5 To specify a different cache size for an individual ESXi host, select an ESXi host and click **Edit cache size**.

   a In the Host cache dialog box, check **Override default host cache size**.

   b Type a **Host cache size** value between 100MB and 2,048MB and click **OK**.

6 On the Storage Settings page, click **Next**.

7 After reviewing the settings on the **Ready to Complete** page, click **Submit**.

What to do next

Configure settings for client sessions and connections. See, "Configuring Settings for Client Sessions," in the *Horizon 7 Administration* document.

To complete Horizon Storage Accelerator settings in Horizon 7, configure Horizon Storage Accelerator for desktop pools. See "Configure Horizon Storage Accelerator for Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document.

Concurrent Operations Limits for vCenter Server and Horizon Composer

When you add vCenter Server to Horizon 7 or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server and Horizon Composer.

You configure these options in the Advanced Settings panel on the **vCenter Server Settings** page in the **Add vCenter Server** wizard.

Table 3-1. Concurrent Operations Limits for vCenter Server and Horizon Composer

Setting	Description
Max concurrent vCenter provisioning operations	Determines the maximum number of concurrent requests that Connection Server can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to full virtual machines only.
Max concurrent power operations	Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by Connection Server in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms This setting applies to full virtual machines and linked clones.

Setting	Description
Max concurrent Horizon Composer maintenance operations	Determines the maximum number of concurrent Horizon Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this Horizon Composer instance. The default value is 12. Remote desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on remote desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on remote desktops that require logoffs is 12. This setting applies to linked clones only.
Max concurrent Horizon Composer provisioning operations	Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this Horizon Composer instance. The default value is 8. This setting applies to linked clones only.
Max concurrent Instant Clone Engine operations	Determines the maximum number of concurrent creation and deletion operations that can take place on instant clones managed by this vCenter Server instance. This setting applies to instant clones only.

Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on remote desktop virtual machines in a vCenter Server instance. This limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see "Architecture Design Elements and Planning Guidelines" in the *Horizon 7 Architecture Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.

The system waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server and Horizon Composer instances to Horizon 7, you must ensure that the TLS certificates that are used for the vCenter Server and Horizon Composer instances are valid and trusted by Connection Server. If the default certificates that are installed with vCenter Server and Horizon Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or Horizon Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

Note If you install vCenter Server and Horizon Composer on the same Windows Server host, they can use the same TLS certificate, but you must configure the certificate separately for each component.

For details about configuring TLS certificates, see "Configuring TLS Certificates for Horizon 7 Servers" in the *Horizon 7 Installation* document.

You first add vCenter Server and Horizon Composer in Horizon Console by using the **Add vCenter Server** wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and vCenter Server.

After these servers are added, you can reconfigure them in the **Edit vCenter Server** dialog box.

Note You also must accept a certificate thumbprint when you upgrade from an earlier release and a vCenter Server or Horizon Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

Procedure

1 When Horizon Console displays an Invalid Certificate Detected dialog box, click **View Certificate**.

2 Examine the certificate thumbprint in the Certificate Information window.

3 Examine the certificate thumbprint that was configured for the vCenter Server or Horizon Composer instance.

   a On the vCenter Server or Horizon Composer host, start the MMC snap-in and open the Windows Certificate Store.

   b Navigate to the vCenter Server or Horizon Composer certificate.

   c Click the Certificate Details tab to display the certificate thumbprint.

   Similarly, examine the certificate thumbprint for a SAML authenticator. If appropriate, take the preceding steps on the SAML authenticator host.

4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or Horizon Composer instance.

   Similarly, verify that the thumbprints match for a SAML authenticator.

5 Determine whether to accept the certificate thumbprint.

Option	Description
The thumbprints match.	Click **Accept** to use the default certificate.
The thumbprints do not match.	Click **Reject**. Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or Horizon Composer.

Remove a vCenter Server Instance from Horizon 7

You can remove the connection between Horizon 7 and a vCenter Server instance. When you do so, Horizon 7 no longer manages the virtual machines created in that vCenter Server instance.

Prerequisites

Delete all the virtual machines that are associated with the vCenter Server instance. For more information about deleting virtual machines, see "Delete a Desktop Pool" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

1 In Horizon Console, navigate to **Settings > Servers**.

2 On the **vCenter Servers** tab, select the vCenter Server instance.

3 Click **Remove**.

   A dialog message warns you that Horizon 7 will no longer have access to the virtual machines that are managed by this vCenter Server instance.

4 Click **OK**.

Horizon 7 can no longer access the virtual machines created in the vCenter Server instance.

Remove Horizon Composer from Horizon 7

You can remove the connection between Horizon 7 and the Horizon Composer service that is associated with a vCenter Server instance.

Before you disable the connection to Horizon Composer, you must remove from Horizon 7 all the linked-clone virtual machines created by Horizon Composer. Horizon 7 prevents you from removing Horizon Composer if any associated linked clones still exist. After the connection to Horizon Composer is disabled, Horizon 7 cannot provision or manage new linked clones.

Procedure

1 Remove the linked-clone desktop pools created by Horizon Composer.

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

   b Select a linked-clone desktop pool and click **Delete**.

   A dialog box warns that you will permanently delete the linked-clone desktop pool from Horizon 7. If the linked-clone virtual machines are configured with persistent disks, you can detach or delete the persistent disks.

   c Click **OK**.

   The virtual machines are deleted from vCenter Server. In addition, the associated Horizon Composer database entries and the replicas created by Horizon Composer are removed.

   d Repeat these steps for each linked-clone desktop pool created by Horizon Composer.

2 Navigate to **Settings > Servers**.

3 On the **vCenter Servers** tab, select the vCenter Server instance with which Horizon Composer is associated.

4 Click **Edit**.

5 On the **Horizon Composer** tab, under Horizon Composer Server Settings, select **Do not use Horizon Composer**, and click **OK**.

You can no longer create linked-clone desktop pools in this vCenter Server instance, but you can continue to create and manage full virtual-machine desktop pools in the vCenter Server instance.

What to do next

If you intend to install Horizon Composer on another host and reconfigure Horizon 7 to connect to the new Horizon Composer service, you must perform certain additional steps. For more information on how to migrate Horizon Composer without linked-clone virtual machines, see the *Horizon 7 Administration* document.

Conflicting vCenter Server Unique IDs

If you have multiple vCenter Server instances configured in your environment, an attempt to add a new instance might fail because of conflicting unique IDs.

Problem

You try to add a vCenter Server instance to Horizon 7, but the unique ID of the new vCenter Server instance conflicts with an existing instance.

Cause

Two vCenter Server instances cannot use the same unique ID. By default, a vCenter Server unique ID is randomly generated, but you can edit it.

Solution

1 In vSphere Client, click **Administration > vCenter Server Settings > Runtime Settings**.

2 Type a new unique ID and click **OK**.

For details about editing vCenter Server unique ID values, see the vSphere documentation.

Backing Up Horizon Connection Server in Horizon Console

After you complete the initial configuration of Horizon Connection Server, you should schedule regular backups of your Horizon 7 and Horizon Composer configuration data.

For information about backing up and restoring your Horizon 7 configuration, see Backing Up Horizon Connection Server and Horizon Composer Data.

Configuring Settings for Client Sessions in Horizon Console

You can configure global settings that affect the client sessions and connections that are managed by a Connection Server instance or replicated group. You can set the session timeout length, display prelogin and warning messages, and set security-related client connection options.

Global Settings for Client Sessions in Horizon Console

General global settings determine session timeout lengths, SSO enablement and timeout limits, status updates in Horizon Console, whether prelogin and warning messages are displayed, whether Horizon Console treats Windows Server as a supported operating system for remote desktops, and other settings.

Changes to any of the settings in the following table take effect immediately. You do not need to restart Horizon 7 Connection Server or Horizon Client.

Table 3-2. General Global Settings for Client Sessions

Setting	Description
View Administrator session timeout	Determines how long an idle Horizon Console session continues before the session times out. **Important** Setting the Horizon Console session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Console. Use caution when you allow an idle session to persist a long time. By default, the Horizon Console session timeout is 30 minutes. You can set a session timeout from 1 to 4320 minutes (72 hours).
Forcibly disconnect users	Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to Horizon 7. All desktops and applications will be disconnected at the same time regardless of when the user opened them. For clients that do not support application remoting, a maximum timeout value of 1200 minutes applies if the value of this setting is **Never** or greater than 1200 minutes. The default is **After 600 minutes**.
Single sign-on (SSO)	If SSO is enabled, Horizon 7 caches a user's credentials so that the user can launch remote desktops or applications without having to provide credentials to log in to the remote Windows session. The default is **Enabled**. If you plan to use the True SSO feature, introduced in Horizon 7 or later, SSO must be enabled. With True SSO, if a user logs in using some other form of authentication than Active Directory credentials, the True SSO feature generates short-term certificates to use, rather than cached credentials, after users log in to VMware Identity Manager. **Note** If a desktop is launched from Horizon Client, and the desktop is locked, either by the user or by Windows based on a security policy, and if the desktop is running Horizon 7 Agent 6.0 or later or Horizon Agent 7.0 or later, Horizon 7 Connection Server discards the user's SSO credentials. The user must provide login credentials to launch a new desktop or a new application, or reconnect to any disconnected desktop or application. To enable SSO again, the user must disconnect from Horizon 7 Connection Server or exit Horizon Client, and reconnect to Horizon 7 Connection Server. However, if the desktop is launched from Workspace ONE or VMware Identity Manager and the desktop is locked, SSO credentials are not discarded.
Enable automatic status updates	Determines if status updates appear in the global status pane in the upper-left corner of Horizon Console every few minutes. The dashboard page of Horizon Console is also updated every few minutes. By default, this setting is not enabled.

Setting	Description
For clients that support applications. **If the user stops using the keyboard and mouse, disconnect their applications and discard SSO credentials:**	Protects application sessions when there is no keyboard or mouse activity on the client device. If set to **After ... minutes**, Horizon 7 disconnects all applications and discards SSO credentials after the specified number of minutes without user activity. Desktop sessions are not disconnected. Users must log in again to reconnect to the applications that were disconnected or launch a new desktop or application. This setting also applies to the True SSO feature. After SSO credentials are discarded, users are prompted for Active Directory credentials. If users logged in to VMware Identity Manager without using AD credentials and do not know what AD credentials to enter, users can log out and log in to VMware Identity Manager again to access their remote desktops and applications. **Important** Users must be aware that when they have both applications and desktops open, and their applications are disconnected because of this timeout, their desktops remain connected. Users must not rely on this timeout to protect their desktops. If set to **Never**, Horizon 7 never disconnects applications or discards SSO credentials due to user inactivity. The default is **Never**.
Other clients. **Discard SSO credentials:**	Discards SSO credentials after the specified number of minutes. This setting is for clients that do not support application remoting. If set to **After ... minutes**, users must log in again to connect to a desktop after the specified number of minutes has passed since the user logged in to Horizon 7, regardless of any user activity on the client device. If set to **Never**, Horizon 7 stores SSO credentials until the user closes Horizon Client, or the **Forcibly disconnect users** timeout is reached, whichever comes first. The default is **After 15 minutes**.
Display a pre-login message	Displays a disclaimer or another message to Horizon Client users when they log in. Type your information or instructions in the text box in the Global Settings dialog box. To display no message, leave the check box unselected.

Display warning before forced logoff	Displays a warning message when users are forced to log off because a scheduled or immediate update such as a desktop-refresh operation is about to start. This setting also determines how long to wait after the warning is shown before the user is logged off.
	Check the box to display a warning message.
	Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is 5 minutes.
	Type your warning message. You can use the default message:
	`Your desktop is scheduled for an important update and`
	`will be shut down in 5 minutes. Please save`
	`any unsaved work now.`

Enable Windows Server desktops	Determines whether you can select available Windows Server 2008 R2 and Windows Server 2012 R2 machines for use as desktops. When this setting is enabled, Horizon Console displays all available Windows Server machines, including machines on which Horizon 7 server components are installed. **Note** The Horizon Agent software cannot coexist on the same virtual or physical machine with any other Horizon 7 server software component, including a security server, Horizon 7 Connection Server, or Horizon 7 Composer.

Setting	Description
Clean up credential when tab closed for HTML Access	Removes a user's credentials from cache when a user closes a tab that connects to a remote desktop or application, or closes a tab that connects to the desktop and application selection page, in the HTML Access client. When this setting is enabled, Horizon 7 also removes the credentials from cache in the following HTML Access client scenarios: ■ A user refreshes the desktop and application selection page or the remote session page. ■ The server presents a self-signed certificate, a user launches a remote desktop or application, and the user accepts the certificate when the security warning appears. ■ A user runs a URI command in the tab that contains the remote session. When this setting is disabled, the credentials remain in cache. This feature is disabled by default. **Note** This feature is available in Horizon 7 version 7.0.2 and later.
Hide server information in client user interface	Enable this security setting to hide server URL information in Horizon Client 4.4 or later.
Hide domain list in client user interface	Enable this security setting to hide the Domain drop-down menu in Horizon Client 4.4 or later. When users log in to a Connection Server instance for which the **Hide domain list in client user interface** global setting is enabled, the Domain drop-down menu is hidden in Horizon Client and users provide domain information in the Horizon Client **User name** text box. For example, users must enter their user name in the format `domain\username` or `username@domain`. **Important** If you enable the **Hide domain list in client user interface** setting and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching prevents users from entering domain information in the user name text box and login always fails. This does not apply to Horizon Client version 5.0 and later if there is a single user domain. **Important** For more information about the security and usability implications of this setting, see the *Horizon 7 Security* document.

Global Security Settings for Client Sessions and Connections in Horizon Console

Global security settings determine whether clients are reauthenticated after interruptions, message security mode is enabled, and security status is enhanced.

TLS is required for all Horizon Client connections and Horizon Console connections to Horizon 7. If your Horizon 7 deployment uses load balancers or other client-facing, intermediate servers, you can off-load TLS to them and then configure non-TLS connections on individual Connection Server instances and security servers.

Table 3-3. Global Security Settings for Client Sessions and Connections

Setting	Description
Reauthenticate secure tunnel connections after network interruption	Determines if user credentials must be reauthenticated after a network interruption when Horizon clients use secure tunnel connections to remote desktops. When you select this setting, if a secure tunnel connection is interrupted, Horizon Client requires the user to reauthenticate before reconnecting. This setting offers increased security. For example, if a laptop is stolen and moved to a different network, the user cannot automatically gain access to the remote desktop without entering credentials. When this setting is not selected, the client reconnects to the remote desktop without requiring the user to reauthenticate. This setting has no effect when the secure tunnel is not used.
Message security mode	Determines the security mechanism used for sending JMS messages between components ■ When the mode is set to **Enabled**, signing and verification of the JMS messages passed between Horizon 7 components takes place. ■ When the mode is set to **Enhanced**, security is provided by mutually authenticated TLS. JMS connections and access control on JMS topics. For new installations, by default, message security mode is set to **Enhanced**. If you upgrade from a previous version, the setting used in the previous version is retained.
Enhanced Security Status (Read-only)	Read-only field that appears when **Message security mode** is changed from **Enabled** to **Enhanced**. Because the change is made in phases, this field shows the progress through the phases: ■ **Waiting for Message Bus restart** is the first phase. This state is displayed until you manually restart either all Connection Server instances in the pod or the VMware Horizon Message Bus Component service on all Connection Server hosts in the pod. ■ **Pending Enhanced** is the next state. After all Horizon Message Bus Component services have been restarted, the system begins changing the message security mode to **Enhanced** for all desktops and security servers. ■ **Enhanced** is the final state, indicating that all components are now using **Enhanced** message security mode.

Disable or Enable Horizon Connection Server in Horizon Console

You can disable a Connection Server instance to prevent users from logging in to their virtual or published desktops and applications. After you disable an instance, you can enable it again.

When you disable a Connection Server instance, users who are currently logged in to desktops and applications are not affected.

Your Horizon 7 deployment determines how users are affected by disabling an instance.

- If this is a single, standalone Connection Server instance, users cannot log in to their desktops or applications. They cannot connect to Connection Server.

- If this is a replicated Connection Server instance, your network topology determines whether users can be routed to another replicated instance. If users can access another instance, they can log in to their desktops and applications.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 On the **Connection Servers** tab, select the Connection Server instance.

3 Click **Disable**.

You can enable the instance again by clicking **Enable**.

Edit the External URLs for Horizon Connection Server Instances

You can use Horizon Console to edit external URLs for Connection Server instances.

By default, a Connection Server host can be contacted only by tunnel clients that reside within the same network. Tunnel clients that run outside of your network must use a client-resolvable URL to connect to a Connection Server host.

When users connect to remote desktops with the PCoIP display protocol, Horizon Client can make a further connection to the PCoIP Secure Gateway on the Connection Server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach the Connection Server host. You specify this IP address in the PCoIP external URL.

A third URL allows users to make secure connections through the Blast Secure Gateway.

The secure tunnel external URL, PCoIP external URL, and Blast external URL must be the addresses that client systems use to reach this host.

Procedure

1 In Horizon Console, select **Settings > Servers**.

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

3 Type the secure tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable host name and port number.

For example: https://horizon.example.com:443

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 host that you contact will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security.

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this Connection Server instance.

5 Type the Blast Secure Gateway external URL in the **Blast External URL** text box.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

For example: `https://myserver.example.com:8443`

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this host.

6 Verify that all addresses in this dialog allow client systems to reach this host.

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

The external URLs are updated immediately. You do not need to restart the Connection Server for the changes to take effect.

Register Gateways in Horizon Console

Horizon Clients connect through a gateway or Unified Access Gateway appliance that you register in Horizon Console.

You can register or unregister gateways in Horizon Console. To unregister the gateway, select the gateway or Unified Access Gateway appliance and click **Unregister**.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 On the **Gateways** tab, click **Register**.

3 Enter the FQDN of the gateway or Unified Access Gateway appliance.

4 Click **OK**.

Setting Up Smart Card Authentication

4

For added security, you can configure a Connection Server instance or security server so that users and administrators can authenticate by using smart cards.

A smart card is a small plastic card that contains a computer chip. The chip, which is like a miniature computer, includes secure storage for data, including private keys and public key certificates. One type of smart card used by the United States Department of Defense is called a Common Access Card (CAC).

With smart card authentication, a user or administrator inserts a smart card into a smart card reader attached to the client computer and enters a PIN. Smart card authentication provides two-factor authentication by verifying both what the person has (the smart card) and what the person knows (the PIN).

See the *Horizon 7 Installation* document for information about hardware and software requirements for implementing smart card authentication. The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.

To use smart cards, client machines must have smart card middleware and a smart card reader. To install certificates on smart cards, you must set up a computer to act as an enrollment station. For information about whether a particular type of Horizon Client supports smart cards, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

This chapter includes the following topics:

Logging In with a Smart Card

When a user or administrator inserts a smart card into a smart card reader, the user certificates on the smart card are copied to the local certificate store on the client system if the client operating system is

Windows. The certificates in the local certificate store are available to all of the applications running on the client computer, including Horizon Client.

When a user or administrator initiates a connection to a Connection Server instance or security server that is configured for smart card authentication, the Connection Server instance or security server sends a list of trusted certificate authorities (CAs) to the client system. The client system checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user or administrator to enter a smart card PIN. If there are multiple valid user certificates, the client system prompts the user or administrator to select a certificate.

The client system sends the user certificate to the Connection Server instance or security server, which verifies the certificate by checking the certificate trust and validity period. Typically, users and administrators can successfully authenticate if their user certificate is signed and valid. If certificate revocation checking is configured, users or administrators who have revoked user certificates are prevented from authenticating.

In some environments, a user's smart card certificate can map to multiple Active Directory domain user accounts. A user might have multiple accounts with administrator privileges and needs to specify which account to use in the Username hint field during smart card login. To make the Username hint field appear on the Horizon Client login dialog box, the administrator must enable the smart card user name hints feature for the Connection Server instance in Horizon Console. The smart card user can then enter a user name or UPN in the Username hint field during smart card login.

If your environment uses a Unified Access Gateway appliance for secure external access, you must configure the Unified Access Gateway appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Unified Access Gateway version 2.7.2 and later. For information about enabling the smart card user name hints feature in a Unified Access Gateway appliance, see the *Deploying and Configuring Unified Access Gateway* document.

Display protocol switching is not supported with smart card authentication in Horizon Client. To change display protocols after authenticating with a smart card in Horizon Client, a user must log off and log on again.

Configure Smart Card Authentication on Horizon Connection Server

To configure smart card authentication, you must obtain a root certificate and add it to a server truststore file, modify the Connection Server configuration properties, and configure smart card authentication settings. Depending on your particular environment, you might need to perform additional steps.

Procedure

1 Obtain the Certificate Authority Certificates

You must obtain all applicable CA (certificate authority) certificates for all trusted user certificates on the smart cards presented by your users and administrators. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

2. Obtain the CA Certificate from Windows

   If you have a CA-signed user certificate or a smart card that contains one, and Windows trusts the root certificate, you can export the root certificate from Windows. If the issuer of the user certificate is an intermediate certificate authority, you can export that certificate.

3. Add the CA Certificate to a Server Truststore File

   You must add root certificates, intermediate certificates, or both to a server truststore file for all users and administrators that you trust. Connection Server instances and security servers use this information to authenticate smart card users and administrators.

4. Modify Horizon Connection Server Configuration Properties

   To enable smart card authentication, you must modify Connection Server configuration properties on your Connection Server.

5. Configure Smart Card Settings in Horizon Console

   You can use Horizon Console to specify settings to accommodate different smart card authentication scenarios.

Obtain the Certificate Authority Certificates

You must obtain all applicable CA (certificate authority) certificates for all trusted user certificates on the smart cards presented by your users and administrators. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

If you do not have the root or intermediate certificate of the CA that signed the certificates on the smart cards presented by your users and administrators, you can export the certificates from a CA-signed user certificate or a smart card that contains one. See Obtain the CA Certificate from Windows.

Procedure

- Obtain the CA certificates from one of the following sources.

  - A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.

  - The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

Obtain the CA Certificate from Windows

If you have a CA-signed user certificate or a smart card that contains one, and Windows trusts the root certificate, you can export the root certificate from Windows. If the issuer of the user certificate is an intermediate certificate authority, you can export that certificate.

Procedure

1. If the user certificate is on a smart card, insert the smart card into the reader to add the user certificate to your personal store.

   If the user certificate does not appear in your personal store, use the reader software to export the user certificate to a file. This file is used in Step 4 of this procedure.

2. In Internet Explorer, select **Tools > Internet Options**.
3. On the **Content** tab, click **Certificates**.
4. On the **Personal** tab, select the certificate you want to use and click **View**.

   If the user certificate does not appear on the list, click **Import** to manually import it from a file. After the certificate is imported, you can select it from the list.

5. On the **Certification Path** tab, select the certificate at the top of the tree and click **View Certificate**.

   If the user certificate is signed as part of a trust hierarchy, the signing certificate might be signed by another higher-level certificate. Select the parent certificate (the one that actually signed the user certificate) as your root certificate. In some cases, the issuer might be an intermediate CA.

6. On the **Details** tab, click **Copy to File**.

   The **Certificate Export Wizard** appears.

7. Click **Next > Next** and type a name and location for the file that you want to export.
8. Click **Next** to save the file as a root certificate in the specified location.

Add the CA Certificate to a Server Truststore File

You must add root certificates, intermediate certificates, or both to a server truststore file for all users and administrators that you trust. Connection Server instances and security servers use this information to authenticate smart card users and administrators.

Prerequisites

- Obtain the root or intermediate certificates that were used to sign the certificates on the smart cards presented by your users or administrators. See Obtain the Certificate Authority Certificates and Obtain the CA Certificate from Windows.

  Important These certificates can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

- Verify that the `keytool` utility is added to the system path on your Connection Server or security server host. See the *Horizon 7 Installation* document for more information.

Procedure

1 On your Connection Server or security server host, use the `keytool` utility to import the root certificate, intermediate certificate, or both into the server truststore file.

   For example:

   ```
   keytool -import -alias alias -file root_certificate -keystore truststorefile.key
   ```

   In this command, *alias* is a unique case-sensitive name for a new entry in the truststore file, *root_certificate* is the root or intermediate certificate that you obtained or exported, and *truststorefile.key* is the name of the truststore file that you are adding the root certificate to. If the file does not exist, it is created in the current directory.

   Note The `keytool` utility might prompt you to create a password for the truststore file. You will be asked to provide this password if you need to add additional certificates to the truststore file at a later time.

2 Copy the truststore file to the SSL gateway configuration folder on the Connection Server or security server host.

   For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key`

What to do next

Modify Connection Server configuration properties to enable smart card authentication.

Modify Horizon Connection Server Configuration Properties

To enable smart card authentication, you must modify Connection Server configuration properties on your Connection Server.

Prerequisites

Add the CA (certificate authority) certificates for all trusted user certificates to a server truststore file. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

Procedure

1 Create or edit the `locked.properties` file in the TLS/SSL gateway configuration folder on the Connection Server host.

   For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2. Add the `trustKeyfile`, `trustStoretype`, and `useCertAuth` properties to the `locked.properties` file.

    a. Set `trustKeyfile` to the name of your truststore file.

    b. Set `trustStoretype` to **`jks`**.

    c. Set `useCertAuth` to **`true`** to enable certificate authentication.

3. Restart the Connection Server service to make your changes take effect.

Example: locked.properties File

The file shown specifies that the root certificate for all trusted users is located in the file `lonqa.key`, sets the trust store type to `jks`, and enables certificate authentication.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

What to do next

If you configured smart card authentication for a Connection Server instance, configure smart card authentication settings in Horizon Console.

Configure Smart Card Settings in Horizon Console

You can use Horizon Console to specify settings to accommodate different smart card authentication scenarios.

Prerequisites

- Modify Connection Server configuration properties on your Connection Server host.
- Verify that Horizon clients make HTTPS connections directly to your Connection Server or security server host. Smart card authentication is not supported if you off-load TLS to an intermediate device.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance and click **Edit**.

3 To configure smart card authentication for remote desktop and application users, perform these steps.

a On the **Authentication** tab, select a configuration option from the **Smart card authentication for users** drop-down menu in the Horizon Authentication section.

Option	Action
Not allowed	Smart card authentication is disabled on the Connection Server instance.
Optional	Users can use smart card authentication or password authentication to connect to the Connection Server instance. If smart card authentication fails, the user must provide a password.
Required	Users are required to use smart card authentication when connecting to the Connection Server instance. When smart card authentication is required, authentication fails for users who select the **Log in as current user** check box when they connect to the Connection Server instance. These users must reauthenticate with their smart card and PIN when they log in to Connection Server. **Note** Smart card authentication replaces Windows password authentication only. If SecurID is enabled, users are required to authenticate by using both SecurID and smart card authentication.

b Configure the smart card removal policy.

You cannot configure the smart card removal policy when smart card authentication is set to **Not Allowed**.

Option	Action
Disconnect users from Connection Server when they remove their smart cards.	Select the **Disconnect user sessions on smart card removal** check box.
Keep users connected to Connection Server when they remove their smart cards and let them start new desktop or application sessions without reauthenticating.	Deselect the **Disconnect user sessions on smart card removal** check box.

The smart card removal policy does not apply to users who connect to the Connection Server instance with the **Log in as current user** check box selected, even if they log in to their client system with a smart card.

c Configure the smart card user name hints feature.

You cannot configure the smart card user name hints feature when smart card authentication is set to **Not Allowed**.

Option	Action
Enable users to use a single smart card certificate to authenticate to multiple user accounts.	Select the **Allow smart card user name hints** check box.
Disable users from using a single smart card certificate to authenticate to multiple user accounts.	Deselect the **Allow smart card user name hints** check box.

4 To configure smart card authentication for administrators logging in to Horizon Console, select a configuration option from the **Smart card authentication for administrators** drop-down menu in the **Horizon Administrator Authentication** section.

Option	Action
Not allowed	Smart card authentication is disabled on the Connection Server instance.
Optional	Administrators can use smart card authentication or password authentication to log in to Horizon Console. If smart card authentication fails, the administrator must provide a password.
Required	Administrators are required to use smart card authentication when they log in to Horizon Console.

5 Click **OK**.

6 Restart the Connection Server service.

You must restart the Connection Server service for changes to smart card settings to take effect, with one exception. You can change smart card authentication settings between **Optional** and **Required** without having to restart the Connection Server service.

Currently logged in user and administrators are not affected by changes to smart card settings.

What to do next

Prepare Active Directory for smart card authentication, if required. See Prepare Active Directory for Smart Card Authentication.

Verify your smart card authentication configuration. See Verify Your Smart Card Authentication Configuration in Horizon Console.

Configure Smart Card Authentication on Third Party Solutions

Third-party solutions such as load balancers and gateways can perform smart card authentication by passing a SAML assertion that contains the smart card's X.590 certificate and encrypted PIN.

This topic outlines the tasks involved in setting up third-party solutions to provide the relevant X.590 certificate to Connection Server after the certificate has been validated by the partner device. Because this feature uses SAML authentication, one of the tasks is to create a SAML authenticator in Horizon Console.

For information about configuring smart card authentication on Unified Access Gateway, see the Unified Access Gateway documentation.

Procedure

1. Create a SAML authenticator for the third-party gateway or load balancer.

   See Configure a SAML Authenticator in Horizon Console.

2. Extend the expiration period of the Connection Server metadata so that remote sessions are not terminated after only 24 hours.

   See Change the Expiration Period for Service Provider Metadata on Connection Server.

3. If necessary, configure the third-party device to use service provider metadata from Connection Server.

   See the product documentation for the third-party device.

4. Configure smart card settings on the third-party device.

   See the product documentation for the third-party device.

Prepare Active Directory for Smart Card Authentication

You might need to perform certain tasks in Active Directory when you implement smart card authentication.

- Add UPNs for Smart Card Users

  Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in Horizon 7 must have a valid UPN.

- Add the Root Certificate to the Enterprise NTAuth Store

  If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- Add the Root Certificate to Trusted Root Certification Authorities

  If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- Add an Intermediate Certificate to Intermediate Certification Authorities

  If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Add UPNs for Smart Card Users

Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in Horizon 7 must have a valid UPN.

If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user’s UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA. If your root certificate was issued from a server in the smart card user's current domain, you do not need to modify the user's UPN.

Note You might need to set the UPN for built-in Active Directory accounts, even if the certificate is issued from the same domain. Built-in accounts, including Administrator, do not have a UPN set by default.

Prerequisites

- Obtain the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.
- If the ADSI Edit utility is not present on your Active Directory server, download and install the appropriate Windows Support Tools from the Microsoft Web site.

Procedure

1. On your Active Directory server, start the ADSI Edit utility.
2. In the left pane, expand the domain the user is located in and double-click `CN=Users`.
3. In the right pane, right-click the user and then click **Properties**.
4. Double-click the `userPrincipalName` attribute and type the SAN value of the trusted CA certificate.
5. Click **OK** to save the attribute setting.

Add the Root Certificate to the Enterprise NTAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

- On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

  For example: `certutil –dspublish –f` ***`path_to_root_CA_cert`*** `NTAuthCA`

The CA is now trusted to issue certificates of this type.

Add the Root Certificate to Trusted Root Certification Authorities

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
Windows 2012R2	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
Windows 2016	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings \Public Key**.

3 Right-click **Trusted Root Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the root certificate in their trusted root store.

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See Add an Intermediate Certificate to Intermediate Certification Authorities.

Add an Intermediate Certificate to Intermediate Certification Authorities

If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
Windows 2012R2	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
Windows 2016	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open the policy for **Windows Settings\Security Settings\Public Key**.

3 Right-click **Intermediate Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the intermediate certificate in their intermediate certification authority store.

Verify Your Smart Card Authentication Configuration in Horizon Console

After you set up smart card authentication for the first time, or when smart card authentication is not working correctly, you should verify your smart card authentication configuration.

Procedure

- Verify that each client system has smart card middleware, a smart card with a valid certificate, and a smart card reader. For end users, verify that they have Horizon Client.

  See the documentation provided by your smart card vendor for information on configuring smart card software and hardware.

- On each client system, select **Start > Settings > Control Panel > Internet Options > Content > Certificates > Personal** to verify that certificates are available for smart card authentication.

  When a user or administrator inserts a smart card into the smart card reader, Windows copies certificates from the smart card to the user's computer. Applications on the client system, including Horizon Client, can use these certificates.

- In the `locked.properties` file on the Connection Server or security server host, verify that the `useCertAuth` property is set to **`true`** and is spelled correctly.

  The `locked.properties` file is located in *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`. The `useCertAuth` property is commonly misspelled as `userCertAuth`.

- If you configured smart card authentication on a Connection Server instance, check the smart card authentication setting in Horizon Console.

  a Select **Settings > Servers**.

  b On the **Connection Servers** tab, select the Connection Server instance and click **Edit**.

  c If you configured smart card authentication for users, on the **Authentication** tab, verify that **Smart card authentication for users** is set to either **Optional** or **Required**.

  d If you configured smart card authentication for administrators, on the **Authentication** tab, verify that **Smart card authentication for administrators** is set to either **Optional** or **Required**.

  You must restart the Connection Server service for changes to smart card settings to take effect.

- If the domain a smart card user resides in is different from the domain your root certificate was issued from, verify that the user’s UPN is set to the SAN contained in the root certificate of the trusted CA.

  a Find the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.

  b On your Active Directory server, select **Start > Administrative Tools > Active Directory Users and Computers**.

  c Right-click the user in the **Users** folder and select **Properties**.

  The UPN appears in the **User logon name** text boxes on the **Account** tab.

- If smart card users select the PCoIP display protocol or the VMware Blast display protocol to connect to single-session desktops, verify that the Horizon Agent component called Smartcard Redirection is installed on the single-user machines. The smart card feature lets users log in to single-session desktops with smart cards. RDS hosts, which have the Remote Desktop Services role installed, support the smart card feature automatically and you do not need to install the feature.

- Check the log files in *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs on the Connection Server or security server host for messages stating that smart card authentication is enabled.

Using Smart Card Certificate Revocation Checking

You can prevent users who have revoked user certificates from authenticating with smart cards by configuring certificate revocation checking. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

Horizon 7 supports certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

You can configure certificate revocation checking on a Connection Server instance or on a security server. When a Connection Server instance is paired with a security server, you configure certificate revocation checking on the security server. The CA must be accessible from the Connection Server or security server host.

You can configure both CRL and OCSP on the same Connection Server instance or security server. When you configure both types of certificate revocation checking, Horizon 7 attempts to use OCSP first and falls back to CRL if OCSP fails. Horizon 7 does not fall back to OCSP if CRL fails.

- Logging in with CRL Checking

  When you configure CRL checking, Horizon 7 constructs and reads a CRL to determine the revocation status of a user certificate.

- Logging in with OCSP Certificate Revocation Checking

  When you configure OCSP certificate revocation checking, Horizon 7 sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. Horizon 7 uses an OCSP signing certificate to verify that the responses it receives from the OCSP Responder are genuine.

- Configure CRL Checking

  When you configure CRL checking, Horizon 7 reads a CRL to determine the revocation status of a smart card user certificate.

- Configure OCSP Certificate Revocation Checking

  When you configure OCSP certificate revocation checking, Horizon 7 sends a verification request to an OCSP Responder to determine the revocation status of a smart card user certificate.

- Smart Card Certificate Revocation Checking Properties

  You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

Logging in with CRL Checking

When you configure CRL checking, Horizon 7 constructs and reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked and smart card authentication is optional, the **Enter your user name and password** dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate. The same events occur if Horizon 7 cannot read the CRL.

Logging in with OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, Horizon 7 sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. Horizon 7 uses an OCSP signing certificate to verify that the responses it receives from the OCSP Responder are genuine.

If the user certificate is revoked and smart card authentication is optional, the **Enter your user name and password** dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate.

Horizon 7 falls back to CRL checking if it does not receive a response from the OCSP Responder or if the response is invalid.

Configure CRL Checking

When you configure CRL checking, Horizon 7 reads a CRL to determine the revocation status of a smart card user certificate.

Prerequisites

Familiarize yourself with the `locked.properties` file properties for CRL checking. See Smart Card Certificate Revocation Checking Properties.

Procedure

1 Create or edit the `locked.properties` file in the TLS/SSL gateway configuration folder on the Connection Server or security server host.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `enableRevocationChecking` and `crlLocation` properties to the `locked.properties` file.

   a Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.

   b Set `crlLocation` to the location of the CRL. The value can be a URL or a file path.

3 Restart the Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures CRL checking, and specifies a URL for the CRL location.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Configure OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, Horizon 7 sends a verification request to an OCSP Responder to determine the revocation status of a smart card user certificate.

Prerequisites

Familiarize yourself with the `locked.properties` file properties for OCSP certificate revocation checking. See Smart Card Certificate Revocation Checking Properties.

Procedure

1 Create or edit the `locked.properties` file in the TLS/SSL gateway configuration folder on the Connection Server or security server host.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `enableRevocationChecking`, `enableOCSP`, `ocspURL`, and `ocspSigningCert` properties to the `locked.properties` file.

a Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.

b Set `enableOCSP` to **`true`** to enable OCSP certificate revocation checking.

c Set `ocspURL` to the URL of the OCSP Responder.

d Set `ocspSigningCert` to the location of the file that contains the OCSP Responder's signing certificate.

3 Restart the Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures both CRL and OCSP certificate revocation checking, specifies the OCSP Responder location, and identifies the file that contains the OCSP signing certificate.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
```

```
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Smart Card Certificate Revocation Checking Properties

You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

Table 4-1. Properties for Smart Card Certificate Revocation Checking lists the `locked.properties` file properties for certificate revocation checking.

Table 4-1. Properties for Smart Card Certificate Revocation Checking

Property	Description
`enableRevocationChecking`	Set this property to **true** to enable certificate revocation checking. When this property is set to **false**, certificate revocation checking is disabled and all other certificate revocation checking properties are ignored. The default value is **false**.
`crlLocation`	Specifies the location of the CRL, which can be either a URL or a file path. If you do not specify a URL, or if the specified URL is invalid, Horizon 7 uses the list of CRLs on the user certificate if `allowCertCRLs` is set to **true** or is not specified. If Horizon 7 cannot access a CRL, CRL checking fails.
`allowCertCRLs`	When this property is set to **true**, Horizon 7 extracts a list of CRLs from the user certificate. The default value is **true**.
`enableOCSP`	Set this property to **true** to enable OCSP certificate revocation checking. The default value is **false**.
`ocspURL`	Specifies the URL of an OCSP Responder.
`ocspResponderCert`	Specifies the file that contains the OCSP Responder's signing certificate. Horizon 7 uses this certificate to verify that the OCSP Responder's responses are genuine.
`ocspSendNonce`	When this property is set to **true**, a nonce is sent with OCSP requests to prevent repeated responses. The default value is **false**.
`ocspCRLFailover`	When this property is set to **true**, Horizon 7 uses CRL checking if OCSP certificate revocation checking fails. The default value is **true**.

Setting Up Other Types of User Authentication 5

Horizon 7 uses your existing Active Directory infrastructure for user and administrator authentication and management. You can also integrate Horizon 7 with other forms of authentication besides smart cards, such as biometric authentication or two-factor authentication solutions, such as RSA SecurID and RADIUS, to authenticate remote desktop and application users.

This chapter includes the following topics:

Using Two-Factor Authentication

You can configure a Horizon Connection Server instance so that users are required to use RSA SecurID authentication or RADIUS (Remote Authentication Dial-In User Service) authentication.

- RADIUS support offers a wide range of alternative two-factor token-based authentication options.
- Horizon 7 also provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into Horizon 7.

Because two-factor authentication solutions such as RSA SecurID and RADIUS work with authentication managers, installed on separate servers, you must have those servers configured and accessible to the Connection Server host. For example, if you use RSA SecurID, the authentication manager would be RSA Authentication Manager. If you have RADIUS, the authentication manager would be a RADIUS server.

To use two-factor authentication, each user must have a token, such as an RSA SecurID token, that is registered with its authentication manager. A two-factor authentication token is a piece of hardware or software that generates an authentication code at fixed intervals. Often authentication requires knowledge of both a PIN and an authentication code.

If you have multiple Connection Server instances, you can configure two-factor authentication on some instances and a different user authentication method on others. For example, you can configure two-factor authentication only for users who access remote desktops and applications from outside the corporate network, over the Internet.

Horizon 7 is certified through the RSA SecurID Ready program and supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, and load balancing.

- Logging in Using Two-Factor Authentication

  When a user connects to a Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in Horizon Client.
- Enable Two-Factor Authentication in Horizon Console

  You can enable a Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying Connection Server settings in Horizon Console.
- Troubleshooting RSA SecureID Access Denied

  Access is denied when Horizon Client connects with RSA SecurID authentication.
- Troubleshooting RADIUS Access Denial

  Access is denied when Horizon Client connects with RADIUS two-factor authentication.

Logging in Using Two-Factor Authentication

When a user connects to a Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in Horizon Client.

Users enter their RSA SecurID or RADIUS authentication user name and passcode in the a special login dialog box. A two-factor authentication passcode typically consists of a PIN followed by a token code.

- If RSA Authentication Manager requires users to enter a new RSA SecurID PIN after entering their RSA SecurID username and passcode, a PIN dialog box appears. After setting a new PIN, users are prompted to wait for the next token code before logging in. If RSA Authentication Manager is configured to use system-generated PINs, a dialog box appears to confirm the PIN.
- When logging in to Horizon 7, RADIUS authentication works much like RSA SecurID. If the RADIUS server issues an access challenge, Horizon Client displays a dialog box similar to the RSA SecurID prompt for the next token code. Currently support for RADIUS challenges is limited to prompting for text input. Any challenge text sent from the RADIUS server is not displayed. More complex forms of challenge, such as multiple choice and image selection, are currently not supported.

  After a user enters credentials in Horizon Client, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism, to the user's cell phone with a code. The user can enter this text and code into Horizon Client to complete the authentication.
- Because some RADIUS vendors provide the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.

Enable Two-Factor Authentication in Horizon Console

You can enable a Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying Connection Server settings in Horizon Console.

Prerequisites

Install and configure the two-factor authentication software, such as the RSA SecurID software or the RADIUS software, on an authentication manager server.

- For RSA SecurID authentication, export the `sdconf.rec` file for the Connection Server instance from RSA Authentication Manager. See the RSA Authentication Manager documentation.
- For RADIUS authentication, follow the vendor's configuration documentation. Make a note of the RADIUS server's host name or IP address, the port number on which it is listening for RADIUS authentication (usually 1812), the authentication type (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2) and the shared secret. You enter these values in Horizon Console. You can enter values for a primary and a secondary RADIUS authenticator.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance and click **Edit**.
3. On the **Authentication** tab, from the **2-factor authentication** drop-down menu in the **Advanced Authentication** section, select **RSA SecureID** or **RADIUS**.
4. To force RSA SecurID or RADIUS user names to match user names in Active Directory, select **Enforce SecurID and Windows user name matching** or **Enforce 2-factor and Windows user name matching**.

   If you select this option, users must use the same RSA SecurID or RADIUS user name for Active Directory authentication. If you do not select this option, the names can be different.
5. For RSA SecurID, click **Upload File**, type the location of the `sdconf.rec` file, or click **Browse** to search for the file.

6 For RADIUS authentication, complete the rest of the fields:

   a Select **Use the same username and password for RADIUS and Windows authentication** if the initial RADIUS authentication uses Windows authentication that triggers an out-of-band transmission of a token code, and this token code is used as part of a RADIUS challenge.

     If you select this check box, users will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication uses the Windows username and password. Users do not have to reenter the Windows username and password after RADIUS authentication.

   b From the **Authenticator** drop-down menu, select **Create New Authenticator** and complete the page.

     - Set **Accounting port** to **0** unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a nonzero number, the messages are sent and ignored and retried a number of times, resulting in a delay in authentication.

       Accounting data can be used in order to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring.

     - If you specify a realm prefix string, the string is placed at the beginning of the username when it is sent to the RADIUS server. For example, if the username entered in Horizon Client is `jdoe` and the realm prefix `DOMAIN-A\` is specified, the username `DOMAIN-A\jdoe` is sent to the RADIUS server. Similarly if you use the realm suffix, or postfix, string `@mycorp.com`, the username `jdoe@mycorp.com` is sent to the RADIUS server.

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

  You do not need to restart the Connection Server service. The necessary configuration files are distributed automatically and the configuration settings take effect immediately.

When users open Horizon Client and authenticate to Connection Server, they are prompted for two-factor authentication. For RADIUS authentication, the login dialog box displays text prompts that contain the token label you specified.

Changes to RADIUS authentication settings affect remote desktop and application sessions that are started after the configuration is changed. Current sessions are not affected by changes to RADIUS authentication settings.

What to do next

If you have a replicated group of Connection Server instances and you want to also set up RADIUS authentication on them, you can re-use an existing RADIUS authenticator configuration.

Troubleshooting RSA SecureID Access Denied

Access is denied when Horizon Client connects with RSA SecurID authentication.

Problem

A Horizon Client connection with RSA SecurID displays `Access Denied` and the RSA Authentication Manager Log Monitor displays the error `Node Verification Failed`.

Cause

The RSA Agent host node secret needs to be reset.

Solution

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance and click **Edit**.
3. On the **Authentication** tab, from the **2-factor authentication** drop-down menu in the **Advanced Authentication** section, select **RSA SecureID**.
4. Select **Clear node secret** and click **OK**.
5. On the computer that is running RSA Authentication Manager, select **Start > Programs > RSA Security > RSA Authentication Manager Host Mode**.
6. Select **Agent Host > Edit Agent Host**.
7. Select Connection Server from the list and deselect the **Node Secret Created** check box.

   Node Secret Created is selected by default each time you edit it.
8. Click **OK**.

Troubleshooting RADIUS Access Denial

Access is denied when Horizon Client connects with RADIUS two-factor authentication.

Problem

A Horizon Client connection using RADIUS two-factor authentication displays `Access Denied`.

Cause

RADIUS does not receive a reply from the RADIUS server, causing Horizon 7 to time out.

The following common configuration mistakes most often lead to this situation:

- The RADIUS server has not been configured to accept the Connection Server instance as a RADIUS client. Each Connection Server instance using RADIUS must be set up as a client on the RADIUS server. See the documentation for your RADIUS two-factor authentication product.
- The shared secret values on the Connection Server instance and the RADIUS server do not match.

Using SAML Authentication

The Security Assertion Markup Language (SAML) is an XML-based standard that is used to describe and exchange authentication and authorization information between different security domains. SAML passes information about users between identity providers and service providers in XML documents called SAML assertions.

You can use SAML authentication to integrate Horizon 7 with VMware Workspace ONE, VMware Identity Manager, or a qualified third-party load balancer or gateway. When configuring SAML for a third-party device, refer to the vendor documentation for information on configuring Horizon 7 to work with it. When SSO is enabled, users who log in to VMware Identity Manager or a third-party device can launch remote desktops and applications without having to go through a second login procedure. You can also use SAML authentication to implement smart card authentication on VMware Access Point, or on third-party devices.

To delegate responsibility for authentication to Workspace ONE, VMware Identity Manager, or a third-party device, you must create a SAML authenticator in Horizon 7. A SAML authenticator contains the trust and metadata exchange between Horizon 7 and Workspace ONE, VMware Identity Manager, or the third-party device. You associate a SAML authenticator with a Connection Server instance.

Using SAML Authentication for VMware Identity Manager Integration

Integration between Horizon 7 and VMware Identity Manager (formerly called Workspace ONE) uses the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. When SSO is enabled, users who log in to VMware Identity Manager or Workspace ONE with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure.

When VMware Identity Manager and Horizon 7 are integrated, VMware Identity Manager generates a unique SAML artifact whenever a user logs in to VMware Identity Manager and clicks a desktop or application icon. VMware Identity Manager uses this SAML artifact to create a Universal Resource Identifier (URI). The URI contains information about the Connection Server instance where the desktop or application pool resides, which desktop or application to launch, and the SAML artifact.

VMware Identity Manager sends the SAML artifact to the Horizon client, which in turn sends the artifact to the Connection Server instance. The Connection Server instance uses the SAML artifact to retrieve the SAML assertion from VMware Identity Manager.

After a Connection Server instance receives a SAML assertion, it validates the assertion, decrypts the user's password, and uses the decrypted password to launch the desktop or application.

Setting up VMware Identity Manager and Horizon 7 integration involves configuring VMware Identity Manager with Horizon 7 information and configuring Horizon 7 to delegate responsibility for authentication to VMware Identity Manager.

To delegate responsibility for authentication to VMware Identity Manager, you must create a SAML authenticator in Horizon 7. A SAML authenticator contains the trust and metadata exchange between Horizon 7 and VMware Identity Manager. You associate a SAML authenticator with a Connection Server instance.

Note 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 Console. 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.

Configure a SAML Authenticator in Horizon Console

To launch remote desktops and applications from VMware Identity Manager or to connect to remote desktops and applications through a third-party load balancer or gateway, you must create a SAML authenticator in Horizon Console. A SAML authenticator contains the trust and metadata exchange between Horizon 7 and the device to which clients connect.

You associate a SAML authenticator with a Connection Server instance. If your deployment includes more than one Connection Server instance, you must associate the SAML authenticator with each instance.

You can allow one static authenticator and multiple dynamic authenticators to go live at a time. You can configure vIDM (Dynamic) and Unified Access Gateway (Static) authenticators and retain them in active state. You can make connections through either of these authenticators.

You can configure more than one SAML authenticator to a Connection Server and all the authenticators can be active simultaneously. However, the entity-ID of each of these SAML authenticators configured on the Connection Server must be different.

The status of the SAML authenticator in dashboard is always green as it is predefined metadata that is static in nature. The red and green toggling is only applicable for dynamic authenticators.

For information about configuring a SAML authenticator for VMware Unified Access Gateway appliances, see the Unified Access Gateway documentation.

Prerequisites

- Verify that Workspace ONE, VMware Identity Manager, or a third-party gateway or load balancer is installed and configured. See the installation documentation for that product.
- Verify that the root certificate for the signing CA for the SAML server certificate is installed on the Connection Server host. VMware does not recommend that you configure SAML authenticators to use self-signed certificates. For information about certificate authentication, see the *Horizon 7 Installation* document.
- Make a note of the FQDN or IP address of the Workspace ONE server, VMware Identity Manager server, or external-facing load balancer.

- If you are using Workspace ONE or VMware Identity Manager, make a note of the URL of the connector Web interface.
- If you are creating an authenticator for a Unified Access Gateway appliance or a third-party appliance that requires you to generate SAML metadata and create a static authenticator, perform the procedure on the device to generate the SAML metadata, and then copy the metadata.

Procedure

1 In Horizon Console, navigate to **Settings > Servers**.

2 On the **Connection Servers** tab, select a server instance to associate with the SAML authenticator and click **Edit**.

3 On the **Authentication** tab, select a setting from the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down menu to enable or disable the SAML authenticator.

Option	Description
Disabled	SAML authentication is disabled. You can launch remote desktops and applications only from Horizon Client.
Allowed	SAML authentication is enabled. You can launch remote desktops and applications from both Horizon Client and VMware Identity Manager or the third-party device.
Required	SAML authentication is enabled. You can launch remote desktops and applications only from VMware Identity Manager or the third-party device. You cannot launch desktops or applications from Horizon Client manually.

You can configure each Connection Server instance in your deployment to have different SAML authentication settings, depending on your requirements.

4 Click **Manage SAML Authenticators** and click **Add**.

5 Configure the SAML authenticator in the Add SAML 2.0 Authenticator dialog box.

Option	Description
Type	For a Unified Access Gateway appliance or a third-party device, select **Static**. For VMware Identity Manager select **Dynamic**. For dynamic authenticators, you can specify a metadata URL and an administration URL. For static authenticators, you must first generate the metadata on the Unified Access Gateway appliance or a third-party device, copy the metadata, and then paste it into the **SAML metadata** text box.
Label	Unique name that identifies the SAML authenticator.
Description	Brief description of the SAML authenticator. This value is optional.
Metadata URL	(For dynamic authenticators) URL for retrieving all of the information required to exchange SAML information between the SAML identity provider and the Connection Server instance. In the URL `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml`, click **<YOUR HORIZON SERVER NAME>** and replace it with the FQDN or IP address of the VMware Identity Manager server or external-facing load balancer (third-party device).

Option	Description
Administration URL	(For dynamic authenticators) URL for accessing the administration console of the SAML identity provider. For VMware Identity Manager, this URL should point to the VMware Identity Manager Connector Web interface. This value is optional.
SAML metadata	(For static authenticators) Metadata text that you generated and copied from the Unified Access Gateway appliance or a third-party device.
Enabled for Connection Server	Select this check box to enable the authenticator. You can enable multiple authenticators. Only enabled authenticators are displayed in the list.

6 Click **OK** to save the SAML authenticator configuration.

If you provided valid information, you must either accept the self-signed certificate (not recommended) or use a trusted certificate for Horizon 7 and VMware Identity Manager or the third-party device.

The Manage SAML Authenticators dialog box displays the newly created authenticator.

What to do next

Extend the expiration period of the Connection Server metadata so that remote sessions are not terminated after only 24 hours. See Change the Expiration Period for Service Provider Metadata on Connection Server.

Configure Proxy Support for VMware Identity Manager

Horizon 7 provides proxy support for the VMware Identity Manager (vIDM) server. The proxy details such as hostname and port number can be configured in the ADAM database and the HTTP requests are routed through the proxy.

This feature supports hybrid deployment where the on-premise Horizon 7 deployment can communicate with a vIDM server that is hosted in the cloud.

Prerequisites

Procedure

1 Start the ADSI Edit utility on your Connection Server host.

2 Expand the ADAM ADSI tree under the object path: `cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`.

3 Select **Action > Properties**, and add the values for the entries `pae-SAMLProxyName` and `pae-SAMLProxyPort`.

Change the Expiration Period for Service Provider Metadata on Connection Server

If you do not change the expiration period, Connection Server will stop accepting SAML assertions from the SAML authenticator, such as a Unified Access Gateway appliance or a third-party identity provider, after 24 hours, and the metadata exchange must be repeated.

Use this procedure to specify the number of days that can elapse before Connection Server stops accepting SAML assertions from the identity provider. This number is used when the current expiration period ends. For example, if the current expiration period is 1 day and you specify 90 days, after 1 day elapses, Connection Server generates metadata with an expiration period of 90 days.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

1 Start the ADSI Edit utility on your Connection Server host.

2 In the console tree, select **Connect to**.

3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name `DC=vdi, DC=vmware, DC=int`.

4 In the Computer pane, select or type `localhost:389` or the fully qualified domain name (FQDN) of the Connection Server host followed by port 389.

   For example: `localhost:389` or `mycomputer.example.com:389`

5 Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.

6 In the Properties dialog box, edit the **pae-NameValuePair** attribute to add the following values

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

   In this example, *number-of-days* is the number of days that can elapse before a remote Connection Server stops accepting SAML assertions. After this period of time, the process of exchanging SAML metadata must be repeated.

Generate SAML Metadata So That Connection Server Can Be Used as a Service Provider

After you create and enable a SAML authenticator for the identity provider you want to use, you might need to generate Connection Server metadata. You use this metadata to create a service provider on the Unified Access Gateway appliance or a third-party load balancer that is the identity provider.

Prerequisites

Verify that you have created a SAML authenticator for the identity provider: Unified Access Gateway or a third-party load balancer or gateway.

Procedure

1 Open a new browser tab and enter the URL for getting the Connection Server SAML metadata.

```
https://connection-server.example.com/SAML/metadata/sp.xml
```

In this example, *connection-server.example.com* is the fully qualified domain name of the Connection Server host.

This page displays the SAML metadata from Connection Server.

2 Use a **Save As** command to save the Web page to an XML file.

For example, you could save the page to a file named `connection-server-metadata.xml`. The contents of this file begin with the following text:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

What to do next

Use the appropriate procedure on the identity provider to copy in the Connection Server SAML metadata. Refer to the documentation for Unified Access Gateway or a third-party load balancer or gateway.

Response Time Considerations for Multiple Dynamic SAML Authenticators

If you configure SAML 2.0 Authentication as optional or required on a Connection Server instance and you associate multiple dynamic SAML authenticators with the Connection Server instance, if any of the dynamic SAML authenticators become unreachable, the response time to launch remote desktops from the other dynamic SAML authenticators increases.

You can decrease the response time for remote desktop launch on the other dynamic SAML authenticators by using Horizon Console to disable the unreachable dynamic SAML authenticators. For information about disabling a SAML authenticator, see Configure a SAML Authenticator in Horizon Console.

Configure Workspace ONE Access Policies in Horizon Console

Workspace ONE, or VMware Identity Manager (vIDM) administrators can configure access policies to restrict access to entitled desktops and applications in Horizon 7. To enforce policies created in vIDM you put Horizon client into Workspace ONE mode so that Horizon client can push the user into Workspace ONE client to launch entitlements. When you log in to Horizon Client, the access policy directs you to log in through Workspace ONE to access your published desktops and applications.

Prerequisites

- Configure the access policies for applications in Workspace ONE. For more information about setting access policies, see the *VMware Identity Manager Administration Guide*.
- Entitle users to published desktops and applications in Horizon Console.

Procedure

1 In Horizon Console, navigate to **Settings > Servers**.

2 On the **Connection Servers** tab, select a server instance that is associated with a SAML authenticator and click **Edit**.

3 On the **Authentication** tab, set the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** option to **Required**.

   The Required option enables SAML authentication. The end user can only connect to the Horizon server with a SAML token provided by vIDM or a third-party identity provider. You cannot start desktops or applications from Horizon Client manually.

4 Select **Enable Workspace ONE mode**.

5 In the **Workspace ONE server hostname** text box, enter the Workspace ONE Hostname FQDN value.

6 (Optional) Select **Block connections from clients that don't support Workspace ONE mode** to restrict Horizon Clients that support Workspace ONE mode from accessing applications.

   Horizon Clients earlier than 4.5 do not support the Workspace ONE mode feature. If you select this option, Horizon Clients earlier than 4.5 cannot access applications in Workspace ONE. The Workspace ONE mode feature is not enabled for versions later than Horizon 7 version 7.2 if the Workspace ONE version is earlier than version 2.9.1.

Configure Biometric Authentication

You can configure biometric authentication by editing the `pae-ClientConfig` attribute in the LDAP database.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows server.

Procedure

1 Start the ADSI Edit utility on the Connection Server host.

2 In the Connection Settings dialog box, select or connect to **DC=vdi,DC=vmware,DC=int**.

3 In the Computer pane, select or type `localhost:389` or the fully qualified domain name (FQDN) of the Connection Server host followed by port 389.

   For example: `localhost:389` or `mycomputer.mydomain.com:389`

4 On the object **CN=Common, OU=Global, OU=Properties**, edit the **pae-ClientConfig** attribute and add the value **BioMetricsTimeout=<integer>**.

   The following `BioMetricsTimeout` values are valid:

BioMetricsTimeout Value	Description
0	Biometric authentication is not supported. This is the default.
-1	Biometric authentication is supported without any time limit.
Any positive integer	Biometric authentication is supported and can be used for the specified number of minutes.

The new setting takes effect immediately. You do not need to restart the Connection Server service or the client device.

Authenticating Users and Groups

6

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 Horizon Client without requiring AD credentials.

This chapter includes the following topics:

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.

Configuring Role-Based Delegated Administration in Horizon Console

7

One key management task in an Horizon 7 environment is to determine who can use Horizon Console and what tasks those users are authorized to perform. With role-based delegated administration, you can selectively assign administrative rights by assigning administrator roles to specific Active Directory users and groups.

This chapter includes the following topics:

Understanding Roles and Privileges

The ability to perform tasks in Horizon Console is governed by an access control system that consists of administrator roles and privileges. This system is similar to the vCenter Server access control system.

An administrator role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool. Privileges also control what an administrator can see in Horizon Console. For example, if an administrator does not have privileges to view or modify global policies, the **Global Policies** setting is not visible in the navigation panel when the administrator logs in to Horizon Console.

Administrator privileges are either global or object-specific. Global privileges control system-wide operations, such as viewing and changing global settings. Object-specific privileges control operations on specific types of objects.

Administrator roles typically combine all of the individual privileges required to perform a higher-level administration task. Horizon Console includes predefined roles that contain the privileges required to perform common administration tasks. You can assign these predefined roles to your administrator users and groups, or you can create your own roles by combining selected privileges. You cannot modify the predefined roles.

To create administrators, you select users and groups from your Active Directory users and groups and assign administrator roles. If the role contains object-specific privileges, you might need to apply the role to an access group. Administrators obtain privileges through their role assignments. You cannot assign privileges directly to administrators. An administrator that has multiple role assignments acquires the sum of all the privileges contained in those roles.

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.

- Different Administrators for Different Access Groups

  You can create a different administrator to manage each access group in your configuration.

- Different Administrators for the Same Access Group

  You can create different administrators to manage the same access group.

Different Administrators for Different Access Groups

You can create a different administrator to manage each access group in your configuration.

For example, if your corporate desktop pools are in one access group and your desktop pools for software developers are in another access group, you can create different administrators to manage the resources in each access group.

Table 7-1. Different Administrators for Different Access Groups shows an example of this type of configuration.

Table 7-1. Different Administrators for Different Access Groups

Administrator	Role	Access Group
view-domain.com\Admin1	Inventory Administrators	`/CorporateDesktops`
view-domain.com\Admin2	Inventory Administrators	`/DeveloperDesktops`

In this example, the administrator called Admin1 has the Inventory Administrators role on the access group called `CorporateDesktops` and the administrator called Admin2 has the Inventory Administrators role on the access group called `DeveloperDesktops.`

Different Administrators for the Same Access Group

You can create different administrators to manage the same access group.

For example, if your corporate desktop pools are in one access group, you can create one administrator that can view and modify those pools and another administrator that can only view them.

Table 7-2. Different Administrators for the Same Access Group shows an example of this type of configuration.

Table 7-2. Different Administrators for the Same Access Group

Administrator	Role	Access Group
view-domain.com\Admin1	Inventory Administrators	`/CorporateDesktops`
view-domain.com\Admin2	Inventory Administrators (Read only)	`/CorporateDesktops`

In this example, the administrator called Admin1 has the Inventory Administrators role on the access group called `CorporateDesktops` and the administrator called Admin2 has the Inventory Administrators (Read only) role on the same access group.

Understanding Permissions

Horizon Console presents the combination of a role, an administrator user or group, and an access group as a permission. The role defines the actions that can be performed, the user or group indicates who can perform the action, and the access group contains the objects that are the target of the action.

Permissions appear differently in Horizon Console depending on whether you select an administrator user or group, an access group, or a role.

The following table shows how permissions appear in Horizon Console when you select an administrator user or group. The administrator user is called Admin 1 and it has two permissions.

Table 7-3. Permissions on the Administrators and Groups Tab for Admin 1

Role	Access Group
Inventory Administrators	`MarketingDesktops`
Administrators (Read only)	`/`

The first permission shows that Admin 1 has the Inventory Administrators role on the access group called `MarketingDesktops`. The second permission shows that Admin 1 has the Administrators (Read only) role on the root access group.

The following table shows how the same permissions appear in Horizon Console when you select the `MarketingDesktops` access group.

Table 7-4. Permissions on the Folders Tab for MarketingDesktops

Admin	Role	Inherited
horizon-domain.com\Admin1	Inventory Administrators	
horizon-domain.com\Admin1	Administrators (Read only)	Yes

The first permission is the same as the first permission shown in Table 7-3. Permissions on the Administrators and Groups Tab for Admin 1. The second permission is inherited from the second permission shown in Table 7-3. Permissions on the Administrators and Groups Tab for Admin 1. Because access groups inherit permissions from the root access group, Admin1 has the Administrators (Read only) role on the `MarketingDesktops` access group. When a permission is inherited, Yes appears in the Inherited column.

The following table shows how the first permission in Table 7-3. Permissions on the Administrators and Groups Tab for Admin 1 appears in Horizon Console when you select the Inventory Administrators role.

Table 7-5. Permissions on the Role Permissions Tab for Inventory Administrators

Administrator	Access Group
horizon-domain.com\Admin1	`/MarketingDesktops`

Manage Administrators

Users who have the Administrators role can use Horizon Console to add and remove administrator users and groups.

The Administrators role is the most powerful role in Horizon Console. Initially, members of the Administrators account are given the Administrators role. You specify the Administrators account when you install Connection Server. The Administrators account can be the local Administrators group (BUILTIN\Administrators) on the Connection Server computer or a domain user or group account.

Note By default, the Domain Admins group is a member of the local Administrators group. If you specified the Administrators account as the local Administrators group, and you do not want domain administrators to have full access to inventory objects and Horizon 7 configuration settings, you must remove the Domain Admins group from the local Administrators group.

- Create an Administrator in Horizon Console

  To create an administrator, you select a user or group from your Active Directory users and groups in Horizon Console and assign an administrator role.

- Remove an Administrator in Horizon Console

  You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root access group.

Create an Administrator in Horizon Console

To create an administrator, you select a user or group from your Active Directory users and groups in Horizon Console and assign an administrator role.

Prerequisites

- Become familiar with the predefined administrator roles. See Predefined Roles and Privileges.
- Become familiar with the best practices for creating administrator users and groups. See Best Practices for Administrator Users and Groups.
- To assign a custom role to the administrator, create the custom role. See Add a Custom Role in Horizon Console.
- To create an administrator that can manage specific desktop pools, create an access group and move the desktop pools to that access group. See Manage and Review Access Groups.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 On the **Administrators and Groups** tab, click **Add User or Group**.

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

4 Select the Active Directory user or group that you want to be an administrator user or group, click **OK** and click **Next**.

You can press the Ctrl and Shift keys to select multiple users and groups.

5 Select a role to assign to the administrator user or group.

The **Applied to an access group** column indicates whether a role applies to access groups. Only roles that contain object-specific privileges apply to access groups. Roles that contain only global privileges do not apply to access groups.

Option	Action
The role you selected applies to access groups	Select one or more access groups and click **Next**.
You want the role to apply to all access groups	Select the root access group and click **Next**.

6 Click **Finish** to create the administrator user or group.

The new administrator user or group appears in the left pane and the role and access group that you selected appear in the right pane on the **Administrators and Groups** tab.

Remove an Administrator in Horizon Console

You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root access group.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 On the **Administrators and Groups** tab, select the administrator user or group, click **Remove User or Group**, and click **OK**.

The administrator user or group no longer appears on the **Administrators and Groups** tab.

Manage and Review Permissions

You can use Horizon Console to add, delete, and review permissions for specific administrator users and groups, roles, and access groups.

- Add a Permission in Horizon Console

  You can add a permission that includes a specific administrator user or group, a specific role, or a specific access group.

- Delete a Permission in Horizon Console

  You can delete a permission that includes a specific administrator user or group, a specific role, or a specific access group.

- Review Permissions in Horizon Console

  You can review the permissions that include a specific administrator or group, a specific role, or a specific access group.

Add a Permission in Horizon Console

You can add a permission that includes a specific administrator user or group, a specific role, or a specific access group.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 Create the permission.

Option	Action
Create a permission that includes a specific administrator user or group.	a On the **Administrators and Groups** tab, select the administrator or group and click **Add Permission**. b Select a role. c If the role does not apply to access groups, click **Finish**. d If the role applies to access groups, click **Next**, select one or more access groups, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group.
Create a permission that includes a specific role.	a On the **Role Permissions** tab, select the role, click **Permissions**, and click **Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d If the role does not apply to access groups, click **Finish**. e If the role applies to access groups, click **Next**, select one or more access groups, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group.
Create a permission that includes a specific access group.	a On the **Access Groups** tab, select the access group and click **Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d Click **Next**, select a role, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group.

Delete a Permission in Horizon Console

You can delete a permission that includes a specific administrator user or group, a specific role, or a specific access group.

If you remove the last permission for an administrator user or group, that administrator user or group is also removed. Because at least one administrator must have the Administrators role on the root access group, you cannot remove a permission that would cause that administrator to be removed. You cannot delete an inherited permission.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 Select the permission to delete.

Option	Action
Delete a permission that applies to a specific administrator or group.	Select the administrator or group on the **Administrators and Groups** tab.
Delete a permission that applies to a specific role.	Select the role on the **Roles** tab.
Delete a permission that applies to a specific access group.	Select the folder on the **Access Groups** tab.

3 Select the permission and click **Remove Permission**.

Review Permissions in Horizon Console

You can review the permissions that include a specific administrator or group, a specific role, or a specific access group.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 Review the permissions.

Option	Action
Review the permissions that include a specific administrator or group.	Select the administrator or group on the **Administrators and Groups** tab.
Review the permissions that include a specific role.	Select the role on the **Role Permissions** tab and click **Permissions**.
Review the permissions that include a specific access group.	Select the folder on the **Access Groups** tab.

Manage and Review Access Groups

You can use Horizon Console to add and delete access groups and to review the desktop pools and machines in a particular 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.

- 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.

- Remove an Access Group in Horizon Console

  You can remove an access group if it does not contain any object. You cannot remove the root access group.

- Review the Objects in an Access Group

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

- 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.

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.

Remove an Access Group in Horizon Console

You can remove an access group if it does not contain any object. You cannot remove the root access group.

Prerequisites

If the access group contains objects, move the objects to another access group or to the root access group. See Move a Desktop Pool or Farm to a Different Access Group in Horizon Console.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 On the **Access Groups** tab, select the access group and click **Remove Access Group**.

3 Click **OK** to remove the access group.

Review the Objects in an Access Group

You can view desktop pools, application pools, farms, or persistent disks 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**.
Persistent Disks	Select **Inventory > Persistent Disks**.

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.

Manage Custom Roles

You can use Horizon Console to add, modify, and delete custom roles.

- Add a Custom Role in Horizon Console

  If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in Horizon Console.

- Modify the Privileges in a Custom Role in Horizon Console

  You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

- Remove a Custom Role in Horizon Console

  You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

Add a Custom Role in Horizon Console

If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in Horizon Console.

Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See Predefined Roles and Privileges.

Note When you create a custom administrator role, no global permissions are available for the custom administrator user. Only predefined administrator roles have global permissions, which enable the management of global entitlements in a Cloud Pod Architecture environment.

Procedure

1 In Horizon Console, navigate to **Settings > Administrators**.

2 On the **Role Privileges** tab, click **Add Role**.

3 Enter a name and description for the new role, select one or more privileges, and click **OK**.

The new role appears in the left pane.

Modify the Privileges in a Custom Role in Horizon Console

You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See Predefined Roles and Privileges.

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Role Privileges** tab, select the role.
3. View the privileges in the role and click **Edit**.
4. Select or deselect privileges.
5. Click **OK** to save your changes.

Remove a Custom Role in Horizon Console

You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

Prerequisites

If the role is included in a permission, delete the permission. See Delete a Permission in Horizon Console.

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Role Privileges** tab, select the role and click **Remove Role**.

   The **Remove Role** button is not available for predefined roles or for custom roles that are included in a permission.
3. Click **OK** to remove the role.

Predefined Roles and Privileges

Horizon Console includes predefined roles that you can assign to your administrator users and groups. You can also create your own administrator roles by combining selected privileges.

- Predefined Administrator Roles

  The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.
- Global Privileges

  Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to access groups.

- Object Specific Privileges

  Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to access groups.

- Internal Privileges

  Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

Predefined Administrator Roles

The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.

Note Assigning users a combination of predefined or custom roles can give users access to operations that are not possible within the individual predefined or custom roles.

The following table describes the predefined roles and indicates whether a role can be applied to an access group.

Table 7-6. Predefined Roles in Horizon Console

Role	User Capabilities	Applies to an Access Group
Administrators	Perform all administrator operations, including creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role can configure and manage a pod federation and manage remote pod sessions. Administrators that have the Administrators role on the root access group are super users because they have full access to all of the inventory objects in the system. Because the Administrators role contains all privileges, you should assign it to a limited set of users. Initially, members of the local Administrators group on your Connection Server host are given this role on the root access group. **Important** An administrator must have the Administrators role on the root access group to perform the following tasks: ■ Add and delete access groups. ■ Manage ThinApp applications and configuration settings in Horizon Console. ■ Use the `vdmadmin` , `vdmimport`, and `lmvutil` commands.	Yes
Administrators (Read only)	■ View, but not modify, global settings and inventory objects. ■ View, but not modify, ThinApp applications and settings. ■ Run all PowerShell commands and command line utilities, including `vdmexport` but excluding `vdmadmin`, `vdmimport`, and `lmvutil`. In a Cloud Pod Architecture environment, administrators that have this role can view inventory objects and settings in the Global Data Layer. When administrators have this role on an access group, they can only view the inventory objects in that access group.	Yes

Role	User Capabilities	Applies to an Access Group
Agent Registration Administrators	Register unmanaged machines such as physical systems, standalone virtual machines, and RDS hosts.	No
Global Configuration and Policy Administrators	View and modify global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Global Configuration and Policy Administrators (Read only)	View, but not modify, global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Help Desk Administrators	Perform desktop and application actions such as shutdown, reset, restart, and perform remote assistance actions such as end processes for a user's desktop or application. An administrator must have permissions on the root access group to access Horizon Help Desk Tool. ■ Read-only access to Horizon Help Desk Tool. ■ Manage global sessions. ■ Can log in to Horizon Console. ■ Perform all machine and session-related commands. ■ Manage remote processes and applications. ■ Remote assistance to the virtual desktop or published desktop.	No
Help Desk Administrators (Read Only)	View user and session information, and drill down on session details. An administrator must have permissions on the root access group to access Horizon Help Desk Tool. ■ Read-only access to Horizon Help Desk Tool. ■ Can log in to Horizon Console.	No
Inventory Administrators	■ Perform all machine, session, and pool-related operations. ■ Manage persistent disks. ■ Resync, Refresh, and Rebalance linked-clone pools and change the default pool image. ■ Manage automated farms. When administrators have this role on an access group, they can only perform these operations on the inventory objects in that access group. Administrators with this role cannot create a manual farm or an unmanaged manual pool or add or remove RDS hosts to the farm or unmanaged manual pool.	Yes
Inventory Administrators (Read only)	View, but not modify, inventory objects. When administrators have this role on an access group, they can only view the inventory objects in that access group.	Yes

Role	User Capabilities	Applies to an Access Group
Local Administrators	Perform all local administrator operations, except for creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role cannot perform operations on the Global Data Layer or manage sessions on remote pods. **Note** An administrator with the Local Administrators role cannot access Horizon Help Desk Tool. Administrators in a non-CPA environment do not have the Manage Global Sessions privilege, which is required to perform tasks in Horizon Help Desk Tool.	Yes
Local Administrators (Read Only)	Same as the Administrators (Read Only) role, except for viewing inventory objects and settings in the Global Data Layer. Administrators that have this role have read-only rights only on the local pod. **Note** An administrator with the Local Administrators (Read Only) role cannot access Horizon Help Desk Tool. Administrators in a non-CPA environment do not have the Manage Global Sessions privilege, which is required to perform tasks in Horizon Help Desk Tool.	Yes

Global Privileges

Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to access groups.

The following table describes the global privileges and lists the predefined roles that contain each privilege.

Table 7-7. Global Privileges

Privilege	User Capabilities	Predefined Roles
Console Interaction	Log in to and use Horizon Console.	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Global Configuration and Policy Administrators Global Configuration and Policy Administrators (Read only) Helpdesk Administrators Helpdesk Administrators (Read Only) Local Administrators Local Administrators (Read Only)
Direct Interaction	Run all PowerShell commands and command line utilities, except for `vdmadmin` and `vdmimport`. Administrators must have the Administrators role on the root access group to use the `vdmadmin`, `vdmimport`, and `lmvutil` commands.	Administrators Administrators (Read only)

Privilege	User Capabilities	Predefined Roles
Manage Global Configuration and Policies	View and modify global policies and configuration settings except for administrator roles and permissions.	Administrators Global Configuration and Policy Administrators
Manage Global Sessions	Manage global sessions in a Cloud Pod Architecture environment.	Administrators
Manage Roles and Permissions	Create, modify, and delete administrator roles and permissions.	Administrators
Register Agent	Install Horizon Agent on unmanaged machines, such as physical systems, standalone virtual machines, and RDS hosts. During Horizon Agent installation, you must provide your administrator login credentials to register the unmanaged machine with the Connection Server instance.	Administrators Agent Registration Administrators

Object Specific Privileges

Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to access groups.

The following table describes the object-specific privileges. The predefined roles Administrators and Inventory Administrators contain all of these privileges.

Table 7-8. Object-Specific Privileges

Privilege	User Capabilities	Object
Enable Farms and Desktop Pools	Enable and disable desktop pools.	Desktop pool, farm
Entitle Desktop and Application Pools	Add and remove user entitlements.	Desktop pool, application pool
Manage Composer Desktop Pool Image	Resync, Refresh, and Rebalance linked-clone pools and change the default pool image.	Desktop pool
Manage Machine	Perform all machine and session-related operations.	Machine
Manage Persistent Disks	Perform all Horizon Composer persistent disk operations, including attaching, detaching, and importing persistent disks.	Persistent disk
Manage Farms and Desktop and Application Pools	Add, modify, and delete farms. Add, modify, delete, and entitle desktop and application pools. Add and remove machines.	Desktop pool, application pool, farm
Manage Sessions	Disconnect and log off sessions and send messages to users.	Session
Manage Reboot Operation	Reset virtual machines or restart virtual desktops.	Machine

Internal Privileges

Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

The following table describes the internal privileges and lists the predefined roles that contain each privilege.

Table 7-9. Internal Privileges

Privilege	Description	Predefined Roles
Full (Read only)	Grants read-only access to all settings.	Administrators (Read only)
Manage Inventory (Read only)	Grants read-only access to inventory objects.	Inventory Administrators (Read only)
Manage Global Configuration and Policies (Read only)	Grants read-only access to configuration settings and global policies except for administrators and roles.	Global Configuration and Policy Administrators (Read only)

Required Privileges for Common Tasks

Many common administration tasks require a coordinated set of privileges. Some operations require permission at the root access group in addition to access to the object that is being manipulated.

Privileges for Managing Pools

An administrator must have certain privileges to manage pools in Horizon Console.

The following table lists common pool management tasks and shows the privileges that are required to perform each task.

Table 7-10. Pool Management Tasks and Privileges

Task	Required Privileges
Enable or disable a desktop pool.	**Enable Farms and Desktop Pools**
Entitle or unentitle users to a pool.	**Entitle Desktop and Application Pools**
Add a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Modify or delete a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for deleting an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.

Task	Required Privileges
Add or remove desktops from a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding or removing unmanaged virtual desktops in the desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Refresh, recompose, rebalance, or change the default Horizon Console image.	**Manage Composer Desktop Pool Image**
Change access groups.	**Manage Farms and Desktop and Application Pools** on both the source and target access groups.

Privileges for Managing Machines

An administrator must have certain privileges to manage machines in Horizon Console.

The following table lists common machine management tasks and shows the privileges that are required to perform each task.

Table 7-11. Machine Management Tasks and Privileges

Task	Required Privileges
Remove a virtual machine.	**Manage Machine** or **Manage Farms and Desktop and Application Pools** **Note** Not applicable for removing unmanaged desktops or RDS hosts from the desktop pool or farm. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Reset a virtual machine.	**Manage Reboot Operation**
Restart a virtual desktop.	**Manage Reboot Operation**
Assign or remove user ownership.	**Manage Machine**
Enter or exit maintenance mode.	**Manage Machine**
Disconnect or log off sessions.	**Manage Sessions**

Privileges for Managing Persistent Disks

An administrator must have certain privileges to manage persistent disks in Horizon Console.

The following table lists common persistent disk management tasks and shows the privileges that are required to perform each task. You perform these tasks on the Persistent Disks page in Horizon Console.

Table 7-12. Persistent Disk Management Tasks and Privileges

Task	Required Privileges
Detach a disk.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** on the pool.
Attach a disk.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** on the machine.
Edit a disk.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** on the selected pool.
Change access groups.	**Manage Persistent Disks** on the source and target access groups.
Recreate a desktop.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** on the last pool.
Import from vCenter.	**Manage Persistent Disks** on the folder and **Manage Pool** on the pool.
Delete a disk.	**Manage Persistent Disks** on the disk.

Privileges for Managing Users and Administrators

An administrator must have certain privileges to manage users and administrators in Horizon Console.

The following table lists common user and administrator management tasks and shows the privileges that are required to perform each task. You manage users on the **Users and Groups** page in Horizon Console. You manage administrators on the **Global Administrators View** page in Horizon Console.

Table 7-13. User and Administrator Management Tasks and Privileges

Task	Required Privileges
Update general user information.	**Manage Global Configuration and Policies**
Send messages to users.	**Manage Remote Sessions** on the machine.
Add an administrator user or group.	**Manage Roles and Permissions**
Add, modify, or delete an administrator permission.	**Manage Roles and Permissions**
Add, modify, or delete an administrator role.	**Manage Roles and Permissions**

Privileges for Horizon Help Desk ToolTasks

Horizon Help Desk Tool administrators must have certain privileges to perform troubleshooting tasks in Horizon Console.

The following table lists common tasks that the Horizon Help Desk Tool administrator can perform and shows the privileges to perform each task.

Table 7-14. Horizon Help Desk Tool Tasks and Privileges

Tasks	Required Privileges
Read-only access to Horizon Help Desk Tool.	**Manage Help Desk (Read Only)**
Manage global sessions.	**Manage Global Sessions**

Tasks	Required Privileges
Can log in to Horizon Console.	**Console Interaction**
Perform all machine and session-related commands.	**Manage Machine**
Reset or restart machines.	**Manage Reboot Operation**
Disconnect and log off sessions.	**Manage Sessions**
Manage remote processes and applications.	**Manage Remote Processes and Applications**
Remote assistance to the virtual desktop or published desktop.	**Remote Assistance**
Disconnect, logoff, reset, and restart operations for global sessions.	**Manage Help Desk (Read Only)** and **Manage Global Sessions**
Reset and restart operations for local sessions.	**Manage Help Desk (Read Only)** and **Manage Reboot Operation**
Remote assistance operations.	**Manage Help Desk (Read Only)** and **Remote Assistance**
End remote processes and applications.	**Manage Help Desk (Read Only)** and **Manage Remote Processes and Applications**
Perform all tasks in Horizon Help Desk Tool.	**Manage Help Desk (Read Only)**, **Mange Global Sessions**, **Manage Reboot Operation**, **Remote Assistance**, and **Manage Remote Processes and Applications**
Remote assistance operations and end remote processes and applications.	**Manage Help Desk (Read Only)**, **Remote Assistance**, and **Manage Remote Processes and Applications**
Disconnect and logoff operations for local sessions.	**Manage Help Desk (Read Only)** and **Manage Sessions**

Privileges for General Administration Tasks and Commands

An administrator must have certain privileges to perform general administration tasks and run command line utilities.

The following table shows the privileges that are required to perform general administration tasks and run command line utilities.

Table 7-15. Privileges for General Administration Tasks and Commands

Task	Required Privileges
Add or delete an access group	Must have the Administrators role on the root access group.
Manage ThinApp applications and settings in Horizon Administrator	Must have the Administrators role on the root access group.
Install Horizon Agent on an unmanaged machine, such as a physical system, standalone virtual machine, or RDS host	**Register Agent**
View or modify configuration settings (except for administrators) in Horizon Administrator	**Manage Global Configuration and Policies**
Run all PowerShell commands and command line utilities except for `vdmadmin` and `vdmimport`.	**Direct Interaction**

Task	Required Privileges
Use the `vdmadmin` and `vdmimport` commands	Must have the Administrators role on the root access group.
Use the `vdmexport` command	Must have the Administrators role or the Administrators (Read only) role on the root access group.

Best Practices for Administrator Users and Groups

To increase the security and manageability of your Horizon 7 environment, you should follow best practices when managing administrator users and groups.

- Create new user groups in Active Directory and assign administrative roles to these groups. Avoid using Windows built-in groups or other existing groups that might contain users who do not need or should not have Horizon 7 privileges.
- Keep the number of users with Horizon 7 administrative privileges to a minimum.
- Because the Administrators role has every privilege, it should not be used for day-to-day administration.
- Because it is highly visible and easily guessed, avoid using the name Administrator when creating administrator users and groups.
- Create access groups to segregate sensitive desktops and farms. Delegate the administration of those access groups to a limited set of users.
- Create separate administrators that can modify global policies and Horizon 7 configuration settings.

Setting Policies in Horizon Console

8

You use Horizon Console to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. Policies that affect specific users and desktop pools are called user-level policies and desktop pool-level policies. Policies that affect all sessions and users are called global policies.

User-level policies inherit settings from the equivalent desktop pool-level policy settings. Similarly, desktop pool-level policies inherit settings from the equivalent global policy settings. A desktop pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and desktop pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, you can set a global policy to **Deny** and the equivalent desktop pool-level policy to **Allow**, or vice versa.

Note Only global policies are available for published desktop and application pools. You cannot set user-level policies or pool-level policies for published desktop and application pools.

This chapter includes the following topics:

- Configure Global Policies

Configure Global Policies

You can configure global policies to control the behavior of all client sessions users.

Procedure

1 In Horizon Console, select **Settings > Global Policies**.

The **Global Policies** pane shows the settings that affect all client sessions, desktop pools, or users.

Table 8-1. Horizon Policies

Policy	Description
Multimedia redirection (MMR)	Determines whether MMR is enabled for client systems. MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on remote desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played. The default value is **Deny**. If client systems have insufficient resources to handle local multimedia decoding, leave the setting as **Deny**. Multimedia Redirection (MMR) data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.
USB Access	Determines whether remote desktops can use USB devices connected to the client system. The default value is **Allow**. To prevent the use of external devices for security reasons, change the setting to **Deny**.
PCoIP hardware acceleration	Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session. This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the remote desktop. The default value is **Allow** at **Medium** priority.

2 Click **Edit Policies** to change the settings.

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

Maintaining Horizon 7 Components

9

To keep your Horizon 7 components available and running, you can perform a variety of maintenance tasks.

This chapter includes the following topics:

Backing Up and Restoring Horizon 7 Configuration Data

You can back up your Horizon 7 and Horizon Composer configuration data by scheduling or running automatic backups in Horizon Console. You can restore your Horizon 7 configuration by manually importing the backed-up View LDAP files and Horizon Composer database files.

You can use the backup and restore features to preserve and migrate Horizon 7 configuration data.

Backing Up Horizon Connection Server and Horizon Composer Data

After you complete the initial configuration of Connection Server, you should schedule regular backups of your Horizon 7 and Horizon Composer configuration data. You can preserve your Horizon 7 and Horizon Composer data by using Horizon Console.

Horizon 7 stores Connection Server configuration data in the View LDAP repository. Horizon Composer stores configuration data for linked-clone desktops in the Horizon Composerdatabase.

When you use Horizon Console to perform backups, Horizon 7 backs up the View LDAP configuration data and Horizon Composer database. Both sets of backup files are stored in the same location. The View LDAP data is exported in encrypted LDAP data interchange format (LDIF). For a description of View LDAP, see "View LDAP Directory" in the *Horizon 7 Administration* document.

You can perform backups in several ways.

- Schedule automatic backups by using the Horizon 7 configuration backup feature.
- Initiate a backup immediately by using the **Backup Now** feature in Horizon Console.
- Manually export View LDAP data by using the `vdmexport` utility. This utility is provided with each instance of Connection Server.

  The `vdmexport` utility can export View LDAP data as encrypted LDIF data, plain text, or plain text with passwords and other sensitive data removed.

  Note The `vdmexport` tool backs up the View LDAP data only. This tool does not back up Horizon Console database information.

  For more information about `vdmexport`, see Export Configuration Data from Horizon Connection Server.

The following guidelines apply to backing up Horizon 7 configuration data:

- Horizon 7 can export configuration data from any Connection Server instance.
- If you have multiple Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.
- Do not rely on using replicated instances of Connection Server to act as your backup mechanism. When Horizon 7 synchronizes data in replicated instances of Connection Server, any data lost in one instance might be lost in all members of the group.
- If Connection Server uses multiple vCenter Server instances with multiple Horizon Composer services, Horizon 7 backs up all the Horizon Composer databases associated with the vCenter Server instances.

Schedule Horizon 7 Configuration Backups

You can schedule your Horizon 7 configuration data to be backed up at regular intervals. Horizon 7 backs up the contents of the View LDAP repository in which your Connection Server instances store their configuration data.

You can back up the configuration immediately by selecting the Connection Server instance and clicking **Backup Now**.

Prerequisites

Familiarize yourself with the backup settings. See Horizon 7 Configuration Backup Settings.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance to be backed up and click **Backup Now**.

3 On the **Backup** tab, specify the Horizon 7 configuration backup settings to configure the backup frequency, maximum number of backups, and the folder location of the backup files.

4 (Optional) Change the data recovery password.

  a Click **Change data recovery password**.

  b Type and retype the new password.

  c (Optional) Type a password reminder.

  d Click **OK**.

5 Click **OK**.

Horizon 7 Configuration Backup Settings

Horizon 7 can back up your Connection Server and Horizon Composer configuration data at regular intervals. In Horizon Console, you can set the frequency and other aspects of the backup operations.

Table 9-1. Horizon 7 Configuration Backup Settings

Setting	Description
Automatic backup frequency	Every Hour. Backups take place every hour on the hour. Every 6 Hours. Backups take place at midnight, 6 am, noon, and 6 pm. Every 12 Hours. Backups take place at midnight and noon. Every Day. Backups take place every day at midnight. Every 2 Days. Backups occur at midnight on Saturday, Monday, Wednesday, and Friday. Every Week. Backups take place weekly at midnight on Saturday. Every 2 Weeks. Backups take place every other week at midnight on Saturday. Never. Backups do not take place automatically.
Backup time	Time to schedule a backup.
Backup time offset	Time offset for a scheduled backup.
Max number of backups	Number of backup files that can be stored on the Connection Server instance. The number must be an integer greater than 0. When the maximum number is reached, Horizon 7 deletes the oldest backup file. This setting also applies to backup files that are created when you use **Backup Now**.
Folder location	Default location of the backup files on the computer where Connection Server is running: `C:\Programdata\VMWare\VDM\backups` When you use **Backup Now**, Horizon 7 also stores the backup files in this location.

Export Configuration Data from Horizon Connection Server

You can back up configuration data of a Horizon Connection Server instance by exporting the contents of its View LDAP repository.

You use the `vdmexport` command to export the View LDAP configuration data to an encrypted LDIF file. You can also use the `vdmexport –v` (verbatim) option to export the data to a plain text LDIF file, or the `vdmexport –c` (cleansed) option to export the data as plain text with passwords and other sensitive data removed.

You can run the vdmexport command on any Connection Server instance. If you have multiple Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.

Note The vdmexport.exe command backs up the View LDAP data only. This command does not back up Horizon Composer database information.

Prerequisites

- Locate the vdmexport.exe command executable file installed with Connection Server in the default path.

  C:\Program Files\VMware\VMware View\Server\tools\bin
- Log in to a Connection Server instance as a user in the Administrators or Administrators (Read only) role.

Procedure

1 Select **Start > Command Prompt**.

2 At the command prompt, type the vdmexport command and redirect the output to a file. For example:

```
vdmexport > Myexport.LDF
```

By default, the exported data is encrypted.

You can specify the output file name as an argument to the -f option. For example:

```
vdmexport -f Myexport.LDF
```

You can export the data in plain text format (verbatim) by using the -v option. For example:

```
vdmexport -f Myexport.LDF -v
```

You can export the data in plain text format with passwords and sensitive data removed (cleansed) by using the -c option. For example:

```
vdmexport -f Myexport.LDF -c
```

Note Do not plan on using cleansed backup data to restore a View LDAP configuration. The cleansed configuration data is missing passwords and other critical information.

For more information about the vdmexport command, see the *Horizon 7 Integration* document.

What to do next

You can restore or transfer the configuration information of Connection Server by using the vdmimport command.

For details about importing the LDIF file, see Restoring Horizon Connection Server and Horizon Composer Configuration Data.

Restoring Horizon Connection Server and Horizon Composer Configuration Data

You can manually restore the Connection Server LDAP configuration files and Horizon Composer database files that were backed up by Horizon 7.

You manually run separate utilities to restore Connection Server and Horizon Composer configuration data.

Before you restore configuration data, verify that you backed up the configuration data in Horizon Console. See Backing Up Horizon Connection Server and Horizon Composer Data.

You use the `vdmimport` utility to import the Connection Server data from the LDIF backup files to the View LDAP repository in the Connection Server instance.

You can use the `SviConfig` utility to import the Horizon Composer data from the `.svi` backup files to the Horizon Composer SQL database.

Note In certain situations, you might have to install the current version of a Connection Server instance and restore the existing Horizon 7 configuration by importing the Connection Server LDAP configuration files. You might require this procedure as part of a business continuity and disaster recovery (BC/DR) plan, as a step in setting up a second datacenter with the existing Horizon 7 configuration, or for other reasons. For more information, see the *Horizon 7 Installation* document.

Import Configuration Data into Horizon Connection Server

You can restore configuration data of a Connection Server instance by importing a backup copy of the data stored in an LDIF file.

You use the `vdmimport` command to import the data from the LDIF file to the View LDAP repository in the Connection Server instance.

If you backed up your View LDAP configuration by using Horizon Console or the default `vdmexport` command, the exported LDIF file is encrypted. You must decrypt the LDIF file before you can import it.

If the exported LDIF file is in plain text format, you do not have to decrypt the file.

Note Do not import an LDIF file in cleansed format, which is plain text with passwords and other sensitive data removed. If you do, critical configuration information will be missing from the restored View LDAP repository.

For information about backing up the View LDAP repository, see Backing Up Horizon Connection Server and Horizon Composer Data.

Prerequisites

- Locate the `vdmimport` command executable file installed with Connection Server in the default path.

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- Log in to a Connection Server instance as a user with the Administrators role.

- Verify that you know the data recovery password. If a password reminder was configured, you can display the reminder by running the `vdmimport` command without the password option.

Procedure

1 Stop all instances of Horizon Composer by stopping the VMware Horizon Composer Windows service on the servers where Horizon Composer runs.

2 Uninstall all instances of Horizon Connection Server.

Uninstall both VMware Horizon Connection Server and AD LDS Instance VMwareVDMDS.

3 Install one instance of Connection Server.

4 Stop the Connection Server instance by stopping the Windows service VMware Horizon Connection Server.

5 Click **Start > Command Prompt**.

6 Decrypt the encrypted LDIF file.

At the command prompt, type the `vdmimport` command. Specify the `–d` option, the `–p` option with the data recovery password, and the `–f` option with an existing encrypted LDIF file followed by a name for the decrypted LDIF file. For example:

If you do not remember your data recovery password, type the command without the `–p` option. The utility displays the password reminder and prompts you to enter the password.

7 Import the decrypted LDIF file to restore the View LDAP configuration.

Specify the `–f` option with the decrypted LDIF file. For example:

8 Uninstall Connection Server.

Uninstall only the package VMware Horizon Connection Server.

9 Reinstall Connection Server.

10 Log in to Horizon Console and validate that the configuration is correct.

11 Start the Horizon Composer instances.

12 Reinstall the replica server instances.

The `vdmimport` command updates the View LDAP repository in Connection Server with the configuration data from the LDIF file. For more information about the `vdmimport` command, see the *Horizon 7 Installation* document.

Note Make sure that the configuration that is being restored matches the virtual machines that are known to vCenter Server, and to Horizon Composer if it is in use. If necessary, restore the Horizon Composer configuration from backup. See Restore a Horizon Composer Database. After you restore the Horizon Composer configuration, you may need to manually resolve inconsistencies if the virtual machines in vCenter Server have changed since the backup of the Horizon Composer configuration.

Restore a Horizon Composer Database

You can import the backup files for your Horizon Composer configuration into the Horizon Composer database that stores linked-clone information.

You can use the `SviConfig restoredata` command to restore Horizon Composer database data after a system failure or to revert your Horizon Composer configuration to an earlier state.

Important Only experienced Horizon Composer administrators should use the `SviConfig` utility. This utility is intended to resolve issues relating to the Horizon Composer service.

Prerequisites

Verify the location of the Horizon Composer database backup files. By default, Horizon 7 stores the backup files on the `C:` drive of the Connection Server computer, at `C:\Programdata\VMWare\VDM\backups`.

Horizon Composer backup files use a naming convention with a date stamp and an `.svi` suffix.

`Backup-`*`YearMonthDayCount-vCenter Server Name_Domain Name`*`.svi`

For example: `Backup-20090304000010-foobar_test_org.svi`

Familiarize yourself with the `SviConfig restoredata` parameters:

- `DsnName` - The DSN that is used to connect to the database. The `DsnName` parameter is mandatory and cannot be an empty string.
- `Username` - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- `Password` - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- `BackupFilePath` - The path to the Horizon Composer backup file.

The `DsnName` and `BackupFilePath` parameters are required and cannot be empty strings. The `Username` and `Password` parameters are optional.

Procedure

1. Copy the Horizon Composer backup files from the Connection Server computer to a location that is accessible from the computer where the VMware Horizon Composer service is installed.
2. On the computer where Horizon Composer is installed, stop the VMware Horizon Composer service.
3. Open a Windows command prompt and navigate to the `SviConfig` executable file.

   The file is located with the Horizon Composer application. The default path is `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

4 Run the `SviConfig restoredata` command.

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

For example:

```
sviconfig -operation=restoredata -dsnname=LinkedClone
-username=Admin -password=Pass
-backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

5 Start the VMware Horizon Composer service.

What to do next

For output result codes for the `SviConfig restoredata` command, see Result Codes for Restoring the Horizon Console Database.

Result Codes for Restoring the Horizon Console Database

When you restore a Horizon Console database, the `SviConfig restoredata` command displays a result code.

Table 9-2. Restoredata Result Codes

Code	Description
0	The operation ended successfully.
1	The supplied DSN could not be found.
2	Invalid database administrator credentials were provided.
3	The driver for the database is not supported.
4	An unexpected problem occurred and the command failed to complete.
14	Another application is using the VMware Horizon Console service. Shut down the service before executing the command.
15	A problem occurred during the restore process. Details are provided in the onscreen log output.

Export Data in Horizon Composer Database

You can export data from your Horizon Composer database to file.

Important Use the `SviConfig` utility only if you are an experienced Horizon Composer administrator.

Prerequisites

By default, Horizon 7 stores the backup files on the `C:` drive of the Connection Server computer, at `C:\Programdata\VMWare\VDM\backups`.

Familiarize yourself with the `SviConfig exportdata` parameters:

- `DsnName` - The DSN that is used to connect to the database. If it is not specified, DSN name, user name and password will be retrieved from server configuration file.
- `Username` - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- `Password` - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- `OutputFilePath` - The path to the output file.

Procedure

1. On the computer where Horizon Composer is installed, stop the VMware Horizon Composer service.
2. Open a Windows command prompt and navigate to the `SviConfig` executable file.

   The file is located with the Horizon Composer application.

   Horizon-Composer-installation-directory`\sviconfig.exe`
3. Run the `SviConfig exportdata` command.

   ```
   sviconfig -operation=exportdata
             -DsnName=target_database_source_name_(DSN)
             -Username=database_administrator_username
             -Password=database_administrator_password
             -OutputFilePath=path_to_Horizon_Composer_output_file
   ```

   For example:

   ```
   sviconfig -operation=exportdata -dsnname=LinkedClone
   -username=Admin -password=Pass
   -outputfilepath="C:\Program Files\VMware\VMware View
   Composer\Export-20090304000010-foobar_test_org.SVI"
   ```

What to do next

For export result codes for the `SviConfig exportdata` command, see Result Codes for Exporting the Horizon Composer Database.

Result Codes for Exporting the Horizon Composer Database

When you export a Horizon Composer database, the `SviConfig exportdata` command displays an exit code.

Table 9-3. Exportdata ExitStatus Codes

Code	Description
0	Exporting data ended successfully.
1	The supplied DSN name can not be found.
2	The supplied credentials are invalid.
3	Unsupported driver for the provided database.
4	An unexpected problem has occurred.
18	Unable to connect to the database server.
24	Unable to open the output file.

Change the Product License Key or License Modes in Horizon Console

If the current license on a system expires, or if you want to access Horizon 7 features that are currently unlicensed, you can use Horizon Console to change the product license key. Based on your Horizon 7 deployment on VMware Horizon Cloud Service, you can get either a perpetual license or a subscription license for Horizon 7. You can use Horizon Console to change from the license mode from a subscription license to a perpetual license and vice versa for a pod.

You can add a license to Horizon 7 while Horizon 7 is running. You do not need to reboot the system, and access to desktops and applications is not interrupted.

Prerequisites

- For the successful operation of Horizon 7 and add-on features such as Horizon Composer and published applications, obtain a valid product license key.
- To use a subscription license, verify that you enable Horizon 7 for a subscription license. See, the *Horizon 7 Installation* document. The **Licensing** panel displays information about the subscription license for the Horizon 7 pod.

Procedure

1. In Horizon Console, select **Settings > Product Licensing and Usage**.

   The first and last five characters of the current license key are displayed in the **Licensing** panel.

2. To edit the license key, click **Edit License**, Enter the license serial number and click **OK**.

   The **Licensing Settings** panel shows the updated licensing information.

3. (Optional) To change from a subscription license to a perpetual license for a Horizon 7 pod, click **Use Perpetual License** and click **OK**.

   The **Licensing Settings** panel shows the updated licensing information.

4 (Optional) To change from a perpetual license to a subscription license for a Horizon 7 pod, click **Use Subscription License** and click **OK**. The VMware Horizon Cloud Service administrator can then enable the Horizon 7 pod for a subscription license.

   The **Licensing Settings** panel shows the updated licensing information.

5 Verify the license expiration date.

6 Verify that the Desktop, Application Remoting, and Horizon Composer licenses are enabled or disabled, based on the edition of VMware Horizon 7 that your product license entitles you to use.

   Not all features and capabilities of VMware Horizon 7 are available in all editions. For a comparison of feature sets in each edition, see http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf.

7 Verify that the licensing usage model matches the model that is used in your product license.

   Usage is counted by the number of named users or concurrent users, depending on the edition and usage agreement for your product license.

Monitoring License Usage

In Horizon Console, you can monitor the active users who are concurrently connected to Horizon 7. The **Usage Settings** panel displays the current and highest historical usage numbers. You can use these numbers to keep track of your product license usage. You can also reset the historical usage data and start over with the current data.

Horizon 7 provides two licensing usage models, one for named users and one for concurrent users. Horizon 7 counts the named users and concurrent users in your environment, regardless of your product license edition or usage model agreement.

For named users, Horizon 7 counts the number of unique users that have accessed the Horizon 7 environment. If a named user runs multiple single-user desktops, published desktops, and published applications, the user is counted once.

For named users, the **Current** column on the **Usage Settings** panel displays the number of users since your Horizon 7 deployment was first configured or since you last reset the named users count. The **Highest** column is not applicable to named users.

For concurrent users, Horizon 7 counts single-user desktop connections per session. If a concurrent user runs multiple single-user desktops, each connected desktop session is counted separately.

For concurrent users, published desktop and application connections are counted per user. If a concurrent user runs multiple published desktop sessions and applications, the user is counted only once, even if different published desktops or applications are hosted on different RDS hosts. If a concurrent user runs a single-user desktop and additional published desktops and applications, the user is counted only once.

For concurrent users, the **Highest** column on the **Usage Settings** panel displays the highest number of concurrent desktop sessions and published desktop and application users since your Horizon 7 deployment was first configured or since you last reset the highest count.

You can monitor the number of collaborative sessions and session collaborators connected to a session.

- Active - collaboration sessions: the number of sessions where a session owner has invited one or more users to join a session. Example: John has invited two people to join his session and Mary has invited one person to join her session. The value of this row is 2, regardless of whether any of the invitees have joined the session.
- Active - total collaborators: the total number of users that are connected to a collaborative session, including the session owner and any collaborators. Example: John has invited two people and only one person has joined the session. Mary has invited one person who has not joined the session. The value of this row is 3: John's collaborative session has one primary and one secondary, while Mary's collaborative session has one primary and zero secondary. Because the session owner is counted, it is guaranteed that the total number of collaborators is always greater than or equal to the total number of collaborative sessions.

Reset License Usage Data

In Horizon Console, you can reset the historical product usage data and start over with the current data.

An administrator with the **Manage Global Configuration and Policies** privilege can select the **Reset Highest Count** and **Reset Named Users Count** settings. To restrict access to these settings, give this privilege to designated administrators only.

Prerequisites

Familiarize yourself with product license usage. See Monitoring License Usage.

Procedure

1. In Horizon Console, select **Settings > Product Licensing and Usage**.
2. (Optional) In the **Usage** pane, select **Reset Highest Count**.

   The highest historical number of concurrent connections is reset to the current number.
3. (Optional) In the **Usage** pane, select **Reset Named Users Count**.

Customer Experience Improvement Program

This product participates in VMware’s Customer Experience Improvement Program (“CEIP”). You can choose to join or leave the CEIP for this product.

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Procedure

1. In Horizon Console, select **Settings > Product Licensing and Usage**.
2. In the **Customer Experience Program** tab, click **Edit Settings**.

3 Select **Join VMware Customer Experience Improvement Program** to join CEIP.

If you do not select this option, you cannot join CEIP.

4 (Optional) Select your geographic location, business vertical, or the number of employees in your organization.

5 Click **OK**.

Creating Virtual Desktop Pools in Horizon Console 10

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 10-1. 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.	

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.	
Refresh OS disk after logoff	Select whether and when to refresh the OS disks. ■ **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. Enter 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 desktop 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 instant clone's OS disk is the size of the replica's OS disk. Enter the percentage at which refresh operations occur. ■ **Never**. The OS disk is never refreshed.	
Reclaim VM disk space	Determine whether to allow ESXi hosts to reclaim unused disk space on instant clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for instant clone desktops.	
Initiate reclamation when unused space on VM exceeds:	Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a instant clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, Horizon 7 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 Horizon 7 starts the space reclamation process on that machine. The default value is 1 GB.	

Option	Description	Fill In Your Value Here
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.	
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.	

Option	Description	Fill In Your Value Here
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.	
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	

Option	Description	Fill In Your Value Here
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.	
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**.	

Option	Description	Fill In Your Value Here
Domain	Select an Active Directory domain. The drop-down list shows the domains that you specify when you configure instant-clone domain administrators.	
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 10-2. 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.	

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.	
Template	Select the virtual machine template to use for creating the pool.	

Option	Description	Fill In Your Value Here
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.	

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 Horizon 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. Horizon 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 10-3. 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.	
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.	

Option	Description	Fill In Your Value Here
Persistent disk	If you select dedicated user assignments, choose whether to store Windows user-profile data on a separate Horizon 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 Horizon Composer persistent disk. Separate persistent disks let you preserve user data and settings. Horizon 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 Horizon Composer persistent disk, provide the disk size in megabytes. ■ **Drive letter**. If you store user profile data on a separate Horizon 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.	

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.	

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 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.	

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 Horizon 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 Horizon Composer maintenance operations take place. This setting allows users to maintain existing connections or make new connection requests while Horizon 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. For more information, see 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.	

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 Horizon 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.	

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.	

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 Horizon Storage Accelerator	Determine whether to use Horizon Storage Accelerator, which allows ESXi hosts to cache common virtual machine disk data. Horizon 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 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.	
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 the *Setting Up Virtual Desktops in Horizon 7* document.	

Option	Description	Fill In Your Value Here
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, Horizon 7 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 Horizon 7 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 Horizon 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.	

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. Horizon 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 Horizon Composer settings for vCenter Server. You can specify multiple domains and users when you configure Horizon Composer settings. When you use the **Add Desktop Pool** wizard to create a pool, you must select one domain and user from the list.	
AD container	Provide the Active Directory container relative distinguished name. For example: `CN=Computers` When you run the **Add Desktop Pool** wizard, you can browse your Active Directory tree for the container.	

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 Horizon 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, Horizon 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 Horizon 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 Horizon 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 10-4. 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 Horizon Composer service dynamically creates a new linked-clone virtual machine in vCenter Server for each desktop.

Prerequisites

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

- Verify that Horizon 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. Horizon 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 Console. 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 Horizon 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.

Horizon 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, Horizon 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 10-5. 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.	

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 10-6. 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		
Max resolution of any one monitor	Yes	Yes		
Adobe Flash quality	Yes	Yes	Yes	Yes

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
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.

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 10-7. 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.

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 10-8. 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 10-9. 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 10-10. 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.
Session Types	You can create application pools based on desktop pools by selecting the supported session type for the desktop pool: ■ **Desktop**. Only desktops are supported. ■ **Application**. Only applications are supported. ■ **Desktop and Application.** Both desktop and applications are supported.

Setting	Options
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.
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. **Note** Multi-session is not supported for applications running on desktop pools, so this setting is not applicable for applications created from a desktop pool.
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.

Setting	Options
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.
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.

Setting	Options
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.
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.

Setting	Options
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.

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 Horizon Composer Linked-Clone Desktop Virtual Machines

You can update Horizon 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, Horizon 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**, **Cancel task**, or **Resume task** to suspend a task, cancel 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 Horizon 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 Horizon 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.

Horizon 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 Horizon 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.

Updated Linked-Clone Desktops in Horizon Console

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.

Horizon 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, Horizon 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 Horizon 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 **Horizon 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 **Horizon 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**, **Cancel task**, or **Resume task** to suspend a task, cancel 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. Horizon 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 Horizon 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.

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

   Horizon 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 Horizon 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 #unique_185.
- Decide when to schedule the rebalance operation. By default, Horizon 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 Horizon 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 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 Horizon Console, you can monitor the operation by selecting **Inventory > Desktops**, double-clicking the pool ID, and clicking the **Tasks** tab. You can click **Pause task**, **Cancel task**, or **Resume task** to suspend a task, cancel 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 Horizon 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 Horizon 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 Horizon 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 Horizon Composer Persistent Disks

You can detach a Horizon 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.

Horizon Composer Persistent Disks

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

A Horizon 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 Horizon Composer Persistent Disk in Horizon Console

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

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

You can assign a detached Horizon 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.

Recreate a Linked Clone With a Detached Persistent Disk in Horizon Console

When you detach a Horizon Composer persistent disk, the linked clone is deleted. You can give the original user access to the detached user settings and information by recreating the linked-clone virtual machine from the detached disk.

Note If you recreate a linked-clone virtual machine in a desktop pool that has reached its maximum size, the recreated virtual machine is still added to the desktop pool. The desktop pool size grows and then reduces as unassigned machines are deleted.

If a persistent disk's original desktop pool or user was deleted from Horizon 7, you can assign a new one to the persistent disk. See Edit a Horizon Composer Persistent Disk's Pool or User in Horizon Console.

Horizon 7 does not support recreating a virtual machine with a persistent disk that is stored on a non-vSAN datastore if the new virtual machine is stored on a vSAN datastore. Similarly, if the persistent disk is stored on vSAN, Horizon 7 does not support recreating a virtual machine on non-vSAN.

To move a detached persistent disk from non-vSAN to vSAN, you can recreate the disk on a virtual machine that is stored on a non-vSAN datastore and rebalance the virtual machine's desktop pool to a vSAN datastore.

Procedure

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

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

   You can select multiple persistent disks to recreate a linked-clone virtual machine for each disk.

3 Click **OK**.

Horizon 7 creates a linked-clone virtual machine for each persistent disk you select and adds the virtual machine to the original desktop pool.

The persistent disks remain on the datastore where they were stored.

Restore a Linked Clone in Horizon Console by Importing a Persistent Disk from vSphere

If a linked-clone virtual machine becomes inaccessible in Horizon 7, you can restore the virtual machine if it was configured with a Horizon Composer persistent disk. You can import the persistent disk from a vSphere datastore into Horizon 7.

You import the persistent disk file as a detached persistent disk in Horizon 7. You can either attach the detached disk to an existing virtual machine or recreate the original linked clone in Horizon 7.

Procedure

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

2 On the **Detached** tab, click **Import from vCenter**.

3 Select a vCenter Server instance.

4 Select the datacenter where the disk file is located.

5 Select a linked-clone desktop pool.

> **Note** After you select a desktop pool, you can only browse and select a persistent disk that is based on the datatstore of the desktop pool. For example, if you select a desktop pool that has a vSAN datastore, you can only browse and select a persistent disk from vSAN datastores.

6 Select an access group.

7 In the **Persistent Disk File** text box, click **Browse**, click the down arrow, and select a datastore from the **Choose a Datastore** menu.

8 To import a persistent disk from a local datastore, select **Show all datastores (including local datastores)**.

9 Click the datastore name to display its disk storage files and virtual-machine files.

10 Select the persistent-disk file you want to import and click **OK**.

11 In the **User** text box, click **Browse**, select a user to assign to the virtual machine, and click **OK**.

12 Click **Submit**.

The disk file is imported into Horizon 7 as a detached persistent disk.

What to do next

To restore the linked-clone virtual machine, you can recreate the original virtual machine or attach the detached persistent disk to another virtual machine.

For details, see Recreate a Linked Clone With a Detached Persistent Disk in Horizon Console and Attach a Horizon Composer Persistent Disk to Another Linked Clone in Horizon Console.

Delete a Detached Horizon 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 **Settings > 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 10-11. 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

11

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

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 11-1. 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**.	

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 **Settings > Registered Machines** and check the status of each RDS host on the RDS Hosts tab.
- Gather the configuration information you must provide to create the farm. See Worksheet for Creating a Manual Farm in Horizon 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 11-2. 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**.	

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**.	

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.	

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.	

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.	
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.	

Setting	Description	Fill in Your Value Here
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 Select **Instant clone**.

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

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

What to do next

Create a published application pool or a published desktop pool. See Creating Published Desktop Pools in Horizon Console or Creating Application Pools in Horizon Console.

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

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

Table 11-3. Worksheet: Configuration Settings for Creating an Automated Linked-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in Horizon Console.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the *Horizon 7 Administration* document.	
Default display protocol	Select **VMware Blast**, **PCoIP** or **RDP**. RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to RDS desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is **Yes**.	

Setting	Description	Fill in Your Value Here
Pre-launch session timeout (applications only)	Determines the amount of time that an application configured for pre-launch is kept open. The default is **10 minutes**. If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out. If you want to end the pre-launch session after timeout, you must set the **Log off disconnected session** option to **Immediate**.	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs off or disconnects within 30 seconds. You can further reduce the time the session logs off or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session log off to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session log off to 5 seconds.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the **Enabled** box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	
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 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.	

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 View Composer maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while View Composer recomposes the machines in the farm.	
Use 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 "UsingvSAN for High-Performance Storage and Policy-Based Management" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Select separate datastores for replica and OS disks	(Available only if you do not use vSAN) You can place replica and OS disks on different datastores for performance or other reasons.	
Parent VM	Select a parent virtual machine from the list. Be aware that the list includes virtual machines that do not have View Composer Agent installed. You must not select any of those machines because View Composer Agent is required. A good practice is to use a naming convention that indicates whether a virtual machine has View Composer Agent installed.	
Snapshot	Select the snapshot of the parent virtual machine to use as the base image for the farm. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no linked clones in the farm use the default image, and no more linked clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new linked clones in the farm, according to farm policies. The parent virtual machine and snapshot are also required for View Composer maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	

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 Linked Clone Datastores** page of the Add Farm wizard provides high-level guidelines for estimating the farm's storage requirements. These guidelines can help you determine which datastores are large enough to store the linked-clone disks. For details, see "Storage Sizing for Instant-Clone and Linked-Clone Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document. You can use shared or local datastores for an individual ESXi host or for ESXi clusters. If you use local datastores in an ESXi cluster, you must consider the vSphere infrastructure constraints that are imposed on your desktop deployment. For details, see "Storing Linked Clones on Local Datastores" in the *Setting Up Virtual Desktops in Horizon 7* document.. **Note** If you use vSAN, select only one datastore.	
Storage Overcommit	Determine the storage-overcommit level at which linked-clones are created on each datastore. As the level increases, more linked clones fit on the datastore and less space is reserved to let individual clones grow. A high storage-overcommit level lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore. For details, see "Storage Overcommit for View Composer Linked-Clone Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document. **Note** This setting has no effect if you use vSAN.	
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 VAAI Storage for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document..	

Setting	Description	Fill in Your Value Here
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, Horizon 7 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 Horizon 7 starts the space reclamation process on that machine. For example: 2 GB. The default value is 1 GB.	
Blackout Times	Configure days and times during which the reclamation of virtual machine disk space do not take place. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days. For details, see " Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Farm**, **Pod**, or **Global**. If you turn on TPS for all the machines in the farm, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the farm level but the farm is spread across multiple ESXi hosts, only virtual machines on the same host and within the same farm will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which farm the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	

Setting	Description	Fill in Your Value Here
Domain	Select the Active Directory domain and user name. View Composer requires certain user privileges to farm. The domain and user account are used by Sysprep to customize the linked-clone machines. You specify this user when you configure View Composer settings for vCenter Server. You can specify multiple domains and users when you configure View Composer settings. When you use the **Add Farm** wizard to create a farm, you must select one domain and user from the list. For information about configuring View Composer, see the *Horizon 7 Administration* document.	
AD container	Provide the Active Directory container relative distinguished name. For example: `CN=Computers` When you run the **Add Farm** wizard, you can browse your Active Directory tree for the container.	
Allow reuse of pre-existing computer accounts	Select this setting to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This setting lets you control the computer accounts that are created in Active Directory. When a linked clone is provisioned, if an existing AD computer account name matches the linked clone machine name, View Composer uses the existing computer account. Otherwise, a new computer account is created. The existing computer accounts must be located in the Active Directory container that you specify with the **Active Directory container** setting. When this setting is disabled, a new AD computer account is created when View Composer provisions a linked clone. This setting is disabled by default. For details, see "Use Existing Active Directory Computer Accounts for Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.	
Use a customization specification (Sysprep)	Provide a Sysprep customization specification to customize the virtual machines.	

Create an Automated Linked-Clone Farm in Horizon Console

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

Prerequisites

- Verify that the View Composer service is installed. See the *Horizon 7 Installation* document.
- Verify that View Composer settings for vCenter Server are configured. 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. Both Horizon Agent and View Composer Agent must be installed on the parent virtual machine. See, the *Horizon 7 Administration* 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 farm from a virtual machine template.

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

Procedure

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

2 Click **Add**.

3 Select **Automated Farm**.

4 Select **View Composer linked clones**.

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

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

In Horizon Console, you can now view the farm by clicking **Inventory > Farms**.

What to do next

Create a published application pool or a published desktop pool. See Creating Published Desktop Pools in Horizon Console or Creating Application Pools in Horizon Console.

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 11-4. 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 or a desktop pool.

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

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

When you create an application pool, Horizon 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 or desktop pool. You can select one or more applications from the list. If you select multiple applications from the list, a separate application pool is created for each application. You can also manually specify an application that is not on the list. If an application that you want to manually specify is not already installed, Horizon 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 or desktop pool.

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 11-5. Worksheet: Application Properties for Creating an Application Pool Manually

Property	Description	Fill in Your Value Here
Select an RDS Farm or Desktop Pool	Select a farm or a desktop pool from the list of desktops with supported session type Application or Application and Desktop.	
ID	Unique name that identifies the pool in Horizon 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** This setting is not supported for applications based on a desktop pool. **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.	

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.	

Property	Description	Fill in Your Value Here
Client Restrictions	Select whether to restrict access to entitled application pools from certain client computers. You must add the names of the computers that are allowed to access the application pool in an Active Directory security group. You can select this security group when you add users or groups to the application pool entitlement.	
Multi-Session Mode	You can start published application sessions in the following modes: Single-session: If the user opens a published application on client A in single-session mode, and then opens the same published application or another published application based on the same farm on client B then, the session on client A is disconnected and reconnected on client B. Multi-session: If the user opens a published application on client A in multi-session mode, and then opens the same published application or another published application based on the same farm on client B, the published application remains open on client A and a new session of the published application opens on client B. Such sessions are logged off on disconnect. You cannot enable the session pre-launch feature when multi-session mode is enabled. The multi-session mode has the following values: ■ **Disabled**. Multi-session mode is not supported. ■ **Enabled (Default Off)**. Multi-session mode is supported, but it is disabled by default. To use multi-session mode, users must enable the **Multi-Launch** setting in Horizon Client 4.10 or later. If the user has an earlier version of Horizon Client, the application is always started in single-session mode. ■ **Enabled (Default On)**. Multi-session mode is supported, and it is enabled by default. Users can disable multi-session mode by disabling the **Multi-Launch** setting in Horizon Client 4.10 or later. If the user has an earlier version of Horizon Client, the application is always started in single-session mode. ■ **Enabled (Enforced)**. Multi-session mode is always enabled. Users cannot disable it in any version of Horizon Client and the application is always launched in multi-session mode. If the user has an earlier version of Horizon Client, users get the following error message: "This application does not support the requested launch mode." When multi-session mode is enabled you can also configure the **max-sessions count** setting. This sets the maximum number of concurrent multi-sessions that can be started by a user for the same published application from different client devices. You can open a published application from a client	

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 or a desktop pool.

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.
- Create a manual or automated desktop pool. See Chapter 10 Creating Virtual Desktop Pools 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.

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

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

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.
- Anti-affinity rules do not affect application launches from within an RDS desktop session.
- RDS session limits prevent application sessions from being created, regardless of anti-affinity rules.
- In certain circumstances, the instances of applications on the RDS host might not be restricted to the maximum count that you specify. For example, Horizon 7 cannot determine the exact instance count if other applications for other pending sessions are in the process of being launched.

- Inter-application anti-affinity rules are not supported. For example, large application classes, such as Autocad and Visual Studio instances, cannot be counted in a single rule.
- Do not use anti-affinity rules in environments where end-users use Horizon Client on mobile clients. Anti-affinity rules can result in multiple sessions in the same farm for an end user. Reconnecting to multiple sessions on mobile clients can result in indeterminate behavior.
- Anti-Affinity rules consider only the connected number of sessions for load balancing. However, load balancing for RDS hosts considers the sum of the connected, pending, and disconnected sessions for load balancing.

Managing 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.

Change the Icon of a Published Application

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

Prerequisites

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

Procedure

1. In Horizon Console, select **Inventory > Applications**.
2. Select an application pool or multiple application pools and click **Application Icon > Associate Application Icon**.
3. To upload an icon, click **Upload Icon File** and browse for an icon in the .PNG format.

   The icon file must be between 16x16 pixels and 256x256 pixels.
4. Click **OK**.

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

Remove the Icon of a Published Application

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

Procedure

1. In Horizon Console, select **Inventory > Applications**.
2. Select an application pool or multiple application pools and click **Application Icon > Remove Application Icon**.

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

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

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

The properties are displayed and have the following meanings:

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

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 11-6. 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. The **Sessions** column also appears on the **Desktop Pools** page for all desktops. Select **Inventory > Farms**, click a farm's ID, and click the **Sessions** tab. The **Sessions** column also appears on the **Farms** page for all farms. Select **Settings > Registered Machines**, and view the **Sessions** column.
Remote desktop and application sessions	Select **Monitor > Sessions**.
Sessions associated with a user or user group	■ Select **Users and Groups**. ■ Click a user's name or a user group's name. ■ Click on the **Sessions** tab.

2 Select a session.

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

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

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

12

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 published applications within the network.

For information about configuring global entitlements in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

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

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**.

Configuring Shortcuts for Entitled Pools

You can configure shortcuts for entitled pools. When an entitled user connects to a Connection Server instance from a Windows client, Horizon Client for Windows places these shortcuts in the Start menu, on the desktop, or both, on the user's client device. You can configure a shortcut when you create or modify a pool.

You must select a category folder, or the root (/) folder, during shortcut configuration. You can add and name your own category folders. You can configure up to four folder levels. For example, you might add a category folder named Office and select that folder for all work-related apps, such as Microsoft Office and Microsoft PowerPoint.

For Start menu shortcuts, on Windows 7 client devices, Horizon Client places category folders and shortcuts in the VMware Applications folder in the Start menu. If you select the root (/) folder for a shortcut, Horizon Client places the shortcut directly in the VMware Applications folder. On Windows 8 and Windows 10 client devices, Horizon Client places category folders and shortcuts in the Apps list. If you select the root (/) folder for a shortcut, Horizon Client places the shortcut directly in the Apps list.

After you create a shortcut, a check mark appears in the **App Shortcut** column for the pool in Horizon Administrator and Horizon Console.

By default, Horizon Client for Windows prompts entitled users to install shortcuts the first time they connect to a server. You can configure Horizon Client for Windows to install shortcuts automatically, or to never install shortcuts, by modifying the **Automatically install shortcuts when configured on the Horizon server** group policy setting. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

By default, changes that you make to shortcuts are synchronized on a user's Windows client device each time the user connects to the server. Windows users can disable the shortcut synchronization feature in Horizon Client. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

For Windows users, this feature requires Horizon Client 4.6 for Windows or later on the client system. For Mac users, this feature requires Horizon Client 4.10 for Mac or later on the client system.

You can also configure a shortcut when you create or modify a global entitlement. For information about configuring global entitlements, see the *Administering Cloud Pod Architecture in Horizon 7* document.

Create Shortcuts for a Desktop Pool in Horizon Console

You can create shortcuts for an entitled desktop pool in Horizon Console so that the desktop pool appears in the Windows Start menu, on the Windows desktop, or both, on the user's Windows client device. You can specify up to four category folder levels for shortcuts. You can create shortcuts when you create a desktop pool. You can also create and modify shortcuts when you edit the desktop pool.

Prerequisites

Decide how to configure the pool settings based on the type of desktop pool that you want to create.

Procedure

1. In Horizon Console, click **Inventory > Desktops** and click **Add**.
2. In the **Add Pool** wizard, select the type of desktop pool you want to create, and click **Next**.
3. Follow the wizard prompts to the **Desktop Pool Settings** page.
4. Create shortcuts for the desktop pool.

   a. Click the Category Folder **Browse** button.

   b. Select the **Select a category folder from the folder list** option.

   c. Type a folder name in the **Select a category folder or create a new folder to place a shortcut to this pool in the client device** text box.

      A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords.

   d. Select the shortcut creation method.

      You can select one or both methods.

Option	Description
Start Menu/Launcher	Creates a Windows Start menu shortcut on the Windows client device.
Desktop	Creates a shortcut on the desktop on the Windows client device.

   e. To save your changes, click **Submit**.
5. Follow the wizard prompts to the **Ready to Complete** page and select **Entitle users after this wizard finishes** and click **Submit**.

6 In the **Add Entitlements** wizard, click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria, select the users or groups you want to entitle to the desktops in the pool and click **OK**.

   A check mark appears in the **App Shortcut** column for the desktop pool on the **Desktop Pools** page.

Create Shortcuts for an Application Pool in Horizon Console

You can create shortcuts for entitled applications in Horizon Console so that the shortcuts appear in the Windows Start menu, on the Windows desktop, or both, on the user's Windows client device. You can specify up to four category folder levels for shortcuts. You can create shortcuts when you create an application pool. You can also create shortcuts when you edit the application pool.

On Mac clients, if Horizon Client for Mac is configured to run published applications from the `Applications` folder on the local system and allow folder settings from servers, category folders appear in the `Applications` folder on the Mac client device. For more information, see the *VMware Horizon Client for Mac Installation and Setup Guide* document.

Prerequisites

- Set up RDS hosts. See "Setting Up Remote Desktop Services Hosts," in the *Setting Up Desktop and Application Pools 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.
- Install Horizon Client 4.6 for Windows or later on the client device.

Procedure

1 In Horizon Console, click **Inventory > Applications** and click **Add**.

2 Select the type of application pool you want to create.

Option	Description
Add application pool manually	Enter the information about the application. See Worksheet for Creating an Application Pool Manually in Horizon Console.
Select installed applications	Filter to find applications by name, installed path, or application type, or select from a list of installed applications. For information about configuring additional options, see Worksheet for Creating an Application Pool Manually in Horizon Console.

3 In the **Add Application Pool** wizard, select an RDS farm, enter a pool ID, and the full pathname of the application.

4 Create a shortcut for the application pool.

   a Click the Category Folder **Browse** button.

   b Select the **Select a category folder from the folder list** option.

c Select a category folder from the list, or type a folder name in the **Select a category folder or create a new folder to place a shortcut to this pool in the client device** text box.

A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords.

Note If needed, non-Windows clients can translate the backslash to a forward slash.

d Select the shortcut creation method.

You can select one or both methods.

Option	Description
Start Menu/Launcher	Creates a Windows Start menu shortcut on the Windows client device.
Desktop	Creates a shortcut on the desktop on the Windows client device.

e To save your changes, click **Submit**.

5 Select **Entitle users after this wizard finishes**.

6 In the **Add Entitlements** wizard, click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria, select the users or groups you want to entitle to the application in the pool and click **OK**.

A check mark appears in the **App Shortcut** column for the application pool on the **Application Pools** page.

Implementing Client Restrictions for Desktop and Application Pools

You can restrict access to entitled published desktop and application pools to specific client computers. To restrict access, you must add the names of the client computers that are allowed to access the published desktops or applications in an Active Directory security group and then entitle this group to a pool. The Active Directory security group can contain client computers that belong to any AD Organizational Units (OUs) or default Computer container.

The client restrictions features has certain requirements and limitations.

- You must enable the client restrictions policy when you create or modify the published desktop or application pool. By default, the client restrictions policy is disabled. For published desktop pool settings, see Worksheet for Creating Published Desktop Pools. For application pool settings, see Worksheet for Creating an Application Pool Manually in Horizon Console.
- When you create or modify entitlements for the published desktop or application pool, you must add the Active Directory security group that contains the names of the client computers that are allowed to access the published desktop or application pool.

- The client restrictions feature allows only specific client computers to access published desktop and application pools. It does not give users access to non-entitled desktop and application pools. For example, if a user is not included in an application pool entitlement (either as a user or as a member of a user group), the user cannot access the application pool, even if the user's client computer is part of the AD security group that is entitled to the application pool.
- The client restrictions feature is supported only with Windows client computers in this release. Horizon Client 4.6 for Windows or later is required on the client computers.
- When the client restrictions policy is enabled for published desktop or application pools, non-Windows clients, Windows clients running pre-4.6 versions of Horizon Client for Windows, and HTML Access clients cannot launch the desktops or applications from the restricted pools.
- The client restrictions feature only restricts new sessions from Windows clients. This feature does not restrict existing application session connections from previous user sessions.
- Horizon Client for Windows version 5.0 requires that the client computers belonging to an Active Directory security group be located in the default AD location "CN=Computers."

Getting Started with JMP Integrated Workflow

13

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

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 14

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

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.
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 **JMP Configuration**.

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 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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 **JMP Configuration**.

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 15

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

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 15 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 15 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 15 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 15 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.

Configuring Event Reporting in Horizon Console

16

You can create an event database to record information about Horizon 7 events. In addition, if you use a Syslog server, you can configure Connection Server to send events to a Syslog server or create a flat file of events written in `Syslog` format.

This chapter includes the following topics:

Add a Database and Database User for Horizon 7 Events in Horizon Console

You create an event database by adding it to an existing database server. You can then use reporting software to analyze the events in the database.

Deploy the database server for the event database on a dedicated server, so that event logging activity does not affect provisioning and other activities that are critical for Horizon 7 deployments.

Note You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server or Oracle database server on a system that a Connection Server instance has access to.

  For the most up-to-date information about supported databases, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. For **Solution/Database Interoperability**, after you select the product and version, for the Add Database step, to see a list of all supported databases, select **Any** and click **Add**.

- Verify that you have the required database privileges to create a database and user on the database server.

- If you are not familiar with the procedure to create databases on Microsoft SQL Server database servers, see "Add a View Composer Database to the SQL Server," in the *Horizon 7 Installation* document.
- If you are not familiar with the procedure to create databases on Oracle database servers, see "Add a View Composer Database to Oracle 12c or 11g," in the *Horizon 7 Installation* document.

Procedure

1 Add a database to the server and give it a descriptive name such as HorizonEvents.

  For an Oracle 12c or Oracle 11g database, also provide an Oracle System Identifier (SID), which you use when you configure the event database in Horizon Console.

2 Add a user for this database that has permission to create tables, views, and, Oracle triggers and sequences, and permission to read from and write to these objects.

  For a Microsoft SQL Server database, do not use the Integrated Windows Authentication security model method of authentication. Verify that you use the SQL Server Authentication method of authentication.

The database is created, but the schema is not installed until you configure the database in Horizon Console.

What to do next

Follow the instructions in Configure the Event Database in Horizon Console.

Prepare an SQL Server Database for Event Reporting in Horizon Console

Before you can use Horizon Console to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites

- Create an SQL Server database for event reporting. See Add a Database and Database User for Horizon 7 Events in Horizon Console.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure

1 Open SQL Server Configuration Manager and expand **SQL Server *YYYY* Network Configuration**.

2 Select **Protocols for *server_name***.

3 In the list of protocols, right-click **TCP/IP** and select **Properties.**

4 Set the **Enabled** property to **Yes.**

5 Verify that a port is assigned or, if necessary, assign one.

   For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.

6 Verify that this port is not blocked by a firewall.

What to do next

Use Horizon Console to connect the database to Connection Server. Follow the instructions in Configure the Event Database in Horizon Console.

Configure the Event Database in Horizon Console

The event database stores information about Horizon 7 events as records in a database rather than in a log file.

You configure an event database after installing a Connection Server instance. You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

Note The security of the database connection between the Connection Server instance and an external database is the responsibility of the administrator, although event traffic is limited to information about the health of the Horizon 7 environment. If you want to take extra precautions, you can secure this channel through IPSec or other means, or you can deploy the database locally on the Connection Server computer.

You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *Horizon 7 Integration* document.

You can also generate Horizon 7 events in `Syslog` format so that the event data can be accessible to third-party analytics software. You use the `vdmadmin` command with the `-I` option to record Horizon 7 event messages in `Syslog` format in event log files. See "Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option" in the *Horizon 7 Administration* document.

Prerequisites

You need the following information to configure an event database:

- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server or Oracle.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See Add a Database and Database User for Horizon 7 Events in Horizon Console.

  For an Oracle 12c or 11g database, you must use the Oracle System Identifier (SID) as the database name when you configure the event database in Horizon Console.

- The username and password of the user you created for this database. See Add a Database and Database User for Horizon 7 Events in Horizon Console.

  Use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.

- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among Horizon 7 installations.

  Note You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

Procedure

1 In Horizon Console, select **Settings > Event Configuration**.

2 In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.

  To clear the event database information, click **Clear**.

3 (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

  These settings pertain to the length of time the events are listed in the Horizon Console interface. After this time, the events are only available in the historical database tables.

4 Select **Monitoring > Events** to verify that the connection to the event database is successful.

  If the connection is unsuccessful, an error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

Configure Event Logging for Syslog Servers in Horizon Console

You can generate Horizon 7 events in `Syslog` format so that the event data can be accessible to analytics software.

You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

If you enable file-based logging of events, events are accumulated in a local log file. If you specify a file share, these log files are moved to that share.

- Use a local file only for quick troubleshooting during configuration, perhaps before the Events database is configured, so that you have some way to see events.

The maximum size of the local directory for event logs, including closed log files, before the oldest files are deleted, is 300MB. The default destination of the Syslog output is `%PROGRAMDATA%\VMware\VDM\events\`.

- Use a UNC path to save log files for a long-term record of events, of if you do not have a Syslog server, or if your current Syslog server does not meet your needs.

You can alternatively use a `vdmadmin` command to configure file-based logging of events in Syslog format. See the topic about generating Horizon 7 event log messages in Syslog format using the `–I` option of the `vdmadmin` command, in the *Horizon 7 Administration* document.

Important Syslog data is sent across the network without software-based encryption, and might contain sensitive data, such as user names. VMware recommends using link-layer security, such as IPSEC, to avoid the possibility of this data being monitored on the network.

Prerequisites

You need the following information to configure Connection Server so that events can be recorded in Syslog format or sent to a Syslog server, or both:

- If you plan to use a Syslog server to listen for the Horizon 7 events on a UDP port, you must have the DNS name or IP address of the Syslog server and the UDP port number. The default UDP port number is 514.
- If you plan to collect logs in a flat-file format, you must have the UNC path to the file share and folder in which to store the log files, and you must have the user name, domain name, and password of an account that has permission to write to the file share.

Procedure

1. In Horizon Console, select **Settings > Event Configuration**.
2. (Optional) In the **Syslog** area, to configure Connection Server to send events to a Syslog server, click **Add** below **Send to syslog servers**, and supply the server name or IP address and the UDP port number.
3. (Optional) To enable Horizon 7 event log messages to be generated and stored in Syslog format, in log files, select the **Log to file: Enable** check box.

   The log files are retained locally unless you specify a UNC path to a file share.
4. (Optional) To store the Horizon 7 event log messages on a file share, click **Add** below **Copy to location**, and supply the UNC path to the file share and folder in which to store the log files, along with the user name, domain name, and password of an account that has permission to write to the file share.

   An example of a UNC path is:

   ```
   \\syslog–server\folder\file
   ```

Monitor Events in Horizon 7

The event database stores information about events that occur in the Connection Server host or group, Horizon Agent, and Horizon Console, and notifies you of the number of events on the dashboard. You can examine the events in detail on the **Events** page.

Note Events are listed in the Horizon Console interface for a limited time period. After this time, the events are only available in the historical database tables. You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *Horizon 7 Integration* document.

Note If the event database becomes unavailable, Horizon 7 maintains the audit trail of the events that occur during this period of unavailability and saves them to event database once it becomes available. You must restart the event database and Connection Server to view these events in the Horizon Console interface.

In addition to monitoring events in Horizon Console, you can generate Horizon 7 events in `Syslog` format so that the event data can be accessible to analytics software. See Configure Event Logging for Syslog Servers in Horizon Console and "Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option," in the *Horizon 7 Installation* document.

If you configure an event database for multiple Connection Servers, Horizon Console displays the events for all Connection Servers on the **Events** page. Horizon Console filters events based on the tasks that you perform and displays these events on relevant pages such as the **Desktop Pools** or **Application Pools** pages.

Prerequisites

Create and configure the event database as described in the *Horizon 7 Installation* document.

Procedure

1 In Horizon Console, select **Monitor > Events**.

2 (Optional) On the **Events** page, you can select the time range of the events, apply filtering to the events, and sort the listed events by one or more of the columns.

What to do next

In Horizon Console, navigate to a desktop or application pool, virtual machine, persistent disk, or a user or group and click the **Events** tab to view specific events.

Horizon 7 Event Messages

Horizon 7 reports events whenever the state of the system changes or it encounters a problem. You can use the information in the event messages to take the appropriate action.

The following table shows the types of events that Horizon 7 reports.

Table 16-1. Types of Event Reported by Horizon 7

Event Type	Description
Audit Failure or Audit Success	Reports the failure or success of a change that an administrator or user makes to the operation or configuration of Horizon 7.
Error	Reports a failed operation by Horizon 7.
Information	Reports normal operations within Horizon 7.
Warning	Reports minor problems with operations or configuration settings that might lead to more serious problems over time.

You might need to take some action if you see messages that are associated with Audit Failure, Error, or Warning events. You do not need to take any action for Audit Success or Information events.

Using Horizon Help Desk Tool in Horizon Console

17

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

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 17-1. 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 17-2. 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.

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 17-3. 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 17-4. 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 17-5. 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.

Option	Description
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 17-6. 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.
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 17-7. 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 17-8. 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 17-9. 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 17-10. 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 17-11. 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 17-12. 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 17-13. 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 17-14. 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.