Horizon 7 Administration

May 29 2018
VMware Horizon 7 7.5

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Horizon 7 Administration

Horizon 7 Administration describes how to configure and administer VMware Horizon® 7, including how to configure Horizon Connection Server, create administrators, set up user authentication, configure policies, and manage VMware ThinApp® applications in Horizon Administrator. This document also describes how to maintain and troubleshoot Horizon 7 components.

Intended Audience

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

Using Horizon Administrator

1

Horizon Administrator is the Web interface through which you configure Horizon Connection Server and manage your remote desktops and applications.

For a comparison of the operations that you can perform with Horizon Administrator, cmdlets, and `vdmadmin`, see the *Horizon 7 Integration* document.

This chapter includes the following topics:

Horizon Administrator and Horizon Connection Server

Horizon Administrator provides a Web-based management interface for Horizon 7.

The Horizon Connection Server can have multiple instances that serve as replica servers or security servers. Depending on your Horizon 7 deployment, you can get a Horizon Administrator interface with each instance of a Connection Server.

Use the following best practices to use Horizon Administrator with a Connection Server:

- Use the host name and IP address of the Connection Server to log in to Horizon Administrator. Use the Horizon Administrator interface to manage the Connection Server, and any associated security server or replica server.
- In a pod environment, verify that all administrators use the host name and IP address of the same Connection Server to log in to Horizon Administrator. Do not use the host name and IP address of the load balancer to access a Horizon Administrator web page.

Note If you use Unified Access Gateway appliances rather than security servers, you must use the Unified Access Gateway REST API to manage the Unified Access Gateway appliances. Earlier versions of Unified Access Gateway are named Access Point. For more information, see *Deploying and Configuring Unified Access Gateway*.

Log In to Horizon Administrator

To perform initial configuration tasks, you must log in to Horizon Administrator. You access Horizon Administrator by using a secure (TLS) connection.

Prerequisites

- Verify that Horizon Connection Server is installed on a dedicated computer.
- Verify that you are using a Web browser supported by Horizon Administrator. For Horizon Administrator requirements, see the *Horizon 7 Installation* document.

Procedure

1 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 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.

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 View Connection Server.	When you first connect, your Web browser displays Horizon Administrator.
The default, self-signed certificate supplied with View 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 using an account that has the Administrators role.

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.

After you log in to Horizon Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the Administrators role.

Tips for Using the Horizon Administrator Interface

You can use Horizon Administrator user-interface features to navigate Horizon Pages and to find, filter, and sort Horizon objects.

Horizon Administrator includes many common user interface features. For example, the navigation pane on the left side of each page directs you to other Horizon Administrator pages. The search filters let you select filtering criteria that are related to the objects you are searching for.

The following table describes a few additional features that can help you to use Horizon Administrator.

Table 1-1. Horizon Administrator Navigation and Display Features

Horizon Administrator Feature	Description
Navigating backward and forward in Horizon Administrator pages	Click your browser's **Back** button to go to the previously displayed Horizon Administrator page. Click the **Forward** button to return to the current page. If you click the browser's **Back** button while you are using a Horizon Administrator wizard or dialog box, you return to the main Horizon Administrator page. The information you entered in the wizard or dialog is lost. In versions earlier than View 5.1, you cannot use your browser's **Back** and **Forward** buttons to navigate within Horizon Administrator. Separate **Back** and **Forward** buttons in the Horizon Administrator window were provided for navigation. These buttons are removed in the View 5.1 release.
Bookmarking Horizon Administrator pages	You can bookmark Horizon Administrator pages in your browser.
Multicolumn sorting	You can sort Horizon objects in a variety of ways by using multicolumn sorting. Click a heading in the top row of a Horizon Administrator table to sort the Horizon objects in alphabetical order based on that heading. For example, in the **Resources > Machines** page, you can click **Desktop Pool** to sort desktops by the pools that contain them. The number **1** appears next to the heading to indicate that it is the primary sorting column. You can click the heading again to reverse the sorting order, indicated by an up or down arrow. To sort the Horizon objects by a secondary item, Ctrl+click another heading. For example, in the Machines table, you can click **Users** to perform a secondary sort by users to whom the desktops are dedicated. A number **2** appears next to the secondary heading. In this example, desktops are sorted by pool and by users within each pool. You can continue to Ctrl+click to sort all the columns in a table in descending order of importance. Press Ctrl+Shift and click to deselect a sort item. For example, you might want to display the desktops in a pool that are in a particular state and are stored on a particular datastore. You can select **Resources > Machines**, click the **Datastore** heading, and Ctrl+click the **Status** heading.

Table 1-1. Horizon Administrator Navigation and Display Features (Continued)

Horizon Administrator Feature	Description
Customizing table columns	You can customize the display of Horizon Administrator table columns by hiding selected columns and locking the first column. This feature lets you control the display of large tables such as **Catalog > Desktop Pools** that contain many columns. Right-click any column header to display a context menu that lets you take the following actions: ■ Hide the selected column. ■ Customize columns. A dialog displays all columns in the table. You can select the columns to display or hide. ■ Lock the first column. This option forces the left-hand column to remain displayed as you scroll horizontally across a table with many columns. For example, on the **Catalog > Desktop Pools** page, the desktop ID remains displayed as you scroll horizontally to see other desktop characteristics.
Selecting Horizon objects and displaying Horizon object details	In Horizon Administrator tables that list Horizon objects, you can select an object or display object details. ■ To select an object, click anywhere in the object's row in the table. At the top of the page, menus and commands that manage the object become active. ■ To display object details, double-click the left cell in the object's row. A new page displays the object's details. For example, on the **Catalog > Desktop Pools** page, click anywhere in an individual pool's row to activate commands that affect the pool. Double-click the **ID** cell in the left column to display a new page that contains details about the pool.
Expanding dialog boxes to view details	You can expand Horizon Administrator dialog boxes to view details such as desktop names and user names in table columns. To expand a dialog box, place your mouse over the dots in the lower right corner of the dialog box and drag the corner.
Displaying context menus for Horizon objects	You can right-click Horizon objects in Horizon Administrator tables to display context menus. A context menu gives you access to the commands that operate on the selected Horizon object. For example, in the **Catalog > Desktop Pools** page, you can right-click a desktop pool to display commands such as **Add**, **Edit**, **Delete**, **Disable (or Enable) Provisioning**, and so on.

Troubleshooting the Text Display in Horizon Administrator

If your Web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac OS, the text in Horizon Administrator does not display properly.

Problem

The text in the Horizon Administrator interface is garbled. For example, spaces occur in the middle of words.

Cause

Horizon Administrator requires Microsoft-specific fonts.

Solution

Install Microsoft-specific fonts on your computer.

Currently, the Microsoft Web site does not distribute Microsoft fonts, but you can download them from independent Web sites.

Configuring Horizon Connection Server 2

After you install and perform initial configuration of Horizon Connection Server, you can add vCenter Server instances and View 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 View Composer

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

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 View Storage Accelerator for vCenter Server.

Create a User Account for View Composer AD Operations

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

To ensure security, you should create a separate user account to use with View 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 View 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 Administrator when you configure View Composer domains in the Add vCenter Server wizard and when you configure and deploy linked-clone desktop pools.

Add vCenter Server Instances to Horizon 7

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 (SSL).

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 View 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/SSL 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 View Composer. See Concurrent Operations Limits for vCenter Server and View Composer and Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. On the **vCenter Servers** 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 Under Advanced Settings, set the concurrent operations limits for vCenter Server and View Composer operations.

9 Click **Next** to display the View Composer Settings page.

What to do next

Configure View Composer settings.

- If the vCenter Server instance is configured with a signed SSL certificate, and Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View 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 View Composer Settings

To use View Composer, you must configure settings that allow Horizon 7 to connect to the VMware Horizon View Composer service. View 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 VMware Horizon View Composer service and vCenter Server instance. A View Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one VMware Horizon View Composer service.

After the initial Horizon 7 deployment, you can migrate the VMware Horizon View Composer service to a new host to support a growing or changing Horizon 7 deployment. You can edit the initial View Composer settings in Horizon Administrator, but you must perform additional steps to ensure that the migration succeeds. See Migrate View Composer to Another Machine.

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

Procedure

1. In Horizon Administrator, complete the vCenter Server Information page in the Add vCenter Server wizard.
   a. Select **View Configuration > Servers**.
   b. On the **vCenter Servers** tab, click **Add** and provide the vCenter Server settings.
2. On the View Composer Settings page, if you are not using View Composer, select **Do not use View Composer**.

   If you select **Do not use View Composer**, the other View Composer settings become inactive. When you click **Next**, the Add vCenter Server wizard displays the Storage Settings page. The View Composer Domains page is not displayed.
3. If you are using View Composer, select the location of the View Composer host.

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

4 Click **Next** to display the View Composer Domains page.

What to do next

Configure View Composer domains.

- If the View Composer instance is configured with a signed TLS certificate, and Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Domains page.
- If the View Composer 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.

Configure View Composer Domains

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

Prerequisites

- Your Active Directory administrator must create a View 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 View Composer AD Operations.
- In Horizon Administrator, verify that you completed the vCenter Server Information and View Composer Settings pages in the Add vCenter Server wizard.

Procedure

1 On the View Composer Domains page, click **Add** to add the View Composer user for AD operations account information.

2 Type the domain name of the Active Directory domain.

For example: **`domain.com`**

3 Type the domain user name, including the domain name, of the View Composer user.

For example: **`domain.com\admin`**

4 Type the account password.

5 Click **OK**.

6 To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.

7 Click **Next** to display the Storage Settings page.

What to do next

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

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

In vSphere 5.1 and later, you can enable the disk space reclamation feature for Horizon 7. Starting in vSphere 5.1, 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 5.1 or later environment, 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 Administrator 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 View Composer persistent disks.
- It works only with vSphere 5.1 or later and only 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 Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
   a. Select **View Configuration > Servers**.
   b. On the **vCenter Servers** tab, click **Add**.
   c. Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.
2. On the Storage Settings page, make sure that **Enable space reclamation** is selected.

   Space reclamation is selected by default if you are performing a fresh installation of Horizon 7 5.2 or later. You must select **Enable space reclamation** if you are upgrading to Horizon 7 5.2 or later from Horizon 7 5.1 or an earlier release.

What to do next

On the Storage Settings page, configure View Storage Accelerator.

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

Configure View Storage Accelerator for vCenter Server

In vSphere 5.1 and later, you can configure ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View 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, View 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 View Storage Accelerator setting in the vCenter Server wizard in Horizon Administrator, as described in this procedure.

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

View 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 View 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 View Storage Accelerator.

View 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 View 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 View pods that share some ESXi hosts, you must enable the View 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 View Composer privileges required for the vCenter Server user.

Procedure

1. In Horizon Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
   a. Select **View Configuration > Servers**.
   b. On the **vCenter Servers** tab, click **Add**.
   c. Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.
2. On the Storage Settings page, make sure that the **Enable View Storage Accelerator** check box is selected.

   This check box is selected by default.
3. 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.
4. 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**.

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

6 Click **Finish** to add vCenter Server, View Composer, and Storage Settings to Horizon 7.

What to do next

Configure settings for client sessions and connections. See Configuring Settings for Client Sessions.

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

Concurrent Operations Limits for vCenter Server and View 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 View Composer.

You configure these options in the Advanced Settings panel on the vCenter Server Information page.

Table 2-1. Concurrent Operations Limits for vCenter Server and View 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.
Max concurrent View Composer maintenance operations	Determines the maximum number of concurrent View Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this View 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 View Composer provisioning operations	Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this View Composer instance. The default value is 8. This setting applies to linked 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 View Composer instances to Horizon 7, you must ensure that the TLS certificates that are used for the vCenter Server and View Composer instances are valid and trusted by Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View 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 View 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 View Servers" in the *Horizon 7 Installation* document.

You first add vCenter Server and View Composer in Horizon Administrator 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 View Composer.

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 View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the Horizon Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. In Horizon Administrator, click **View Configuration > Servers** and edit the vCenter Server entry associated with the View Composer Service. Then, click **Edit** in the vCenter Server settings and follow the prompts to verify the and accept the self-signed certificate.

Similarly, in Horizon Administrator you can configure a SAML authenticator for use by a Connection Server instance. If the SAML server certificate is not trusted by Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML authenticator in Horizon 7. After a SAML authenticator is configured, you can reconfigure it in the Edit Connection Server dialog box.

Procedure

1. When Horizon Administrator 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 View Composer instance.
   a. On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.
   b. Navigate to the vCenter Server or View 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 View 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 View 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 Administrator, click **View Configuration > Servers**.

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

3 Click **Remove**.

   A dialog 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 View Composer from Horizon 7

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

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

Procedure

1 Remove the linked-clone desktop pools that were created by View Composer.

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

   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 View Composer database entries and the replicas that were created by View Composer are removed.

   d Repeat these steps for each linked-clone desktop pool that was created by View Composer.

2 Select **View Configuration > Servers**.

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

4 Click **Edit**.

5 Under View Composer Server Settings, click **Edit**, select **Do not use View 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 View Composer on another host and reconfigure Horizon 7 to connect to the new VMware Horizon View Composer service, you must perform certain additional steps. See Migrate View Composer Without Linked-Clone Virtual Machines.

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

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

For information about backing up and restoring your Horizon 7 configuration, see Backing Up and Restoring Horizon 7 Configuration Data.

Configuring Settings for Client Sessions

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.

Set Options for Client Sessions and Connections

You configure global settings to determine the way client sessions and connections work.

The global settings are not specific to a single Connection Server instance. They affect all client sessions that are managed by a standalone Connection Server instance or a group of replicated instances.

You can also configure Connection Server instances to use direct, nontunneled connections between Horizon clients and remote desktops. See Configure the Secure Tunnel and PCoIP Secure Gateway for information about configuring direct connections.

Prerequisites

Familiarize yourself with the global settings. See Global Settings for Client Sessions and Global Security Settings for Client Sessions and Connections.

Procedure

1 In Horizon Administrator, select **View Configuration > Global Settings**.

2 Choose whether to configure general settings or security settings.

Option	Description
General global settings	In the General pane, click **Edit**.
Global security settings	In the Security pane, click **Edit**.

3 Configure the global settings.

4 Click **OK**.

What to do next

You can change the data recovery password that was provided during installation. See Change the Data Recovery Password.

Change the Data Recovery Password

You provide a data recovery password when you install Connection Server version 5.1 or later. After installation, you can change this password in View Administrator. The password is required when you restore the View LDAP configuration from a backup.

When you back up Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup Horizon 7 configuration, you must provide the data recovery password.

The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.

Procedure

1 In Horizon Administrator, select **View Configuration > Global Settings**.

2 In the Security pane, click **Change data recovery password**.

3 Type and retype the new password.

4 (Optional) Type a password reminder.

Note You can also change the data recovery password when you schedule your Horizon 7 configuration data to be backed up. See Schedule Horizon 7 Configuration Backups.

What to do next

When you use the `vdmimport` utility to restore a backup Horizon 7 configuration, provide the new password.

Global Settings for Client Sessions

General global settings determine session timeout lengths, SSO enablement and timeout limits, status updates in Horizon Administrator, whether prelogin and warning messages are displayed, whether Horizon Administrator 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 2-2. General Global Settings for Client Sessions

Setting	Description
View Administrator session timeout	Determines how long an idle Horizon Administrator session continues before the session times out. **Important** Setting the Horizon Administrator session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Administrator. Use caution when you allow an idle session to persist a long time. By default, the Horizon Administrator 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.
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**.

Table 2-2. General Global Settings for Client Sessions (Continued)

Setting	Description
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**.
Enable automatic status updates	Determines if status updates appear in the global status pane in the upper-left corner of Horizon Administrator every few minutes. The dashboard page of Horizon Administrator is also updated every few minutes. By default, this setting is not enabled.
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 Administrator 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.

Table 2-2. General Global Settings for Client Sessions (Continued)

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.
Mirage Server configuration	Allows you to specify the URL of a Mirage server, using the format `mirage://server-name:port` or `mirages://server-name:port`. Here *server-name* is the fully qualified domain name. If you do not specify the port number, the default port number 8000 is used. **Note** You can override this global setting by specifying a Mirage server in the desktop pool settings. Specifying the Mirage server in Horizon Administrator is an alternative to specifying the Mirage server when installing the Mirage client. To find out which versions of Mirage support having the server specified in Horizon Administrator, see the Mirage documentation, at https://www.vmware.com/support/pubs/mirage_pubs.html.
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 server information in client user interface** and **Hide domain list in client user interface** settings 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. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.

Global Security Settings for Client Sessions and Connections

Global security settings determine whether clients are reauthenticated after interruptions, message security mode is enabled, and IPSec is used for security server connections.

TLS is required for all Horizon Client connections and Horizon Administrator 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. See Off-load TLS Connections to Intermediate Servers.

Table 2-3. 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 details, see Message Security Mode for Horizon 7 Components. 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.

Table 2-3. Global Security Settings for Client Sessions and Connections (Continued)

Setting	Description
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. You can also use the `vdmutil` command-line utility to monitor progress. See Using the vdmutil Utility to Configure the JMS Message Security Mode.
Use IPSec for Security Server connections	Determines whether to use Internet Protocol Security (IPSec) for connections between security servers and Connection Server instances. By default, secure connections (using IPSec) for security server connections is enabled.

Note If you upgrade to View 5.1 or later from an earlier Horizon 7 release, the global setting **Require SSL for client connections** is displayed in Horizon Administrator, but only if the setting was disabled in your Horizon 7 configuration before you upgraded. Because TLS is required for all Horizon Client connections and Horizon Administrator connections to Horizon 7, this setting is not displayed in fresh installations of Horizon 7 5.1 or later versions and is not displayed after an upgrade if the setting was already enabled in the previous Horizon 7 configuration.

After an upgrade, if you do not enable the **Require SSL for client connections** setting, HTTPS connections from Horizon clients will fail, unless they connect to an intermediate device that is configured to make onward connections using HTTP. See Off-load TLS Connections to Intermediate Servers.

Message Security Mode for Horizon 7 Components

You can set the message security mode to specify the security mechanism used when JMS messages pass among Horizon 7 components.

The following table shows the options you can select to configure the message security mode. To set an option, select it from the **Message security mode** list in the Global Settings dialog window.

Table 2-4. Message Security Mode Options

Option	Description
Disabled	Message security mode is disabled.
Mixed	Message security mode is enabled but not enforced. You can use this mode to detect components in your Horizon 7 environment that predate Horizon 7 3.0. The log files generated by Connection Server contain references to these components. This setting is not recommended. Use this setting only to discover components that need to be upgraded.

Table 2-4. Message Security Mode Options (Continued)

Option	Description
Enabled	Message security mode is enabled, using a combination of message signing and encryption. JMS messages are rejected if the signature is missing or invalid, or if a message was modified after it was signed. Some JMS messages are encrypted because they carry sensitive information such as user credentials. If you use the **Enabled** setting, you can also use IPSec to encrypt all JMS messages between Connection Server instances, and between Connection Server instances and security servers. **Note** Horizon 7 components that predate version 3.0 are not allowed to communicate with other Horizon 7 components.
Enhanced	SSL is used for all JMS connections. JMS access control is also enabled so that desktops, security servers, and Connection Server instances can only send and receive JMS messages on certain topics. Horizon 7 components that predate Horizon 6 version 6.1 cannot communicate with a Connection Server 6.1 instance. **Note** Using this mode requires opening TCP port 4002 between DMZ-based security servers and their paired Connection Server instances.

When you first install Horizon 7 on a system, the message security mode is set to **Enhanced**. If you upgrade Horizon 7 from a previous release, the message security mode remains unchanged from its existing setting.

Important If you plan to change an upgraded Horizon 7 environment from **Enabled** to **Enhanced**, you must first upgrade all Connection Server instances, security servers, and Horizon 7 desktops to Horizon 6 version 6.1 or a later release. After you change the setting to **Enhanced**, the new setting takes place in stages.

1 You must manually restart the VMware Horizon View Message Bus Component service on all Connection Server hosts in the pod, or restart the Connection Server instances.

2 After the services are restarted, the Connection Server instances reconfigure the message security mode on all desktops and security servers, changing the mode to **Enhanced**.

3 To monitor the progress in Horizon Administrator, go to **View Configuration > Global Settings**.

   On the **Security** tab, the **Enhanced Security Status** item will show **Enhanced** when all components have made the transition to Enhanced mode.

   Alternatively, you can use the `vdmutil` command-line utility to monitor progress. See Using the vdmutil Utility to Configure the JMS Message Security Mode.

Horizon 7 components that predate Horizon 6 version 6.1 cannot communicate with a Connection Server 6.1 instance that uses Enhanced mode.

If you plan to change an active Horizon 7 environment from **Disabled** to **Enabled**, or from **Enabled** to **Disabled**, change to **Mixed** mode for a short time before you make the final change. For example, if your current mode is **Disabled**, change to **Mixed** mode for one day, then change to **Enabled**. In **Mixed** mode, signatures are attached to messages but not verified, which allows the change of message mode to propagate through the environment.

Using the vdmutil Utility to Configure the JMS Message Security Mode

You can use the `vdmutil` command-line interface to configure and manage the security mechanism used when JMS messages are passed between Horizon 7 components.

Syntax and Location of the Utility

The `vdmutil` command can perform the same operations as the `lmvutil` command that was included with earlier versions of Horizon 7. In addition, the `vdmutil` command has options for determining the message security mode being used and monitoring the progress of changing all Horizon 7 components to Enhanced mode. Use the following form of the `vdmutil` command from a Windows command prompt.

```
vdmutil command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option. This topic focuses on the options for message security mode. For the other options, which relate to Cloud Pod Architecture, see the *Administering Cloud Pod Architecture in Horizon 7* document.

By default, the path to the `vdmutil` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid entering the path on the command line, add the path to your PATH environment variable.

Authentication

You must run the command as a user who has the Administrators role. You can use Horizon Administrator to assign the Administrators role to a user. See Chapter 6 Configuring Role-Based Delegated Administration.

The `vdmutil` command includes options to specify the user name, domain, and password to use for authentication.

Table 2-5. vdmutil Command Authentication Options

Option	Description
`--authAs`	Name of a Horizon 7 administrator user. Do not use *domain\username* or user principal name (UPN) format.
`--authDomain`	Fully qualified domain name for the Horizon 7 administrator user specified in the `--authAs` option.
`--authPassword`	Password for the Horizon 7 administrator user specified in the `--authAs` option. Entering **"*"** instead of a password causes the `vdmutil` command to prompt for the password and does not leave sensitive passwords in the command history on the command line.

You must use the authentication options with all `vdmutil` command options except for `--help` and `--verbose`.

Options Specific to JMS Message Security Mode

The following table lists only the `vdmutil` command-line options that pertain to viewing, setting, or monitoring the JMS message security mode. For a list of the arguments you can use with a specific option, use the `--help` command-line option.

The `vdmutil` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails. The `vdmutil` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `vdmutil` command writes output to standard output, in US English.

Table 2-6. vdmutil Command Options

Option	Description
`--activatePendingConnectionServerCertificates`	Activates a pending security certificate for a Connection Server instance in the local pod.
`--countPendingMsgSecStatus`	Counts the number of machines preventing a transition to or from Enhanced mode.
`--createPendingConnectionServerCertificates`	Creates a new pending security certificate for a Connection Server instance in the local pod.
`--getMsgSecLevel`	Gets the enhanced message security status for the local pod. This status pertains to the process of changing the JMS message security mode from **Enabled** to **Enhanced** for all the components in an Horizon 7 environment.
`--getMsgSecMode`	Gets the message security mode for the local pod.
`--help`	Lists the `vdmutil` command options. You can also use `--help` on a particular command, such as `--setMsgSecMode --help`.
`--listMsgBusSecStatus`	Lists the message bus security status for all connection servers in the local pod.
`--listPendingMsgSecStatus`	List machines preventing a transition to or from Enhanced mode. Limited to 25 entries by default.
`--setMsgSecMode`	Sets the message security mode for the local pod.
`--verbose`	Enables verbose logging. You can add this option to any other option to obtain detailed command output. The `vdmutil` command writes to standard output.

Configure the Secure Tunnel and PCoIP Secure Gateway

When the secure tunnel is enabled, Horizon Client makes a second HTTPS connection to the View Connection Server or security server host when users connect to a remote desktop.

When the PCoIP Secure Gateway is enabled, Horizon Client makes a further secure connection to the Connection Server or security server host when users connect to a remote desktop with the PCoIP display protocol.

Note With Horizon 6 version 6.2 and later releases, you can use Unified Access Gateway appliances, rather than security servers, for secure external access to Horizon 6 servers and desktops. If you use Unified Access Gateway appliances, you must disable the secure gateways on Connection Server instances and enable these gateways on the Unified Access Gateway appliances. For more information, see *Deploying and Configuring Unified Access Gateway*.

When the secure tunnel or PCoIP Secure Gateway is not enabled, a session is established directly between the client system and the remote desktop virtual machine, bypassing the Connection Server or security server host. This type of connection is called a direct connection.

Important A typical network configuration that provides secure connections for external clients includes a security server. To use Horizon Administrator or to enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that Connection Server instance in Horizon Administrator.

Prerequisites

- If you intend to enable the PCoIP Secure Gateway, verify that the Connection Server instance and paired security server are Horizon 7 4.6 or later.
- If you pair a security server to a Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is Horizon 7 4.6 or later.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.
3. Configure use of the secure tunnel.

Option	Description
Enable the secure tunnel	Select **Use Secure Tunnel connection to machine**.
Disable the secure tunnel	Deselect **Use Secure Tunnel connection to machine**.

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

Option	Description
Enable the PCoIP Secure Gateway	Select **Use PCoIP Secure Gateway for PCoIP connections to machine**
Disable the PCoIP secure Gateway	Deselect **Use PCoIP Secure Gateway for PCoIP connections to machine**

The PCoIP Secure Gateway is disabled by default.

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

Configure the Blast Secure Gateway

In Horizon Administrator, you can configure the use of the Blast Secure Gateway to provide secure access to remote desktops and applications, either through HTML Access or through client connections that use the VMware Blast display protocol.

The Blast Secure Gateway includes Blast Extreme Adaptive Transport (BEAT) networking, which dynamically adjusts to network conditions such as varying speeds and packet loss.

- Horizon Clients can use BEAT networking with an excellent network condition while connecting to the Connection Server, security server, or Unified Access Gateway appliance.
- Horizon Clients that use a typical network condition must connect to a Connection Server (BSG disabled), security server (BSG disabled), or versions later than 2.8 of an Unified Access Gateway appliance. If Horizon Client uses a typical network condition to connect to a Connection Server (BSG enabled), security server (BSG enabled), or versions earlier than 2.8 of an Unified Access Gateway appliance, the client automatically senses the network condition and falls back to TCP networking.
- Horizon Clients that use a poor network condition must connect to version 2.9 or later of an Unified Access Gateway appliance (with UDP Tunnel Server Enabled). If Horizon Client uses a poor network condition to connect to the Connection Server (BSG enabled), security server (BSG enabled), or versions earlier than 2.8 of an Unified Access Gateway appliance, the client automatically senses the network condition and falls back to TCP networking.
- Horizon Clients that use a poor network condition to connect to Connection Server (BSG disabled), security server (BSG disabled), or version 2.9 or later of Unified Access Gateway appliance (without UDP Tunnel Server Enabled), or version 2.8 of Unified Access Gateway appliance, the client automatically senses the network condition and falls back to the typical network condition.

For more information, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Note You can also use Unified Access Gateway appliances, rather than security servers, for secure external access to Horizon 7 servers and desktops. If you use Unified Access Gateway appliances, you must disable the secure gateways on Connection Server instances and enable these gateways on the Unified Access Gateway appliances. For more information, see *Deploying and Configuring Unified Access Gateway*.

When the Blast Secure Gateway is not enabled, client devices and client Web browsers use the VMware Blast Extreme protocol to establish direct connections to remote desktop virtual machines and applications, bypassing the Blast Secure Gateway.

Important A typical network configuration that provides secure connections for external users includes a security server. To enable or disable the Blast Secure Gateway on a security server, you must edit the Connection Server instance that is paired with the security server. If external users connect directly to a Connection Server host, you enable or disable the Blast Secure Gateway by editing that Connection Server instance.

Prerequisites

If users select remote desktops by using VMware Identity Manager, verify that VMware Identity Manager is installed and configured for use with Connection Server and that Connection Server is paired with a SAML 2.0 Authentication server.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.
3. Configure use of the Blast Secure Gateway.

Option	Description
Enable the Blast Secure Gateway	Select **Use Blast Secure Gateway for Blast connections to machine**
Disable the Blast secure Gateway	Deselect **Use Blast Secure Gateway for Blast connections to machine**

   The Blast Secure Gateway is enabled by default.

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

Off-load TLS Connections to Intermediate Servers

Horizon Client must use HTTPS to connect to Horizon 7. If your Horizon clients connect to load balancers or other intermediate servers that pass on the connections to Connection Server instances or security servers, you can off-load TLS to the intermediate servers.

Import TLS Off-loading Servers' Certificates to Horizon 7 Servers

If you off-load TLS connections to an intermediate server, you must import the intermediate server's certificate onto the Connection Server instances or security servers that connect to the intermediate server. The same TLS server certificate must reside on both the off-loading intermediate server and each off-loaded Horizon 7 server that connects to the intermediate server.

If you deploy security servers, the intermediate server and the security servers that connect to it must have the same TLS certificate. You do not have to install the same TLS certificate on Connection Server instances that are paired to the security servers and do not connect directly to the intermediate server.

If you do not deploy security servers, or if you have a mixed network environment with some security servers and some external-facing Connection Server instances, the intermediate server and any Connection Server instances that connect to it must have the same TLS certificate.

If the intermediate server's certificate is not installed on the Connection Server instance or security server, clients cannot validate their connections to Horizon 7. In this situation, the certificate thumbprint sent by the Horizon 7 server does not match the certificate on the intermediate server to which Horizon Client connects.

Do not confuse load balancing with TLS off-loading. The preceding requirement applies to any device that is configured to provide TLS off-loading, including some types of load balancers. However, pure load balancing does not require copying of certificates between devices.

For information about importing certificates to Horizon 7 servers, see "Import a Signed Server Certificate into a Windows Certificate Store" in the *Horizon 7 Installation* document.

Set Horizon 7 Server External URLs to Point Clients to TLS Off-loading Servers

If TLS is off-loaded to an intermediate server and Horizon Client devices use the secure tunnel to connect to Horizon 7, you must set the secure tunnel external URL to an address that clients can use to access the intermediate server.

You configure the external URL settings on the Connection Server instance or security server that connects to the intermediate server.

If you deploy security servers, external URLs are required for the security servers but not for the Connection Server instances that are paired with the security servers.

If you do not deploy security servers, or if you have a mixed network environment with some security servers and some external-facing Connection Server instances, External URLs are required for any Connection Server instances that connect to the intermediate server.

Note You cannot off-load TLS connections from a PCoIP Secure Gateway (PSG) or Blast Secure Gateway. The PCoIP external URL and Blast Secure Gateway external URL must allow clients to connect to the computer that hosts the PSG and Blast Secure Gateway. Do not reset the PCoIP external URL and Blast external URL to point to the intermediate server unless you plan to require TLS connections between the intermediate server and the Horizon 7 server.

For information about configuring External URLs, see “Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections” in the *Horizon 7 Installation* document.

Allow HTTP Connections From Intermediate Servers

When TLS is off-loaded to an intermediate server, you can configure Connection Server instances or security servers to allow HTTP connections from the client-facing, intermediate devices. The intermediate devices must accept HTTPS for Horizon Client connections.

To allow HTTP connections between Horizon 7 servers and intermediate devices, you must configure the `locked.properties` file on each Connection Server instance and security server on which HTTP connections are allowed.

Even when HTTP connections between Horizon 7 servers and intermediate devices are allowed, you cannot disable TLS in Horizon 7. Horizon 7 servers continue to accept HTTPS connections as well as HTTP connections.

Note If your Horizon clients use smart card authentication, the clients must make HTTPS connections directly to Connection Server or security server. TLS off-loading is not supported with smart card authentication.

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. To configure the Horizon 7 server's protocol, add the `serverProtocol` property and set it to `http`.

   The value `http` must be typed in lower case.

3. (Optional) Add properties to configure a non-default HTTP listening port and a network interface on the Horizon 7 server.

   - To change the HTTP listening port from 80, set `serverPortNonTLS` to another port number to which the intermediate device is configured to connect.
   - If the Horizon 7 server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set `serverHostNonTLS` to the IP address of that network interface.

4. Save the `locked.properties` file.

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

Example: locked.properties file

This file allows non-TLS HTTP connections to a Horizon 7 server. The IP address of the Horizon 7 server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value `http` must be lower case.

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```

Configure the Gateway Location for a Horizon Connection Server or Security Server Host

By default, Horizon Connection Server instances set the gateway location to `Internal` and security servers set the gateway location to `External`. You can change the default gateway location by setting the `gatewayLocation` property in the `locked.properties` file.

The gateway location determines the value of the `ViewClient_Broker_GatewayLocation` registry key in a remote desktop. You can use this value with Smart Policies to create a policy that takes effect only if a user connects to a remote desktop from inside or outside your corporate network. For more information, see "Using Smart Policies" in the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

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

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

   The properties in the `locked.properties` file are case sensitive.

2. Add the following line to the `locked.properties` file:

   `gatewayLocation=`*`value`*

   value can be either `External` or `Internal`. `External` indicates that the gateway is available for users outside the corporate network. `Internal` indicates that the gateway is available only for users inside the corporate network.

   For example: `gatewayLocation=External`

3. Save the `locked.properties` file.

4. Restart the VMware Horizon Connection Server service or the VMware Horizon Security Server service to make your changes take effect.

Disable or Enable Horizon Connection Server

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 Administrator, select **View Configuration > 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

You can use Horizon Administrator to edit external URLs for Connection Server instances and security servers.

By default, a Connection Server or security 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 or security 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 or security 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 or security 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.

Note You cannot edit the external URLs for a security server that has not been upgraded to Connection Server 4.5 or later.

Procedure

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

Option	Action
View Connection Server instance	Select the Connection Server instance on the **Connection Servers** tab and click **Edit**.
Security server	Select the security server on the **Security Servers** tab and click **Edit**.

2 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://view.example.com:443

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

3 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 security server or Connection Server instance.

4 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.

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

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

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

Join or Withdraw from the Customer Experience Program

When you install Connection Server with a new configuration, you can choose to participate in a customer experience improvement program. If you change your mind about participating after the installation, you can join or withdraw from the program by using Horizon Administrator.

If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected.

To review the list of fields from which data is collected, including the fields that are made anonymous, see GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54#GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54.

Procedure

1 In Horizon Administrator, select **View Configuration > Product Licensing and Usage**.

2 In the Customer Experience Program pane, click **Edit Settings**.

3 Decide whether to participate in or withdraw from the program by selecting or deselecting the **Send anonymous data to VMware** checkbox.

4 (Optional) If you participate, you can select the geographic location, type of business, and number of employees in your organization.

5 Click **OK**.

View LDAP Directory

View LDAP is the data repository for all Horizon 7 configuration information. View LDAP is an embedded Lightweight Directory Access Protocol (LDAP) directory that is provided with the Connection Server installation.

View LDAP contains standard LDAP directory components that are used by Horizon 7.

- Horizon 7 schema definitions
- Directory information tree (DIT) definitions
- Access control lists (ACLs)

View LDAP contains directory entries that represent Horizon 7 objects.

- Remote desktop entries that represent each accessible desktop. Each entry contains references to the Foreign Security Principal (FSP) entries of Windows users and groups in Active Directory who are authorized to use the desktop.
- Remote desktop pool entries that represent multiple desktops managed together
- Virtual machine entries that represent the vCenter Server virtual machine for each remote desktop
- Horizon 7 component entries that store configuration settings

View LDAP also contains a set of Horizon 7 plug-in DLLs that provide automation and notification services for other Horizon 7 components.

Note Security server instances do not contain a View LDAP directory.

LDAP Replication

When you install a replicated instance of Connection Server, Horizon 7 copies the View LDAP configuration data from the existing Connection Server instance. Identical View LDAP configuration data is maintained on all Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage. With Horizon 7 and later releases, a replication status check is performed every 15 minutes to determine whether each instance can communicate with the other servers in the replicated group and whether each instance can fetch LDAP updates from the other servers in the group.

You can use the dashboard in Horizon Administrator to check the replication status. If any Connection Server instances have a red icon in the dashboard, click the icon to see the replication status. Replication might be impaired for any of the following reasons:

- A firewall might be blocking communication
- The VMware VDMDS service might be stopped on a Connection Server instance
- The VMware VDMDS DSA options might be blocking the replications
- A network problem has occurred

By default, the replication check occurs every 15 minutes. You can use ADSI Edit on a Connection Server instance to change the interval. To set the number of minutes, connect to **DC=vdi,DC=vmware,DC=int** and edit the **pae-ReplicationStatusDataExpiryInMins** attribute on the **CN=Common,OU=Global,OU=Properties** object.

The **pae-ReplicationStatusDataExpiryInMins** attribute value should be between 10 minutes and 1440 minutes (one day). If the attribute value is less than 10 minutes, Horizon 7 treats it as 10 minutes. If the attribute value is greater than 1440, Horizon 7 treats it as 1440 minutes.

Setting Up Smart Card Authentication

3

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 Administrator. 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 Access Point, 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 or security server host.

5 Configure Smart Card Settings in Horizon Administrator

You can use Horizon Administrator 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.

What to do next

Add the root certificate, intermediate certificate, or both to a server truststore file.

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.

What to do next

Add the CA certificate to a server truststore file.

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 or security server host.

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 or security 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 or security 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 Administrator. You do not need to configure smart card authentication settings for a security server. Settings that are configured on a Horizon Connection Server instance are also applied to a paired security server.

Configure Smart Card Settings in Horizon Administrator

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

When you configure these settings on a Connection Server instance, the settings are also applied to paired security servers.

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 Administrator, select **View Configuration > 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 View 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.

Option	Action
	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 View Connection Server when they remove their smart cards.	Select the **Disconnect user sessions on smart card removal** check box.
Keep users connected to View 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 Administrator, click the **Authentication** tab and select a configuration option from the **Smart card authentication for administrators** drop-down menu in the View Administration 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 Administrator. 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 Administrator.

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.

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 Administrator.

For information about configuring smart card authentication on Unified Access Gateway, see *Deploying and Configuring Unified Access Gateway*.

Procedure

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

See Configure a SAML Authenticator in Horizon Administrator.

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

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 Administrator.

  a Select **View Configuration > 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 View Agent or 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 3-1 lists the `locked.properties` file properties for certificate revocation checking.

Table 3-1. 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`**.

Table 3-1. Properties for Smart Card Certificate Revocation Checking (Continued)

Property	Description
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

4

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 View 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 Administrator

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

- Troubleshooting RSA SecurID Access Denial

  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 View 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 Administrator

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

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 will enter these values in Horizon Administrator. You can enter values for a primary and a secondary RADIUS authenticator.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. On the **Connection Servers** tab, select the server and click **Edit**.
3. On the **Authentication** tab, from the **2-factor authentication** drop-down list 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 list, 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 will be 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 SecurID Access Denial

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 Administrator, select **View Configuration > Servers**.
2. On the **Connection Servers** tab, select the Connection Server and click **Edit**.
3. On the **Authentication** tab, select **Clear node secret**.
4. Click **OK** to clear the node secret.
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 **View 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.

Solution

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

- The RADIUS server has not been configured to accept the View Connection Server instance as a RADIUS client. Each View 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 View 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 third-party load balancer or gateway. 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 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.

Configure a SAML Authenticator in Horizon Administrator

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 Administrator. 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 *Deploying and Configuring Unified Access Gateway*.

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.

- (Optional) 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 Unified Access Gateway 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 Administrator, select **Configuration > 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 Unified Access Gateway 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 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).
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.

Option	Description
SAML metadata	(For static authenticators) Metadata text that you generated and copied from the Unified Access Gateway 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.

7 In the System Health section on the Horizon Administrator dashboard, select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

If the configuration is successful, the authenticator's health is green. An authenticator's health can display red if the certificate is untrusted, if VMware Identity Manager is unavailable, or if the metadata URL is invalid. If the certificate is untrusted, you might be able to click **Verify** to validate and accept the certificate.

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 under the **pae-NameValuePair** attribute, add the new 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 Unified Access Gateway 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-samlencryptionkeyvalidityдays=number-of-days
   cs-samlsigningkeyvalidityдays=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. In the System Health section on the Horizon Administrator dashboard, you can select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

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 Administrator to disable the unreachable dynamic SAML authenticators. For information about disabling a SAML authenticator, see Configure a SAML Authenticator in Horizon Administrator.

Configure Workspace ONE Access Policies in Horizon Administrator

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 Administrator.

Procedure

1. In Horizon Administrator, select **Configuration > 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 Without Requiring Credentials 5

After users log in to a client device or to VMware Identity Manager, they can connect to a published application or desktop without being prompted for Active Directory credentials.

Administrators can choose to set up the configuration based on user requirements.

- Provide users unauthenticated access to published applications. Administrators can configure the set up so that users do not need to log in to Horizon Client with Active Directory (AD) credentials.
- Use Log In as Current User for Windows-based clients. For Windows-based clients, administrators can configure the setup so that users do not need to supply additional credentials to log in to a Horizon server after they log in to a Windows-based client with AD credentials.
- Save credentials in mobile and Mac clients. For mobile and Mac clients, administrators can configure the Horizon server to save credentials. With this feature, users do not need to remember AD credentials for SSO (single sign-on) after supplying them once to a mobile or Mac client.
- Configure True SSO for VMware Identity Manager. For VMware Identity Manager, administrators can configure True SSO so that users who authenticate using some method other than AD credentials can then also log in to a published desktop or application without being prompted for AD credentials.

This chapter includes the following topics:

Providing Unauthenticated Access for Published Applications

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 Horizon Client version 4.4 or later. For the HTML Access client, this feature requires version 4.5 or later.

Workflow for Configuring Unauthenticated Users

1 Create users for unauthenticated access. See, Create Users for Unauthenticated Access.

2 Enable unauthenticated access to users and set a default unauthenticated user. See, Enable Unauthenticated Access for Users.

3 Entitle unauthenticated users to published applications. See, Entitle Unauthenticated Access Users to Published Applications.

4 Enable unauthenticated access from the Horizon Client. See, Unauthenticated Access From Horizon Client.

Rules and Guidelines for Configuring Unauthenticated Users

- Two-factor authentication, such as RSA and RADIUS, and smart card authentication are not supported for unauthenticated access.
- Smart card authentication and unauthenticated access are mutually exclusive. When smart card authentication is set to **Required** in Connection Server, unauthenticated access is disabled even if it was previously enabled.
- VMware Identity Manager and VMware App Volumes are not supported for unauthenticated access.
- Both PCoIP and VMware Blast display protocols are supported for this feature.
- The unauthenticated access feature does not verify license information for RDS hosts. The administrator must configure and use device licenses.
- The unauthenticated access feature does not retain any user-specific data. The user can verify the data storage requirements for the application.
- You cannot reconnect to unauthenticated application sessions. When a user disconnects from the client, the RDS host logs off the local user session automatically.
- Unauthenticated access is only supported for published applications.
- Unauthenticated access is not supported with a security server or an Unified Access Gateway appliance.
- User preferences are not preserved for unauthenticated users.
- Virtual desktops are not supported for unauthenticated users.
- Horizon Administrator displays a red status for the Connection Server, if the Connection Server is configured with a CA signed certificate and enabled for unauthenticated access but a default unauthenticated user is not configured.

- The unauthenticated access feature does not work if the `AllowSingleSignon` group policy setting for Horizon Agent installed on an RDS host is disabled. Administrators can also control whether to disable or enable unauthenticated access with the `UnAuthenticatedAccessEnabled` Horizon Agent group policy setting. The Horizon Agent group policy settings are included in the `vdm_agent.admx` template file. You must reboot the RDS host for this policy to take effect.

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

- Verify that the Active Directory (AD) user for whom you want to configure unauthenticated access for has a valid UPN. Only an AD user can be configured as an unauthenticated access user.

Note Administrators can create only one user for each AD 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.

Procedure

1. In Horizon Administrator, 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.

   The user must have a valid UPN.
4. Select a user and click **Next**.

   Repeat this step to add multiple users.
5. (Optional) 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 **Finish**.

Connection Server creates the unauthenticated access user and displays the user details including user alias, user name, first and last name, number of source pods, application entitlements, and sessions. You can click the number in the Source Pods column to display pod information.

What to do next

Enable unauthenticated access for users in Connection Server. See, Enable Unauthenticated Access for Users.

Enable Unauthenticated Access for Users

After you create users for unauthenticated access, you must enable unauthenticated access in the Connection Server to enable users to connect and access published applications.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. Click the **Connection Servers** tab.
3. Select the Connection Server instance and click **Edit**.
4. Click the **Authentication** tab.
5. Change **Unauthenticated Access** to **Enabled**.
6. From the **Default unauthenticated access user** drop-down menu, select a user as the default user.

   The default user must be present on the local pod in a Cloud Pod Architecture environment. If you select a default user from a different pod, Connection Server creates the user on the local pod before it makes the user the default user.
7. (Optional) Enter the default session timeout for the user.

   The default session timeout is 10 minutes after being idle.
8. Click **OK**.

What to do next

Entitle unauthenticated users to published applications. See Entitle Unauthenticated Access Users to Published Applications.

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 the *Setting Up Published Desktops and Applications in Horizon 7* document.
- Create an application pool for published applications that run on a farm of RDS hosts. See "Creating Application Pools" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

1. In Horizon Administrator, select **Catalog > Application Pools** and click the name of the application pool.
2. Select **Add entitlement** from the **Entitlements** drop-down menu.

3 Click **Add**, select one or more search criteria, click **Find**, and select the **Unauthenticated Users** check box 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 Click **OK** to save your changes.

An unauthenticated access icon appears next to the unauthenticated access user after the entitlement process completes.

What to do next

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

Search Unauthenticated Access Sessions

Use Horizon Administrator to list or search for application sessions that unauthenticated access users have connected to. The unauthenticated access user icon appears next to those sessions that unauthenticated access users have connected to.

Procedure

1 In Horizon Administrator, select **Monitoring > Sessions**.

2 Click **Applications** to search for application sessions.

3 Select search criteria and being the search.

The search results include the user, type of session (desktop or application), machine, pool or farm, DNS name, client ID and security gateway. The session start time, duration, state, and last session also appear in the search results.

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.

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 Administrator, select **Users and Groups**.

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

3 Click **OK**.

What to do next

Remove application entitlements for the user. See " Remove Entitlements from a Desktop or Application Pool" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

Unauthenticated Access From Horizon Client

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

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

Prerequisites

- Verify that Horizon 7 version 7.1 Connection Server is configured for unauthenticated access.
- Verify that the unauthenticated access users are created in Horizon Administrator. If the default unauthenticated user is the only unauthenticated access user, Horizon Client connects to the Connection Server instance with the default user.

Procedure

1. Start Horizon Client.
2. In Horizon Client, select **Log in anonymously with Unauthenticated Access**.
3. Connect to the Connection Server instance.
4. Select a user alias from the drop-down menu and click **Login**.

   The default user has the "default" suffix.
5. Double-click a published application to start the application.

Using the Log In as Current User Feature Available with Windows-Based Horizon Client

With Horizon Client for Windows, when users select the **Log in as current user** check box, the credentials that they provided when logging in to the client system are used to authenticate to the Horizon Connection Server instance and to the remote desktop. No further user authentication is required.

To support this feature, user credentials are stored on both the Connection Server instance and on the client system.

- On the Connection Server instance, user credentials are encrypted and stored in the user session along with the username, domain, and optional UPN. The credentials are added when authentication occurs and are purged when the session object is destroyed. The session object is destroyed when the user logs out, the session times out, or authentication fails. The session object resides in volatile memory and is not stored in Horizon LDAP or in a disk file.

- On the client system, user credentials are encrypted and stored in a table in the Authentication Package, which is a component of Horizon Client. The credentials are added to the table when the user logs in and are removed from the table when the user logs out. The table resides in volatile memory.

Administrators can use Horizon Client group policy settings to control the availability of the **Log in as current user** check box and to specify its default value. Administrators can also use group policy to specify which Connection Server instances accept the user identity and credential information that is passed when users select the **Log in as current user** check box in Horizon Client.

The Recursive Unlock feature is enabled after a user logs in to Connection Server with the Log in as current user feature. The Recursive Unlock feature unlocks all remote sessions after the client machine has been unlocked. Administrators can control the Recursive Unlock feature with the **Unlock remote sessions when the client machine is unlocked** global policy setting in Horizon Client. For more information about global policy settings for Horizon Client, see the Horizon Client documentation at the VMware Horizon Clients documentation Web page.

The Log in as current user feature has the following limitations and requirements:

- When smart card authentication is set to Required on a Connection Server instance, 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.
- The time on the system where the client logs in and the time on the Connection Server host must be synchronized.
- If the default **Access this computer from the network** user-right assignments are modified on the client system, they must be modified as described in VMware Knowledge Base (KB) article 1025691.
- The client machine must be able to communicate with the corporate Active Directory server and not use cached credentials for authentication. For example, if users log in to their client machines from outside the corporate network, cached credentials are used for authentication. If the user then attempts to connect to a security server or a Connection Server instance without first establishing a VPN connection, the user is prompted for credentials, and the Log in as Current User feature does not work.

Saving Credentials in Mobile and Mac Horizon Clients

Administrators can configure Connection Server to enable mobile and Mac Horizon Clients to remember a user's user name, password, and domain information.

For Horizon Client for mobile devices, this feature causes the **Save password** check box to appear on the login dialog boxes. For Horizon Client for Mac, this feature causes the **Remember this password** check box to appear on the login dialog box.

If users choose to save their credentials, the credentials are added to the login fields in Horizon Client on subsequent connections.

To enable this feature, you must set a value in View LDAP to indicate how long to save credential information in the client. For Horizon Client for Mac, this feature is supported only in version 4.1 or later.

Note On Windows-based Horizon clients, the feature for logging in as the current user avoids requiring users to supply credentials multiple times.

Configure a Timeout Limit to Save Horizon Client Credentials

You configure a timeout limit that indicates how long to save Horizon Client credential information on mobile devices and Mac client systems by setting a value in View LDAP. The timeout limit is set in minutes. When you change View LDAP on a Connection Server instance, the change is propagated to all replicated Connection Server instances.

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 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 **clientCredentialCacheTimeout** attribute value.

   When `clientCredentialCacheTimeout` is not set or is set to **`0`**, the feature is disabled. To enable this feature, you can set the number of minutes to retain the credential information, or set a value of **-1**, meaning that there is no timeout.

On Connection Server, the new setting takes effect immediately. You do not need to restart the Connection Server service or the client computer.

Setting Up True SSO

With the True SSO (single sign-on) feature, after users log in to VMware Identity Manager using a smart card or RSA SecurID or RADIUS authentication, users are not required to also enter Active Directory credentials in order to use a virtual desktop or published desktop or application.

If a user authenticates by using Active Directory credentials, the True SSO feature is not necessary, but you can configure True SSO to be used even in this case, so that the AD credentials that the user provides are ignored and True SSO is used.

When connecting to a virtual desktop or published application, users can select to use either the native Horizon Client or HTML Access.

This feature has the following limitations:

- This feature does not work for virtual desktops that are provided by using the View Agent Direct Connection plug-in.
- This feature is supported only in IPv4 environments.

Following is a list tasks you must perform to set up your environment for True SSO:

1 Determining an Architecture for True SSO

2 Set Up an Enterprise Certificate Authority

3 Create Certificate Templates Used with True SSO

4 Install and Set Up an Enrollment Server

5 Export the Enrollment Service Client Certificate

6 Configure SAML Authentication to Work with True SSO

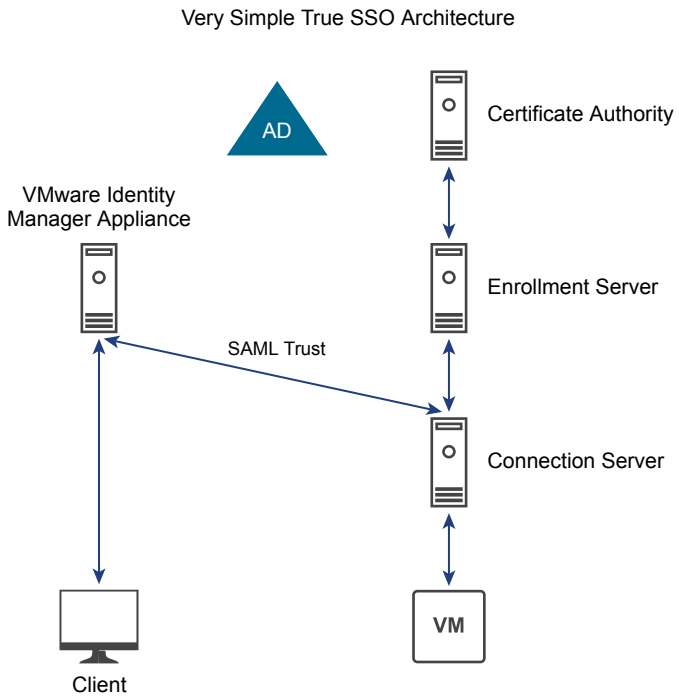
7 Configure Horizon Connection Server for True SSO

Determining an Architecture for True SSO

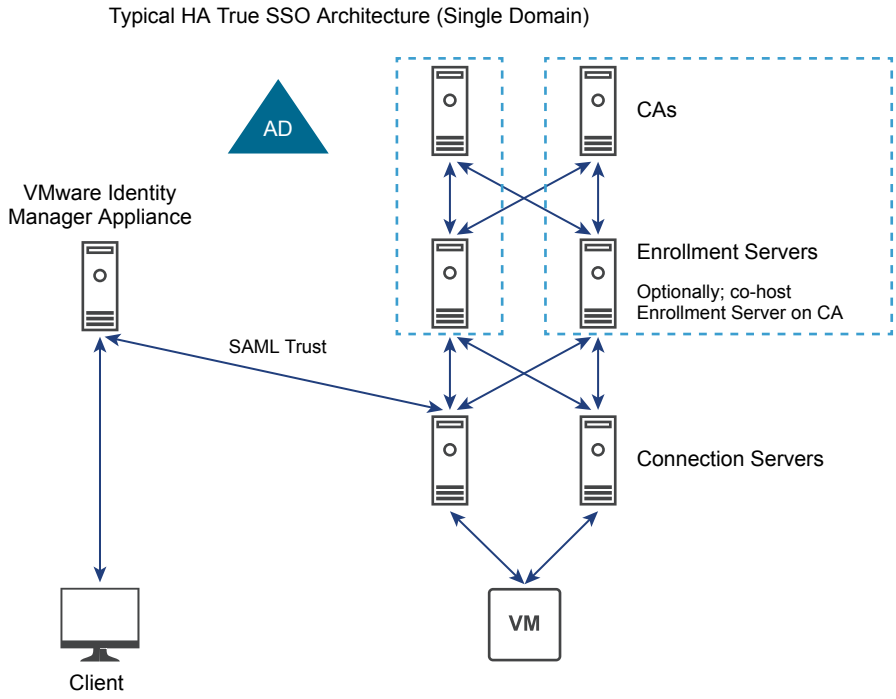
To use True SSO, you must have or add a certificate authority and create an enrollment server. These two servers communicate to create the short-lived Horizon virtual certificate that enables a password-free Windows logon. You can use True SSO in a single domain, in a single-forest with multiple domains, and in a multiple-forest, multiple-domain setup.

VMware recommends to have two CAs and two ESs deployed to use True SSO. The following examples illustrate True SSO in different architectures.

The following figure illustrates a simple True SSO architecture.

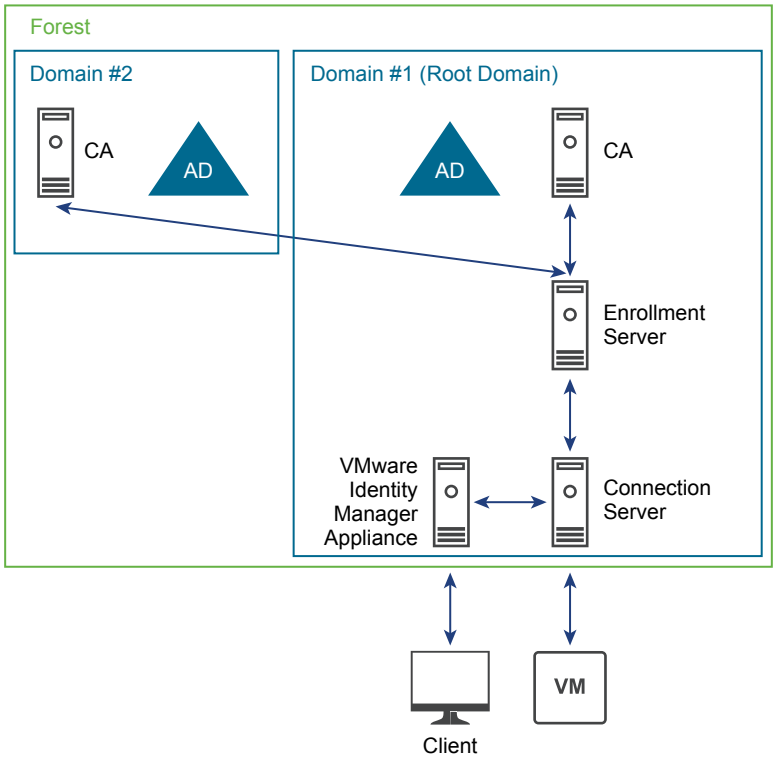


The following figure illustrates True SSO in a single domain architecture.



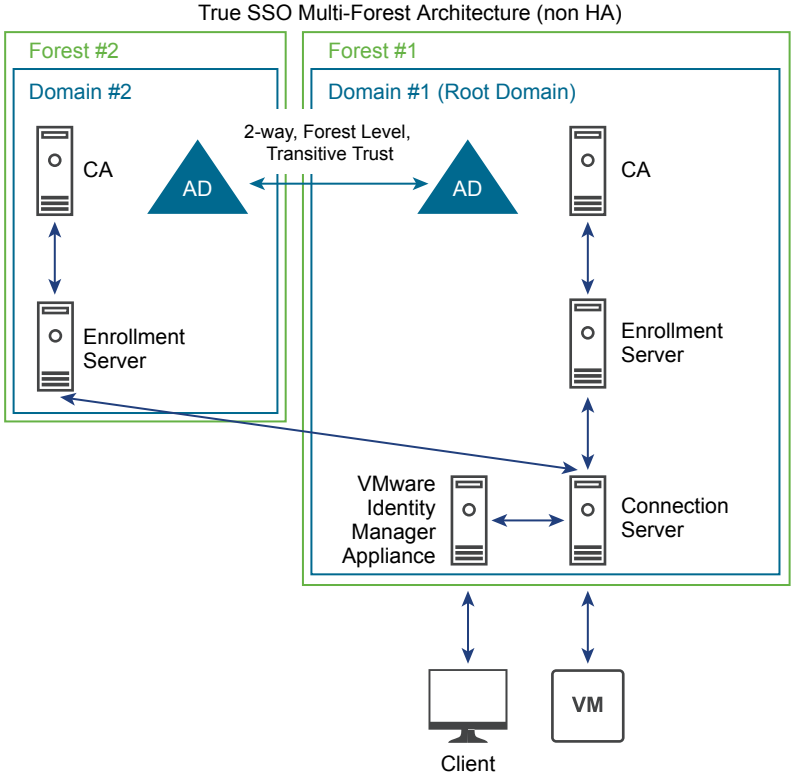
The following figure illustrates True SSO in a single-forest with multiple domains architecture.

True SSO Single Forest Multiple Domain Architecture (non HA)



The following figure illustrates True SSO in a multiple-forest architecture.

True SSO Multi-Forest Architecture (non HA)



Set Up an Enterprise Certificate Authority

If you do not already have a certificate authority set up, you must add the Active Directory Certificate Services (AD CS) role to a Windows server and configure the server to be an enterprise CA.

If you do already have an enterprise CA set up, verify that you are using the settings described in this procedure.

You must have at least one enterprise CA, and VMware recommends that you have two for purposes of failover and load balancing. The enrollment server you will create for True SSO communicates with the enterprise CA. If you configure the enrollment server to use multiple enterprise CAs, the enrollment server will alternate between the CAs available. If you install the enrollment server on the same machine that hosts the enterprise CA, you can configure the enrollment server to prefer using the local CA. This configuration is recommended for best performance.

Part of this procedure involves enabling non-persistent certificate processing. By default, certificate processing includes storing a record of each certificate request and issued certificate in the CA database. A sustained high volume of requests increases the CA database growth rate and could consume all available disk space if not monitored. Enabling non-persistent certificate processing can help reduce the CA database growth rate and frequency of database management tasks.

Prerequisites

- Create a Windows Server 2008 R2 or Windows Server 2012 R2 virtual machine.
- Verify that the virtual machine is part of the Active Directory domain for the Horizon 7 deployment.
- Verify that you are using an IPv4 environment. This feature is currently not supported in an IPv6 environment.
- Verify that the system has a static IP address.

Procedure

1. Log in to the virtual machine operating system as an administrator and start Server Manager.
2. Select the settings for adding roles.

Operating System	Selections
Windows Server 2012 R2	a Select **Add roles and features**. b On the Select Installation Type page, select **Role-based or feature-based installation**. c On the Select Destination Server page, select a server.
Windows Server 2008 R2	a Select **Roles** in the navigation tree. b Click **Add Roles** to start the **Add Role** wizard.

3. On the Select Server Roles page, select **Active Directory Certificate Services**.
4. In the Add Roles and Features wizard, click **Add Features**, and leave the **Include management tools** check box selected.

5 On the Select Features page, accept the defaults.

6 On the Select Role Services page, select **Certification Authority**.

7 Follow the prompts and finish the installation.

8 When installation is complete, on the Installation Progress page, click the **Configure Active Directory Certificate Services on destination server** link to open the AD CS Configuration wizard.

9 On the Credentials page, click **Next** and complete the AD CS Configuration wizard pages as described in the following table.

Option	Action
Role Services	Select **Certification Authority**, and click **Next** (rather than **Configure**).
Setup Type	Select **Enterprise CA**.
CA Type	Select **Root CA** or **Subordinate CA**. Some enterprises prefer two-tier PKI deployment. For more information, see http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx.
Private Key	Select **Create a new private key**.
Cryptography for CA	For hash algorithm, you can select **SHA1**, **SHA256**, **SHA384**, or **SHA512**. For key length, you can select **1024**, **2048**, **3072**, or **4096**. VMware recommends a minimum of SHA256 and a 2048 key.
CA Name	Accept the default or change the name.
Validity Period	Accept the default of 5 years.
Certificate Database	Accept the defaults.

10 On the Confirmation page, click **Configure**, and when the wizard reports a successful configuration, close the wizard.

11 Open a command prompt and enter the following command to configure the CA for non-persistent certificate processing:

```
certutil –setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

12 Enter the following command to ignore offline CRL (certificate revocation list) errors on the CA:

```
certutil –setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

This flag is required because the root certificate that True SSO uses will usually be offline, and thus revocation checking will fail, which is expected.

13 Enter the following commands to restart the service:

```
sc stop certsvc
sc start certsvc
```

What to do next

Create a certificate template. See Create Certificate Templates Used with True SSO.

Create Certificate Templates Used with True SSO

You must create a certificate template that can be used for issuing short-lived certificates, and you must specify which computers in the domain can request this type of certificate.

You can create more than one certificate template. You can configure only one template per domain but you can share the template across multiple domains. For example, if you have an Active Directory forest with three domains and you want to use True SSO for all three domains, you can choose to configure one, two, or three templates. All domains can share the same template, or you can have different templates for each domain.

Prerequisites

- Verify that you have an enterprise CA to use for creating the template described in this procedure. See Set Up an Enterprise Certificate Authority.
- Verify that you have prepared Active Directory for smart card authentication. For more information, see the *Horizon 7 Installation* document.
- Create a security group in the domain and forest for the enrollment servers, and add the computer accounts of the enrollment servers to that group.

Procedure

1. To configure True SSO, on the machine that you are using for the certificate authority, log in to the operating system as an administrator and go to **Administrative Tools > Certification Authority**.
   a. Expand the tree in the left pane, right-click **Certificate Templates** and select **Manage**.
   b. Right-click the **Smartcard Logon** template and select **Duplicate**.

c Make the following changes on the following tabs:

Tab	Action
Compatibility tab	■ For **Certificate Authority**, select **Windows Server 2008 R2**. ■ For **Certificate Recipient**, select **Windows 7/Windows Server 2008 R2**.
General tab	■ Change the template display name to `True SSO`. ■ Change the validity period to a period that is as long as a typical working day; that is, as long as the user is likely to remain logged into the system. So that the user does not lose access to network resources while logged on, the validity period must be longer than the Kerberos TGT renewal time in the users domain. (The default maximum lifetime of the ticket is 10 hours. To find the default domain policy, you can go to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Kerberos Policy:Maximum lifetime for user ticket**.) ■ Change the renewal period to 50%-75% of the validity period.
Request Handling tab	■ For **Purpose**, select **Signature and smartcard logon**. ■ Select, **For automatic renewal of smart cards, …**
Cryptography tab	■ For **Provider Category**, select **Key Storage Provider**. ■ For **Algorithm name**, select **RSA**.
Server tab	Select **Do not store certificates and requests in the CA database**. **Important** Make sure to deselect **Do not include revocation information in issued certificates**. (This box gets selected when you select the first one, and you have to deselect (clear) it.)
Issuance Requirements tab	■ Select **This number of authorized signatures**, and type `1` in the box. ■ For **Policy type**, select **Application Policy** and set the policy to **Certificate Request Agent**. ■ For, **Require the following for reenrollment**, select **Valid existing certificate**.
Security tab	For the security group that you created for the enrollment server computer accounts, as described in the prerequisites, provide the following permissions: Read, Enroll 1 Click **Add**. 2 Specify which computers to allow to enroll for certificates. 3 For these computers select the appropriate check boxes to give the computers the following permissions: Read, Enroll.

d Click **OK** in the Properties of New Template dialog box.

e Close the Certificate Templates Console window.

f Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.

Note This step is required for all certificate authorities that issue certificates based on this template.

g In the Enable Certificate Templates window, select the template you just created (for example, **True SSO Template**) and click **OK**.

2 To configure Enrollment Agent Computer, on the machine that you are using for the certificate authority, log in to the operating system as an administrator and go to **Administrative Tools > Certification Authority**.

   a Expand the tree in the left pane, right-click **Certificate Templates** and select **Manage**.

   b Locate and open the Enrollment Agent Computer template and then make the following change on the **Security** tab:

      For the security group that you created for the enrollment server computer accounts, as described in the prerequisites, provide the following permissions: Read, Enroll

      1 Click **Add**.

      2 Specify which computers to allow to enroll for certificates.

      3 For these computers select the appropriate check boxes to give the computers the following permissions: Read, Enroll.

   c Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.

      Note This step is required for all certificate authorities that issue certificates based on this template.

   d In the Enable Certificate Templates window, select **Enrollment Agent Computer** and click **OK**.

What to do next

Create an enrollment service. See Install and Set Up an Enrollment Server.

Install and Set Up an Enrollment Server

You run the Connection Server installer and select the Horizon 7 Enrollment Server option to install an enrollment server. The enrollment server requests short-lived certificates on behalf of the users you specify. These short-term certificates are the mechanism True SSO uses for authentication to avoid prompting users for Active Directory credentials.

You must install and set up at least one enrollment server, and the enrollment server cannot be installed on the same host as View Connection Server. VMware recommends that you have two enrollment servers for purposes of failover and load balancing. If you have two enrollment servers, by default one is preferred and the other is used for failover. You can change this default, however, so that the connection server alternates sending certificate requests to both enrollment servers.

If you install the enrollment server on the same machine that hosts the enterprise CA, you can configure the enrollment server to prefer using the local CA. For best performance, VMware recommends combining the configuration to prefer using the local CA with the configuration to load balance the enrollment servers. As a result, when certificate requests arrive, the connection server will use alternate enrollment servers, and each enrollment server will service the requests using the local CA. For information about the configuration settings to use, see Enrollment Server Configuration Settings and Connection Server Configuration Settings.

Prerequisites

- Create a Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016 virtual machine with at least 4GB of memory, or use the virtual machine that hosts the enterprise CA. Do not use a machine that is a domain controller.
- Verify that no other View component, including View Connection Server, View Composer, security server, Horizon Client, or View Agent or Horizon Agent is installed on the virtual machine.
- Verify that the virtual machine is part of the Active Directory domain for the Horizon 7 deployment.
- Verify that you are using an IPv4 environment. This feature is currently not supported in an IPv6 environment
- VMware recommends that the system must have a static IP address.
- Verify that you can log in to the operating system as a domain user with Administrator privileges. You must log in as an administrator to run the installer.

Procedure

1. On the machine that you plan to use for the enrollment server, add the Certificate snap-in to MMC:
   a. Open the MMC console and select **File > Add/Remove Snap-in**
   b. Under **Available snap-ins**, select **Certificates** and click **Add**.
   c. In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
   d. In the Add or Remove Snap-in window, click **OK**.
2. Issue an enrollment agent certificate:
   a. In the Certificates console, expand the console root tree, right-click the **Personal** folder, and select **All Tasks > Request New Certificate**.
   b. In the Certificate Enrollment wizard, accept the defaults until you get to the Request Certificates page.
   c. On the Request Certificates page, select the **Enrollment Agent (Computer)** check box and click **Enroll**.
   d. Accept the defaults on the other wizard pages, and click **Finish** on the last page.

   In the MMC console, if you expand the **Personal** folder and select **Certificates** in the left pane, you will see a new certificate listed in the right pane.

3 Install the enrollment server:

a Download the View Connection Server installer file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes View Connection Server.

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

b Double-click the installer file to start the wizard, and follow the prompts until you get to the Installation Options page.

c On the Installation Options page, select **Horizon 7 Enrollment Server** and choose an authentication mode for the enrollment server instance, then click **Next**.

Option	Description
Horizon 7	Configures the authentication mode for a Horizon 7 environment.
Horizon Cloud	Configures the authentication mode for a Horizon Cloud environment.

d Follow the prompts to finish the installation.

You must enable the incoming connections on Port 32111 (TCP) for enrollment server to be functional. The installer opens the port by default during installation.

What to do next

- If you installed the enrollment server on the same machine that hosts an enterprise CA, configure the enrollment server to prefer using the local CA. See Enrollment Server Configuration Settings. Optionally, if you install and set up more than one enrollment server, configure connection servers to enable load balancing between the enrollment servers. See Connection Server Configuration Settings.
- Pair connection servers with enrollment servers. See Export the Enrollment Service Client Certificate.

Export the Enrollment Service Client Certificate

To accomplish pairing, you can use the MMC Certificates snap-in to export automatically generated, self-signed Enrollment Service Client certificate from one connection server in the cluster. This certificate is called a client certificate because the connection server is a client of the Enrollment Service provided by the enrollment server.

Enrollment Service must trust the VMware Horizon Connection Server when it prompts the Enrollment Servers to issue the short lived certificates for Active Directory users. Hence, the VMware Horizon Connection Server clusters or pods must be paired with Enrollment Servers.

The Enrollment Service Client certificate is automatically created when a Horizon 7 or later Connection Server is installed and the VMware Horizon Connection Server service starts. The certificate is distributed through View LDAP to other Horizon 7 Connection Servers that get added to the cluster later. The certificate is then stored in a custom container (`VMware Horizon View Certificates\Certificates`) in the Windows Certificate Store on the computer.

Prerequisites

Verify that you have a Horizon 7 or later Connection Server. For installation instructions, see *Horizon 7 Installation*. For upgrade instructions, see *Horizon 7 Upgrades*.

Important Customers can use their own certificates for pairing, rather than using the self-generated certificate created by the connection server. To do so, place the preferred certificate (and the associated private key) in the custom container (`VMware Horizon View Certificates\Certificates`) in the Windows Certificate Store on the connection server machine. You must then set the friendly name of the certificate to **`vdm.ec.new`**, and restart the server. The other servers in the cluster will fetch this certificate from LDAP. You can then perform the steps in this procedure.

Procedure

1. On one of the Connection Server machines in the cluster, add the Certificates snap-in to MMC:
   a. Open the MMC console and select **File > Add/Remove Snap-in**
   b. Under **Available snap-ins**, select **Certificates** and click **Add**.
   c. In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
   d. In the Add or Remove Snap-in window, click **OK**.
2. In the MMC console, in the left pane, expand the **VMware Horizon View Certificates** folder and select the **Certificates** folder.
3. In the right pane, right-click the certificate file with the friendly name **vdm.ec**, and select **All Tasks > Export**.
4. In the Certificate Export wizard, accept the defaults, including leaving the **No, do not export the private key** radio button selected.
5. When you are prompted to name the file, type a file name such as **`EnrollClient`**, for Enrollment Service Client certificate, and follow the prompts to finish exporting the certificate.

What to do next

Import the certificate into the enrollment server. See Import the Enrollment Service Client Certificate on the Enrollment Server.

Import the Enrollment Service Client Certificate on the Enrollment Server

To complete the pairing process, you use the MMC Certificates snap-in to import the Enrollment Service Client certificate into the enrollment server. You must perform this procedure on every enrollment server.

Prerequisites

- Verify that you have a Horizon 7 or later enrollment server. See Install and Set Up an Enrollment Server.
- Verify that you have the correct certificate to import. You can use either your own certificate or the automatically generated, self-signed Enrollment Service Client certificate from one Connection Server in the cluster, as described in Export the Enrollment Service Client Certificate.

  Important To use your own certificates for pairing, place the preferred certificate (and the associated private key) in the custom container (`VMware Horizon View Certificates\Certificates`) in the Windows Certificate Store on the Connection Server machine. You must then set the friendly name of the certificate to **`vdm.ec.new`**, and restart the server. The other servers in the cluster will fetch this certificate from LDAP. You can then perform the steps in this procedure.

  If you have your own client certificate, the certificate that you must copy to the enrollment server is the root certificate used to generate the client certificate.

Procedure

1. Copy the appropriate certificate file to the enrollment server machine.

   To use the automatically generated certificate, copy the Enrollment Service Client certificate from the Connection Server. To use your own certificate, copy the root certificate that was used to generate the client certificate.
2. On the enrollment server, add the Certificates snap-in to MMC:
   a. Open the MMC console and select **File > Add/Remove Snap-in**
   b. Under **Available snap-ins**, select **Certificates** and click **Add**.
   c. In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
   d. In the Add or Remove Snap-in window, click **OK**.
3. In the MMC console, in the left pane, right-click the **VMware Horizon View Enrollment Server Trusted Roots** folder and select **All Tasks > Import**.
4. In the Certificate Import wizard, follow the prompts to browse to and open the **EnrollClient** certificate file.
5. Follow the prompts and accept the defaults to finish importing the certificate.
6. Right-click the imported certificate and add a friendly name such as **`vdm.ec`** (for Enrollment Client certificate).

   VMware recommends you use a friendly name that identifies the Horizon 7 cluster, but you can use any name that helps you easily identify the client certificate.

What to do next

Configure the SAML authenticator used for delegating authentication to VMware Identity Manager. See Configure SAML Authentication to Work with True SSO.

Configure SAML Authentication to Work with True SSO

With the True SSO feature introduced in Horizon 7, users can log in to VMware Identity Manager 2.6 and later releases using smart card, RADIUS, or RSA SecurID authentication, and they will no longer be prompted for Active Directory credentials, even when they launch a remote desktop or application for the first time.

With earlier releases, SSO (single sign-on) worked by prompting users for their Active Directory credentials the first time they launched a remote desktop or published application if they had not previously authenticated with their Active Directory credentials. The credentials were then cached so that subsequent launches would not require users to re-enter their credentials. With True SSO, short-term certificates are created and used instead of AD credentials.

Although the process for configuring SAML authentication for VMware Identity Manager has not changed, one additional step has been added for True SSO. You must configure VMware Identity Manager so that password pop-ups are suppressed.

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

Prerequisites

- Verify that single sign-on is enabled as a global setting. In Horizon Administrator, select **Configuration > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.
- Verify that VMware Identity Manager is installed and configured. See the VMware Identity Manager documentation, available at https://docs.vmware.com/en/VMware-Identity-Manager/index.html
- 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. See the topic "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store," in the chapter "Configuring SSL Certificates for Horizon 7 Servers," in the *Horizon 7 Installation* document.
- Make a note of the FQDN of the VMware Identity Manager server instance.

Procedure

1. In Horizon Administrator, select **Configuration > 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, from the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down menu, select **Allowed** or **Required**.

   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
Label	You can use the FQDN of the VMware Identity Manager server instance.
Description	(Optional) You can use the FQDN of the VMware Identity Manager server instance.
Metadata URL	URL for retrieving all of the information required to exchange SAML information between the SAML identity provider and the Horizon 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 of the VMware Identity Manager server instance.
Administration URL	URL for accessing the administration console of the SAML identity provider (VMware Identity Manager instance). This URL has the format **`https://<Identity-Manager-FQDN>:8443.`**

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.

   The **SAML 2.0 Authenticator** drop-down menu displays the newly created authenticator, which is now set as the selected authenticator.

7 In the System Health section on the Horizon Administrator dashboard, select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

   If the configuration is successful, the authenticator's health is green. An authenticator's health can display red if the certificate is untrusted, if the VMware Identity Manager service is unavailable, or if the metadata URL is invalid. If the certificate is untrusted, you might be able to click **Verify** to validate and accept the certificate.

8 Log in to the VMware Identity Manager administration console, go to the View Pools page, and select the **Suppress Password Popup** check box.

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.
- Use the `vdmutil` command-line interface to configure True SSO on a connection server. See Configure Horizon Connection Server for True SSO.

For more information about how SAML authentication works, see Using SAML Authentication.

Configure Horizon Connection Server for True SSO

You can use the `vdmutil` command-line interface to configure and enable or disable True SSO.

This procedure is required to be performed on only one Connection Server in the cluster.

Important This procedure uses only the commands necessary for enabling True SSO. For a list of all the configuration options available for managing True SSO configurations, and a description of each option, see Command-line Reference for Configuring True SSO.

Prerequisites

- Verify that you can run the command as a user who has the Administrators role. You can use Horizon Administrator to assign the Administrators role to a user. See Chapter 6 Configuring Role-Based Delegated Administration.
- Verify that you have the fully qualified domain name (FQDN) for the following servers:
  - Connection Server
  - Enrollment server

    For more information, see Install and Set Up an Enrollment Server.
  - Enterprise certificate authority

    For more information, see Set Up an Enterprise Certificate Authority.
- Verify that you have the Netbios name or the FQDN of the domain.
- Verify that you have created a certificate template. See Create Certificate Templates Used with True SSO.
- Verify that you have created a SAML authenticator to delegate authentication to VMware Identity Manager. See Configure SAML Authentication to Work with True SSO.

Procedure

1 On a Connection Server in the cluster, open a command prompt and enter the command to add an enrollment server.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --environment --add --enrollmentServer enroll-server-fqdn
```

The enrollment server is added to the global list.

2 Enter the command to list the information for that enrollment server.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

The output shows the forest name, whether the certificate for the enrollment server is valid, the name and details of the certificate template you can use, and the common name of the certificate authority. To configure which domains the enrollment server can connect to, you can use a Windows Registry setting on the enrollment server. The default is to connect to all trusting domains.

Important You will be required to specify the common name of the certificate authority in the next step.

3 Enter the command to create a True SSO connector, which will hold the configuration information, and enable the connector.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --
primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

In this command, *TrueSSO-template-name* is the name of the template shown in the output for the previous step, and *ca-common-name* is the common name of the enterprise certificate authority shown in that output.

The True SSO connector is enabled on a pool or cluster for the domain specified. To disable True SSO at the pool level, run `vdmUtil --certsso --edit --connector <domain> --mode disabled`. To disable true SSO for an individual virtual machine, you can use GPO (vdm_agent.adm).

4 Enter the command to discover which SAML authenticators are available.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --list --authenticator
```

Authenticators are created when you configure SAML authentication between VMware Identity Manager and a connection server, using Horizon Administrator.

The output shows the name of the authenticator and shows whether True SSO is enabled.

Important You will be required to specify the authenticator name in the next step.

5 Enter the command to enable the authenticator to use True SSO mode.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

For `--truessoMode`, use `ENABLED` if you want True SSO to be used only if no password was supplied when the user logged in to VMware Identity Manager. In this case if a password was used and cached, the system will use the password. Set `--truessoMode` to `ALWAYS` if you want True SSO to be used even if a password was supplied when the user logged in to VMware Identity Manager.

What to do next

In Horizon Administrator, verify the health status of the True SSO configuration. For more information, see Using the System Health Dashboard to Troubleshoot Issues Related to True SSO.

To configure advanced options, use Windows advanced settings on the appropriate system. See Advanced Configuration Settings for True SSO.

Command-line Reference for Configuring True SSO

You can use the vdmutil command-line interface to configure and manage the True SSO feature.

Location of the Utility

By default, the path to the `vdmutil` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid entering the path on the command line, add the path to your PATH environment variable.

Syntax and Authentication

Use the following form of the `vdmutil` command from a Windows command prompt.

```
vdmutil authentication options --truesso additional options and arguments
```

The additional options that you can use depend on the command option. This topic focuses on the options for configuring True SSO (`--truesso`). Following is an example of a command for listing connectors that have been configured for True SSO:

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso
--list --connector
```

The `vdmutil` command includes authentication options to specify the user name, domain, and password to use for authentication.

Table 5-1. vdmutil Command Authentication Options

Option	Description
`--authAs`	Name of a Horizon 7 administrator user. Do not use *domain\username* or user principal name (UPN) format.
`--authDomain`	Fully qualified domain name or Netbios name of the domain for the Horizon 7 administrator user specified in the `--authAs` option.
`--authPassword`	Password for the Horizon 7 administrator user specified in the `--authAs` option. Entering **"*"** instead of a password causes the `vdmutil` command to prompt for the password and does not leave sensitive passwords in the command history on the command line.

You must use the authentication options with all `vdmutil` command options except for `--help` and `--verbose`.

Command Output

The `vdmutil` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails. The `vdmutil` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `vdmutil` command writes output to standard output, in US English.

Commands for Managing Enrollment Servers

You must add one enrollment server for each domain. You can also add a second enrollment server and later designate that server to be used as a backup.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--environment --list --enrollmentServers` options, but the `vdmUtil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServers
```

For more information about the authentication options, see Command-line Reference for Configuring True SSO.

Table 5-2. vdmutil truesso Command Options for Managing Enrollment Servers

Command and Options	Description
`--environment --add --enrollmentServer` *enroll-server-fqdn*	Adds the specified enrollment server to the environment, where *enroll-server-fqdn* is the FQDN of the enrollment server. If the enrollment server has already been added, when you run this command, nothing happens.
`--environment --remove --enrollmentServer` *enroll-server-fqdn*	Removes the specified enrollment server from the environment, where *enroll-server-fqdn* is the FQDN of the enrollment server. If the enrollment server has already been removed, when you run this command, nothing happens.
`--environment --list --enrollmentServers`	Lists the FQDNs of all enrollment servers in the environment.

Table 5-2. vdmutil truesso Command Options for Managing Enrollment Servers (Continued)

Command and Options	Description
`--environment --list --enrollmentServer` *enroll-server-fqdn*	List s the FQDNs of the domains and forests that are trusted by the domains and forests to which the enrollment server belongs, and the state of the enrollment certificate, which can be VALID or INVALID. VALID means the enrollment server has an Enrollment Agent certificate installed. The state might be INVALID for any of several reasons: ■ The certificate has not been installed. ■ The certificate Is not yet valid, or has expired. ■ The certificate was not issued by a trusted Enterprise CA. ■ The private key is not available. ■ The certificate has been corrupted. The log file on the enrollment server can provide the reason for the INVALID state.
`--environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn*	For the enrollment server in the specified domain, lists the CNs (common names) of the available certificate authorities, and provides the following information about each certificate template that can be used for True SSO: name, minimum key length, and hash algorithm.

Commands for Managing Connectors

You create one connector for each domain. The connector defines the parameters that are used for True SSO.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--list --connector` options, but the `vdmUtil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --list --connector
```

For more information about the authentication options, see Command-line Reference for Configuring True SSO.

Table 5-3. vdmutil truesso Command Options for Managing Connectors

Options	Description
`--create --connector --domain` *domain-fqdn* `--template` *template-name* `--primaryEnrollmentServer` *enroll-server1-fqdn* [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] `--certificateServer` *CA-common-name* `--mode {enabled |disabled}`	Creates a connector for the specified domain and configures the connector to use the following settings: ■ *template-name* is the name of the certificate template to use. ■ *enroll-server1-fqdn* is the FQDN of the primary enrollment server to use. ■ *enroll-server2-fqdn* is the FQDN of the secondary enrollment server to use. This setting is optional. ■ *CA-common-name* is the common name of the certificate authority to use. This can be a comma-separated list of CAs. To determine which certificate template and certificate authority are available for a particular enrollment server, you can run the `vdmutil` command with the `--truesso --environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn* options.
`--list --connector`	Lists the FQDNs of the domains that already have a connector created.
`--list --connector --verbose`	Lists all the domains that have connectors, and for each connector, provides the following information: ■ Primary enrollment server ■ Secondary enrollment server, if there is one ■ Name of the certificate template ■ Whether the connector is enabled or disabled ■ Common name of the certificate authority server or servers, if there are more than one
`--edit --connector` *domain-fqdn* [`--template` *template-name*] [`--mode {enabled |disabled]` [`--primaryEnrollmentServer` *enroll-server1-fqdn*] [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] [`--certificateServer` *CA-common-name*]	For the connector created for the domain specified by *domain-fqdn*, allows you to change any of the following settings: ■ *template-name* is the name of the certificate template to use. ■ The mode can be either `enabled` or `disabled`. ■ *enroll-server1-fqdn* is the FQDN of the primary enrollment server to use. ■ *enroll-server2-fqdn* is the FQDN of the secondary enrollment server to use. This setting is optional. ■ *CA-common-name* is the common name of the certificate authority to use. This can be a comma-separated list of CAs.
`--delete --connector` *domain-fqdn*	Deletes the connector that has been created for the domain specified by *domain-fqdn*.

Commands for Managing Authenticators

Authenticators are created when you configure SAML authentication between VMware Identity Manager Horizon 7and a Connection Server. The only management task is to enable or disable True SSO for the authenticator.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--list --authenticator` options, but the `vdmUtil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --list --authenticator
```

For more information about the authentication options, see Command-line Reference for Configuring True SSO.

Table 5-4. vdmutil truesso Command Options for Managing Authenticators

Command and Options	Description
`--list --authenticator [--verbose]`	Lists the fully qualified domain names (FQDNs) of all SAML authenticators found in the domain. For each one, specifies whether True SSO is enabled. If you use the `--verbose` option, the FQDNs of the associated connection servers are also listed.
`--list --authenticator --name` *label*	For the specified authenticator, lists whether True SSO is enabled, and lists the FQDNs of the associated connection servers. For *label* use one of the names listed when you use the `--authenticator` option without the `--name` option.
`--edit --authenticator --name` *label* `--truessoMode` *mode-value*	For the specified authenticator, sets the True SSO mode to the value you specify, where *mode-value* can be one of the following values: ■ `ENABLED`. True SSO is used only when the Active Directory credentials of the user is not available. ■ `ALWAYS`. True SSO is always used even if vIDM has the AD credentials of the user. ■ `DISABLED`. True SSO is disabled. For *label* use one of the names listed when you use the `--authenticator` option without the `--name` option.

Advanced Configuration Settings for True SSO

You can manage the True SSO advanced settings by using the GPO template on the Horizon Agent machine, registry settings on the enrollment server, and LDAP entries on the Connection Server. These settings include default timeout, configure load balancing, specify domains to be included, and more.

Horizon Agent Configuration Settings

You can use GPO template on the agent OS to turn off True SSO at the pool level or to change defaults for certificate settings such as key size and count and settings for reconnect attempts.

Note The following table shows the settings to use for configuring the agent on individual virtual machines, but you can alternatively use the Horizon Agent Configuration template files. The ADMX template file is named (`vdm_agent.admx`). Use the template files to make these policy settings apply to all the virtual machines in a desktop or application pool. If a policy is set the policy takes precedence over the registry settings.

The ADMX files are available in `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, which you can download from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the ZIP file.

Table 5-5. Keys for Configuring True SSO on Horizon Agent

Key	Min & Max	Description
`Disable True SSO`	N/A	Set this key to **`true`** to disable the feature on the agent. Use this setting in the group policy to disable True SSO at the pool level. The default is **`false`**.
`Certificate wait timeout`	10 -120	Specifies timeout period of certificates to arrive on the agent, in seconds. The default is **`40`**.
`Minimum key size`	1024 - 8192	Minimum allowed size for a key. The default is **`1024`**, meaning that by default, if the key size is below 1024, the key cannot be used.
`All key sizes`	N/A	Comma-separated list of key sizes that can be used. Up to 5 sizes can be specified; for example: **`1024,2048,3072,4096`**. The default is **`2048`**.
`Number of keys to pre-create`	1-100	Number of keys to pre-create on RDS servers that provide remote desktops and hosted Windows applications. The default is **`5`**.
`Minimum validity period required for a certificate`	N/A	Minimum validity period, in minutes, required for a certificate when it is being reused to reconnect a user. The default is **`5`**.

Enrollment Server Configuration Settings

You can use Windows Registry settings on the enrollment server OS to configure which domains to connect to, various timeout periods, polling periods, and retries, and whether to prefer using the certificate authority that is installed on the same local server (recommended).

To change the advanced configuration settings, you can open the Windows Registry Editor (`regedit.exe`) on the enrollment server machine and navigate to the following registry key:

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

Table 5-6. Registry Keys for Configuring True SSO on the Enrollment Server

Registry Key	Min & Max	Type	Description
`ConnectToDomains`	N/A	REG_MULTI_SZ	List of domains the enrollment server attempts to connect to automatically. For this multi-string registry type, the DNS fully qualified domain name (FQDN) of each domain is listed on its own line. The default is to trust all domains.
`ExcludeDomains`	N/A	REG_MULTI_SZ	List of domains the enrollment server does not connect to automatically. If the connection server provides a configuration set with any of the domains, the enrollment server will attempt to connect to that domain or domains. For this multi-string registry type, the DNS FQDN of each domain is listed on its own line. The default is to exclude no domains.
`ConnectToDomainsInForest`	N/A	REG_SZ	Specifies whether to connect to and use all domains in the forest that the enrollment server is a member of. The default is TRUE. Use one of the following values: ■ **`0`** means false; do not connect to the domains of the forest being used. ■ **`!=0`** means true.
`ConnectToTrustingDomains`	N/A	REG_SZ	Specifies whether to connect to explicitly trusting/incoming domains. The default is TRUE. Use one of the following values: ■ **`0`** means false; do not connect to explicitly trusting/incoming domains. ■ **`!=0`** means true.
`PreferLocalCa`	N/A	REG_SZ	Specifies whether to prefer the locally installed CA, if available, for performance benefits. If set to TRUE, the enrollment server will send requests to the local CA. If the connection to the local CA fails, the enrollment server will try to send certificates requests to alternate CAs. The default is FALSE. Use one of the following values: ■ **`0`** means false. ■ **`!=0`** means true.
`MaxSubmitRetryTime`	9500-59000	DWORD	Amount of time to wait before retrying to submit a certificate signing request, in milliseconds. The default is **`25000`**.

Table 5-6. Registry Keys for Configuring True SSO on the Enrollment Server (Continued)

Registry Key	Min & Max	Type	Description
SubmitLatencyWarningTime	500 - 5000	DWORD	Submit latency warning time when the interface is marked "Degraded" (in milliseconds). The default is **1500**. The enrollment server uses this setting to determine whether a CA should be considered to be in a degraded state. If the last three certificate requests took more milliseconds to complete than are specified by this setting, the CA is considered degraded, and this status appears in the Horizon Administrator Health Status dashboard. A CA usually issues a certificate within 20 ms, but if the CA has been idle for a few hours, any initial request might take longer to complete. This setting allows an administrator to find out that a CA is slow, without necessary having the CA marked as slow. Use this setting to configure the threshold for marking the CA as slow.
WarnForLonglivedCert	N/A	REG_SZ	Disable warning for long-lived True-SSO certificate (templates). The default is **True**. The enrollment server displays a warning status in the Horizon Administrator Health Status dashboard by reporting True SSO templates as being in a degraded or non-optimal state if the certificate lifetime is set to greater than 14 days. The enrollment server uses this setting to disable the warning. The enrollment server must be restarted for this setting to take effect.

Connection Server Configuration Settings

You can edit View LDAP on Connection Server to configure a timeout for generating certificates and whether to enable load balancing certificate requests between enrollment server (recommended).

To change the advanced configuration settings, you must use ADSI Edit on a Connection Server host. You can connect by typing in the distinguished name **DC=vdi, DC=vmware, DC=int** as the connection point, and typing in the server name and port for the computer **localhost:389**. Expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.

You can then edit the **pae-NameValuePair** attribute to add one or more of the values listed in the following table. You must use the syntax *name*=*value* when adding values.

Table 5-7. Advanced True SSO Settings for Connection Servers

Registry Key	Description
`cs-view-certsso-enable-es-loadbalance=[true|false]`	Specifies whether to enable load balancing CSR requests between two enrollment servers. The default is false. For example, add `cs-view-certsso-enable-es-loadbalance=true` to enable load balancing so that when certificate requests arrive, the connection server will use alternate enrollment servers,. Each enrollment server can service the requests using the local CA, if you have the enrollment server and CA on the same host.
`cs-view-certsso-certgen-timeout-sec=`*number*	Amount of time to wait for generating a certificate after receiving a CSR, in seconds. The default is **35**.

Identify an AD User That Does not Have an AD UPN

You can configure LDAP URL filters for Connection Server to identify an AD user that does not have an AD UPN.

You must use ADAM ADSI Edit on a Connection Server host. You can connect by typing in the distinguished name **DC=vdi, DC=vmware, DC=int**. Expand **OU=Properties**, and select **OU=Authenticator**.

You can then edit the **pae-LDAPURLList** attribute to add an LDAP URL filter.

For example, add the following filter:

`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)`

Connection Server uses the following default LDAP URL filters:

`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///??? (&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///??? (&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))`

`urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///??? (&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///??? (&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))`

If you configure an LDAP URL filter, Connection Server uses this LDAP URL filter and does not use the default LDAP URL filter to identity the user.

Examples of identifiers that you can use for SAML authentication for an AD user that does not have an AD UPN:

- `"cn"`
- `"mail"`
- `"description"`
- `"givenName"`
- `"sn"`

- "canonicalName"
- "sAMAccountName"
- "member"
- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

Using the System Health Dashboard to Troubleshoot Issues Related to True SSO

You can use the system health dashboard in Horizon Administrator to quickly see problems that might affect the operation of the True SSO feature.

For end users, if True SSO stops working, when the system attempts to log the user in to the remote desktop or application, the user sees the following message: "`The user name or password is incorrect`." After the user clicks **OK**, the user is taken to the login screen. On the Windows login screen the user sees an extra tile labeled **VMware SSO User**. If the user has the Active Directory credentials for an entitled user, the user can log in with AD credentials.

The system health dashboard in the top-left portion of the Horizon Administrator display contains a couple of items that pertain to True SSO.

Note The True SSO feature provides information to the dashboard only once per minute. Click the refresh icon in the upper-right corner to refresh the information immediately.

- You can click to expand **View Components > True SSO** to see a list of the domains that are using True SSO.

  You can click a domain name to see the following information: a list of enrollment servers configured for that domain, a list of enterprise certificate authorities, the name of the certificate template being used, and the status. If there is a problem, the Status field explains what it is.

  To change any of the configuration settings shown in the True SSO Domain Details dialog box, use the `vdmutil` command-line interface to edit the True SSO connector. For more information, see Commands for Managing Connectors.

- You can click to expand **Other Components > SAML 2.0 Authenticators** to see a list of the SAML authenticators that have been created for delegating authentication to VMware Identity Manager instances. You can click the authenticator name to examine the details and status.

Note In order for True SSO to be used, the global setting for SSO must be enabled. In Horizon Administrator, select **Configuration > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.

Table 5-8. Connection Server to Enrollment Server Connection Status

Status Text	Description
Failed to fetch True SSO health information.	The dashboard is unable to retrieve the health information from the Connection Server instance.
The <FQDN> enrollment server cannot be contacted by the True SSO configuration service.	In a pod, one of the Connection Server instances is elected to send the configuration information to all enrollment servers used by the pod. This Connection Server instance will refresh the enrollment server configuration once every minute. This message is displayed if the configuration task has failed to updated the enrollment server. For additional information, see the table for Enrollment Server Connectivity.
The <FQDN> enrollment server cannot be contacted to manage sessions on this connection server.	The current Connection Server instance is unable to connect to the enrollment server. This status is only displayed for the Connection Server instance that your browser is pointing to. If there are multiple Connection Server instances in the pod, you need to change your browser to point to the other Connection Server instances in order to check their status. For additional information, see the table for Enrollment Server Connectivity.

Table 5-9. Enrollment Server Connectivity

Status Text	Description
This domain <Domain Name> does not exist on the <FQDN> enrollment server.	The True SSO connector has been configured to use this enrollment server for this domain, but the enrollment server has not yet been configured to connect to this domain. If the state remains for longer than one minute, you need to check the state of the Connection Server currently responsible for refreshing the enrollment configuration.
The <FQDN> enrollment server's connection to the domain <Domain Name> is still being established.	The enrollment server has not been able to connect to a domain controller in this domain. If this state remains for longer than a minute, you might have to verify that name resolution from the enrollment server to the domain is correct, and that there is network connectivity between the enrollment server and the domain.
The <FQDN> enrollment server's connection to the domain <Domain Name> is stopping or in a problematic state.	The enrollment server has connected to a domain controller in the domain, but it has not been able to read the PKI information from the domain controller. If this happens, then there is likely a problem with the actual domain controller. This issue can also happen if DNS is not configured correctly. Check the log file on the enrollment server to see what domain controller the enrollment server is trying to use, and verify that the domain controller is fully operational.
The <FQDN> enrollment server has not yet read the enrollment properties from a domain controller.	This state is transitional, and is only displayed during startup of the enrollment server, or when a new domain has been added to the environment. This state usually lasts less than one minute. If this state lasts longer than a minute, either the network is extremely slow, or there is an issue causing difficulties accessing the domain controller.
The <FQDN> enrollment server has read the enrollment properties at least once, but has not been able to reach a domain controller for some time.	As long as the enrollment server reads the PKI configuration from a domain controller, it keeps polling for changes once every two minutes. This status will be set if the domain controller (DC) has been unreachable for a short period of time. Typically this inability to contact the DC might mean the enrollment server cannot detect any changes in PKI configuration. As long the certificate servers can still access a domain controller, certificates can still be issued.
The <FQDN> enrollment server has read the enrollment properties at least once but either has not been able to reach a domain controller for an extended time or another issue exists.	If the enrollment server has not been able to reach the domain controller for an extended period, then this state is displayed. The enrollment server will then try to discover an alternative domain controller for this domain. If a certificate server can still access a domain controller, then certificates can still be issued, but if this state remains for more than one minute, it means the enrollment server has lost access to all domain controllers for the domain, and it is likely that certificates can no longer be issued.

Table 5-10. Enrollment Certificate Status

Status Text	Description
A valid enrollment certificate for this domain's <domain name> forest is not installed on the <FQDN> enrollment server, or it may have expired	No enrollment certificate for this domain has been installed, or the certificate is invalid or has expired. The enrollment certificate must be issued by an enterprise CA that is trusted by the forest this domain is a member of. Verify that you have completed the steps in the *Horizon 7 Administration* document, which describes how to install the enrollment certificate on the enrollment server. You can also open the MMC, certificate management snap-in, opening the local computer store. Open the Personal certificate container and verify that the certificate is installed, and that it is valid. You can also open the enrollment server log file. The enrollment server will log additional information about the state of any certificate it located.

Table 5-11. Certificate Template Status

Status Text	Description
The template <name> does not exist on the <FQDN> enrollment server domain.	Check that you specified the correct template name.
Certificates generated by this template can NOT be used to log on to windows.	This template does not have the smart card usage enabled and data signing enabled. Check that you specified the correct template name. Verify that you have .completed the steps described in Create Certificate Templates Used with True SSO.
The template <name> is smartcard logon enabled, but cannot be used.	This template is enabled for smart card logon, but the template cannot be used with True SSO. Check that you specified the correct template name, verify that you have gone through the steps described in Create Certificate Templates Used with True SSO. You can also check the enrollment server log file, since it will log what setting in the template is preventing it from being used for True SSO.

Table 5-12. Certificate Server Configuration Status

Status Text	Description
The certificate server <CN of CA> does not exist in the domain.	Verify that you specified the correct name for the CA. You must specify the Common Name (CN).
The certificate is not in the NTAuth (Enterprise) store.	This CA is not an enterprise CA or its CA certificate has not been added to the NTAUTH store. If this CA is not a member of the forest, you must manually add the CA certificate to the NTAUTH store of this forest.

Table 5-13. Certificate Server Connection Status

Status Text	Description
The <FQDN> enrollment server is not connected to the certificate server <CN of CA>.	The enrollment server is not connected to the certificate server. This state might be a transitional state if the enrollment server just started, or if the CA was recently added to a True SSO connector. If the state remains for longer than one minute, it means that the enrollment server failed to connect to the CA. Validate that name resolution is working correctly, and that you have network connectivity to the CA, and that the system account for the enrollment server has permission to access the CA.
The <FQDN> enrollment server has connected to the certificate server <CN of CA>, but the certificate server is in a degraded state	This state is displayed if the CA is slow at issuing certificates. If the CA remains in this state, check the load of the CA or the domain controllers used by the CA. **Note** If the CA has been marked as slow, it will retain this state until at least one certificate request has been completed successfully, and that certificate was issued within a normal time frame.
The <FQDN> enrollment server can connect to the certificate server <CN of CA>, but the service is unavailable.	This state is issued if the enrollment server has an active connection to the CA but it is unable to issue certificates. This state is typically a transitional state. If the CA does not become available quickly, the state will be changed to disconnected.

Configuring Role-Based Delegated Administration

6

One key management task in an Horizon 7 environment is to determine who can use Horizon Administrator 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 Administrator 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 Administrator. 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 Administrator.

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 Administrator 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. 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

By default, automated desktop pools, manual desktop pools, and farms are created in the root access group, which appears as / or Root(/) in Horizon Administrator. 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 Administrator 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.

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 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.

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 6-1 shows an example of this type of configuration.

Table 6-1. 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 6-2 shows an example of this type of configuration.

Table 6-2. 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 Administrator 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 Administrator 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 Administrator when you select an administrator user or group. The administrator user is called Admin 1 and it has two permissions.

Table 6-3. 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 Administrator when you select the MarketingDesktops access group.

Table 6-4. Permissions on the Folders Tab for MarketingDesktops

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

The first permission is the same as the first permission shown in Table 6-3. The second permission is inherited from the second permission shown in Table 6-3. 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 6-3 appears in Horizon Administrator when you select the Inventory Administrators role.

Table 6-5. Permissions on the Role Tab for Inventory Administrators

Administrator	Access Group
view-domain.com\Admin1	/MarketingDesktops

Manage Administrators

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

The Administrators role is the most powerful role in Horizon Administrator. 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

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

- Remove an Administrator

  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

To create an administrator, you select a user or group from your Active Directory users and groups in Horizon Administrator 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.
- 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 Administrator, select **View Configuration > 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 Applies 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

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 View Administrator, select **View Configuration > 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 Administrator to add, delete, and review permissions for specific administrator users and groups, for specific roles, and for specific access groups.

- Add a Permission

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

- Delete a Permission

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

- Review Permissions

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

Add a Permission

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 Administrator, select **View Configuration > 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 **Roles** 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

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 Administrator, select **View Configuration > 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 **Delete Permission**.

Review Permissions

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

Procedure

1 Select **View Configuration > 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 **Roles** 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 Administrator to add and delete access groups and to review the desktop pools and machines in a particular access group.

- Add an Access Group

  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 a Farm to a Different Access Group

  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

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

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

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

- Review the vCenter Virtual Machines in an Access Group

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

Add an Access Group

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 Administrator, navigate to the Add Access Group dialog box.

Option	Action
From Catalog	■ Select **Catalog > Desktop Pools**. ■ From the **Access Group** drop-down menu in the top window pane, select **New Access Group**.
From Resources	■ Select **Resources > Farms**. ■ From the **Access Group** drop-down menu in the top window pane, select **New Access Group**.
From View Configuration	■ Select **View Configuration > Administrators**. ■ From the **Access Groups** tab, select **Add 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 a Farm to a Different Access Group

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 Administrator, select **Catalog > Desktop Pools** or **Resources > Farms**.

2 Select a pool or a farm.

3 Select **Change Access Group** from the **Access Group** drop-down menu in the top window pane.

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

Horizon Administrator moves the pool to the access group that you selected.

Remove an Access Group

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 a Farm to a Different Access Group.

Procedure

1 In Horizon Administrator, select **View Configuration > 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 Desktop Pools, Application Pools, or Farms in an Access Group

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

Procedure

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

Object	Action
Desktop Pools	Select **Catalog > Desktop Pools**.
Application Pools	Select **Catalog > Application Pools**.
Farms	Select **Resources > Farms**.

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

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

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

Review the vCenter Virtual Machines in an Access Group

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

Procedure

1 In Horizon Administrator, select **Resources > 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 Administrator to add, modify, and delete custom roles.

- Add a Custom Role

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

- Modify the Privileges in a Custom Role

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

- Remove a Custom Role

  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

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

Prerequisites

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

Procedure

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

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

3 Type 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

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 Administrator, select **View Configuration > Administrators**.

2 On the **Roles** tab, select the role.

3 Click **Privileges** to display the privileges in the role and click **Edit**.

4 Select or deselect privileges.

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

Remove a Custom Role

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.

Procedure

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

2 On the **Roles** 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 Administrator 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.

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

Table 6-6. Predefined Roles in Horizon Administrator

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 Administrator. ■ 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

Table 6-6. Predefined Roles in Horizon Administrator (Continued)

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. ■ Read-only access to Horizon Help Desk Tool. ■ Manage global sessions. ■ Can log in to Horizon Administrator. ■ 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. ■ Read-only access to Horizon Help Desk Tool. ■ Cannot log in to Horizon Administrator.	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. When administrators have this role on an access group, they can only perform these operations on the inventory objects in that access group.	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

Table 6-6. Predefined Roles in Horizon Administrator (Continued)

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 6-7. Global Privileges

Privilege	User Capabilities	Predefined Roles
Console Interaction	Log in to and use Horizon Administrator.	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)

Table 6-7. Global Privileges (Continued)

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 6-8. 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 View 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 6-9. 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 Administrator.

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

Table 6-10. 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**
Modify or delete a pool	**Manage Farms and Desktop and Application Pools**
Add or remove desktops from a pool	**Manage Farms and Desktop and Application Pools**
Refresh, Recompose, Rebalance, or change the default View Composer 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 Administrator.

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

Table 6-11. Machine Management Tasks and Privileges

Task	Required Privileges
Remove a virtual machine	**Manage Machine**
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 Administrator.

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 Administrator.

Table 6-12. 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 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 Administrator.

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 Administrator. You manage administrators on the Global Administrators View page in Horizon Administrator.

Table 6-13. 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 Tool Tasks

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

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

Table 6-14. 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**
Can log in to Horizon Administrator.	**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 6-15. 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**
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.

Configuring Policies in Horizon Administrator and Active Directory

7

You can use Horizon Administrator to set policies for client sessions. You can configure Active Directory group policy settings to control the behavior of View Connection Server, the PCoIP display protocol, and Horizon 7 logging and performance alarms.

You can also configure Active Directory group policy settings to control the behavior of Horizon Agent, Horizon Client for Windows, Horizon Persona Management, and certain features. For information about these policy settings, see the *Configuring Remote Desktop Features in Horizon 7* document.

This chapter includes the following topics:

Setting Policies in Horizon Administrator

You use Horizon Administrator 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.

- Configure Global Policy Settings

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

- Configure Policies for Desktop Pools

  You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

- Configure Policies for Users

  You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

- Horizon 7 Policies

  You can configure Horizon 7 policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

Configure Global Policy Settings

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

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Policies > Global Policies**.
2. Click **Edit policies** in the **View Policies** pane.
3. Click **OK** to save your changes.

Configure Policies for Desktop Pools

You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Catalog > Desktop Pools**.
2. Double-click the ID of the desktop pool and click the **Policies** tab.

   The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
3. Click **Edit Policies** in the **View Policies** pane.
4. Click **OK** to save your changes.

Configure Policies for Users

You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Catalog > Desktop Pools**.
2. Double-click the ID of the desktop pool and click the **Policies** tab.

   The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
3. Click **User Overrides** and then click **Add User**.
4. To find a user, click **Add**, type the name or description of the user, and then click **Find**.
5. Select one or more users from the list, click **OK**, and then click **Next**.

   The Add Individual Policy dialog box appears.
6. Configure the Horizon policies and click **Finish** to save your changes.

Horizon 7 Policies

You can configure Horizon 7 policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

The following table describes each Horizon 7 policy setting.

Table 7-1. 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.

Using Horizon 7 Group Policy Administrative Template Files

Horizon 7 provides several component-specific Group Policy Administrative ADMX template files. You can optimize and secure remote desktops and applications by adding the policy settings in the ADMX template files to a new or existing GPO in Active Directory.

All ADMX files that provide group policy settings for Horizon 7 are available in `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download the file from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the ZIP file.

The Horizon 7 ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

Horizon 7 ADMX Template Files

The Horizon 7 ADMX template files provide group policy settings that allow you to control and optimize Horizon 7 components.

Table 7-2. Horizon ADMX Template Files

Template Name	Template File	Description
VMware View Agent Configuration	`vdm_agent.admx`	Contains policy settings related to the authentication and environmental components of Horizon Agent. See the *Configuring Remote Desktop Features in Horizon 7* document.
VMware Horizon Client Configuration	`vdm_client.admx`	Contains policy settings related to Horizon Client for Windows. Clients that connect from outside the Connection Server host domain are not affected by policies applied to Horizon Client. See the *VMware Horizon Client for Windows Installation and Setup Guide* document.
VMware Horizon URL Redirection	`urlRedirection.admx`	Contains policy settings related to the URL Content Redirection Feature. If you add this template to a GPO for a remote desktop pool or application pool, certain URL links clicked inside the remote desktops or app can be redirected to a Windows-based client and opened in a client-side browser. If you add this template to a client-side GPO, when a user clicks certain URL links in a Windows-based client system, the URL can be opened in a remote desktop or application. See the *Configuring Remote Desktop Features in Horizon 7* document and see the *VMware Horizon Client for Windows Installation and Setup Guide* document.
VMware View Server Configuration	`vdm_server.admx`	Contains policy settings related to Connection Server.
VMware View Common Configuration	`vdm_common.admx`	Contains policy settings that are common to all Horizon components.
PCoIP Session Variables	`pcoip.admx`	Contains policy settings related to the PCoIP display protocol. See the *Configuring Remote Desktop Features in Horizon 7* document.
PCoIP Client Session Variables	`pcoip.client.admx`	Contains policy settings related to the PCoIP display protocol that affect Horizon Client for Windows. See the *VMware Horizon Client for Windows Installation and Setup Guide* document.

Table 7-2. Horizon ADMX Template Files (Continued)

Template Name	Template File	Description
Persona Management	`ViewPM.admx`	Contains policy settings related to Horizon Persona Management. See the *Setting Up Virtual Desktops in Horizon 7* document.
Remote Desktop Services	`vmware_rdsh_server.admx`	Contains policy settings related to Remote Desktop Services. See the *Configuring Remote Desktop Features in Horizon 7* document.
View RTAV Configuration	`vdm_agent_rtav.admx`	Contains policy settings related to webcams that are used with the Real-Time Audio-Video feature. See the *Configuring Remote Desktop Features in Horizon 7* document.
Scanner Redirection	`vdm_agent_scanner.admx`	Contains policy settings related to scanning devices that are redirected for use in published desktops and applications. See the *Configuring Remote Desktop Features in Horizon 7* document.
Serial COM	`vdm_agent_serialport.admx`	Contains policy settings related to serial (COM) ports that are redirected for use in virtual desktops. See the *Configuring Remote Desktop Features in Horizon 7* document.
VMware Horizon Printer Redirection	`vdm_agent_printing.admx`	Contains policy settings related to filtering redirected printers. See the *Configuring Remote Desktop Features in Horizon 7* document.

Horizon Connection Server Configuration ADMX Template Settings

The View Server Configuration ADMX (`vdm_server.admx`) template files contain policy settings related to all Horizon Connection Servers.

The following table describes each policy setting in the Connection Server configuration ADMX template file. The template contains only Computer Configuration settings. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Server Configuration** folder in the Group Policy Management Editor.

Table 7-3. Horizon Server Configuration Template Settings

Setting	Properties
`Enumerate Forest Trust Child Domains`	Determines if every domain trusted by the domain in which the server resides is enumerated. In order to establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to Connection Server in order to ensure that all trusted domains are available to the client on login. This property is enabled by default. When disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place. **Note** In environments with complex domain relationships, such as those that use multiple forest structures with trust between domains in their forests, the process can take a few minutes to complete.
`Recursive Enumeration of Trusted Domains`	Determines whether every domain trusted by the domain in which the server resides is enumerated. To establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to View Connection Server so that all trusted domains are available to the client on login. This setting is enabled by default. When it is disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place. In environments with complex domain relationships, such as those that use multiple forest structures with trust between domains in their forests, this process can take a few minutes to complete.
`Windows Password Authentication Mode`	Select the windows password authentication mode. ■ `KerberosOnly`. Authenticate using Kerberos. ■ `KerberosWithFallbackToNTLM`. Authenticate using Kerberos, but fallback to using NTLM on failure. ■ `Legacy`. Authenticate using NTLM, but fallback to using Kerberos on failure. Used to support legacy NT domain controllers. Default is `KerberosOnly`.

Horizon 7 Common Configuration ADMX Template Settings

The Horizon 7 Common Configuration ADMX (`vdm_common.admx`) template files contain policy settings common to all Horizon components. These templates contain only Computer Configuration settings.

Log Configuration Settings

The following table describes the log configuration policy setting in the Horizon Common Configuration ADMX template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Log Configuration** folder in the Group Policy Management Editor.

Table 7-4. View Common Configuration Template: Log Configuration Settings

Setting	Properties
`Number of days to keep production logs`	Specifies the number of days for which log files are retained on the system. If no value is set, the default applies and log files are kept for seven days.
`Maximum number of debug logs`	Specifies the maximum number of debug log files to retain on the system. When a log file reaches its maximum size, no further entries are added and a new log file is created. When the number of previous log files reaches this value, the oldest log file is deleted.
`Maximum debug log size in Megabytes`	Specifies the maximum size in megabytes that a debug log can reach before the log file is closed and a new log file is created.
`Log Directory`	Specifies the full path to the directory for log files. If the location is not writeable, the default location is used. For client log files, an extra directory with the client name is created.
`Send logs to a Syslog server`	Allows View server logs to be sent to a Syslog server such as VMware vCenter Log Insight. Logs are sent from all View servers in the OU or domain in which this GPO is configured. You can send Horizon Agent logs to a Syslog server by enabling this setting in a GPO that is linked to an OU that contains your desktops. To send log data to a Syslog server, enable this setting and specify the log level and the server's fully qualified domain name (FQDN) or IP address. You can specify an alternate port if you do not want to use default port 514. Separate each element in your specification with a vertical bar (|). Use the following syntax: `Log Level|Server FQDN or IP [|Port number(514 default)]` For example: `Debug|192.0.2.2` **Important** Syslog data is sent across the network without software-based encryption. Because View server logs might contain sensitive data, avoid sending Syslog data on an insecure network. If possible, use link-layer security such as IPsec to prevent the possibility of this data being monitored on the network.

Performance Alarm Settings

Table 7-5 describe the performance alarm settings in the Horizon Common Configuration ADMX template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Performance Alarms** folder in the Group Policy Management Editor.

Table 7-5. View Common Configuration Template: Performance Alarm Settings

Setting	Properties
`CPU and Memory Sampling Interval in Seconds`	Specifies the CPU and memory polling interval CPU. A low sampling interval can result in an high level of output to the log.
`Overall CPU usage percentage to issue log info`	Specifies the threshold at which the overall CPU use of the system is logged. When multiple processors are available, this percentage represents the combined usage.

Table 7-5. View Common Configuration Template: Performance Alarm Settings (Continued)

Setting	Properties
`Overall memory usage percentage to issue log info`	Specifies the threshold at which the overall committed system memory use is logged. Committed system memory is memory that has been allocated by processes and to which the operating system has committed physical memory or a page slot in the pagefile.
`Process CPU usage percentage to issue log info`	Specifies the threshold at which the CPU usage of any individual process is logged.
`Process memory usage percentage to issue log info`	Specifies the threshold at which the memory usage of any individual process is logged.
`Process to check, comma separated name list allowing wild cards and exclusion`	Specifies a comma-separated list of queries that correspond to the name of one or more processes to be examined. You can filter the list by using wildcards within each query. ■ An asterisk (*) matches zero or more characters. ■ A question mark (?) matches exactly one character. ■ An exclamation mark (!) at the beginning of a query excludes any results produced by that query. For example, the following query selects all processes starting with **`ws`** and excludes all processes ending with **`sys`**: **`'!*sys,ws*'`**

Note Performance alarm settings apply to Horizon Connection Server and Horizon Agent systems only. They do not apply to Horizon Client systems.

Security Settings

Table 7-6 describe the security settings in the Horizon Common Configuration ADMX template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Security Settings** folder in the Group Policy Management Editor.

Table 7-6. View Common Configuration Template: Security Settings

Setting	Properties
`Only use cached revocation URLS`	Certificate revocation checking will only access cached URLs. Default if not configured is false.
`Revocation URL check timeout milliseconds`	The cumulative timeout across all revocation URL wire retrievals in milliseconds. Not configured or value set to 0 means that Microsoft default handling is used.
`Type of certificate revocation check`	Select the type of certificate revocation check to be done: ■ None ■ EndCertificateOnly ■ WholeChain ■ WholeChain Default is WholeChainButRoot.

General Settings

Table 7-7 describes the general settings in the Horizon Common Configuration ADMX template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration** folder in the Group Policy Management Editor.

Table 7-7. View Common Configuration Template: General Settings

Setting	Properties
`Disk threshold for log and events in Megabytes`	Specifies the minimum remaining disk space threshold for logs and events. If no value is specified, the default is 200. When the specified value is met, event logging stops.
`Enable extended logging`	Determines whether trace and debug events are included in the log files.
`Override the default View Windows event generation`	The following values are supported: ■ 0 = Event log entries are only produced for view events (no event log entries are generated for log messages) ■ 1 = Event log entries are produced in 4.5 (and earlier) compatibility mode. Event log entries are not produced for standard view events. Event log entries are based solely on log file text. ■ 2 = Event log entries are produced in 4.5 (and earlier) compatibility mode with view events also being included.

Maintaining Horizon 7 Components

8

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

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

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

When you use Horizon Administrator to perform backups, Horizon 7 backs up the View LDAP configuration data and View 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.

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 Administrator.
- 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 View Composer 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 Composer services, Horizon 7 backs up all the View 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 Administrator, select **View Configuration > Servers**.

2 On the **Connection Servers** tab, select the Connection Server instance to be backed up and click **Edit**.

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 View Composer configuration data at regular intervals. In Horizon Administrator, you can set the frequency and other aspects of the backup operations.

Table 8-1. 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.
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 View 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 View Composer Configuration Data.

Restoring Horizon Connection Server and View Composer Configuration Data

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

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

Before you restore configuration data, verify that you backed up the configuration data in Horizon Administrator. See Backing Up Horizon Connection Server and View 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 View Composer data from the `.svi` backup files to the View 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 Administrator 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 View 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 View Composer by stopping the Windows service VMware Horizon View Composer on the servers where View Composer runs.
2. Stop all security server instances by stopping the Windows service VMware Horizon Security Server on all security servers.
3. Uninstall all instances of Horizon Connection Server.

   Uninstall both VMware Horizon Connection Server and AD LDS Instance VMwareVDMDS.
4. Install one instance of Connection Server.
5. Stop the Connection Server instance by stopping the Windows service VMware Horizon Connection Server.
6. Click **Start > Command Prompt**.
7. 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:

   ```
   vdmimport –d –p mypassword
   –f MyEncryptedexport.LDF > MyDecryptedexport.LDF
   ```

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

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

   ```
   vdmimport –f MyDecryptedexport.LDF
   ```
9. Uninstall Connection Server.

   Uninstall only the package VMware Horizon Connection Server.
10. Reinstall Connection Server.
11. Log in to Horizon Administrator and validate that the configuration is correct.
12. Start the View Composer instances.
13. Reinstall the replica server instances.
14. Start the security server instances.

If there is a risk that the security servers have inconsistent configuration, they should also be uninstalled rather than stopped and then reinstalled at the end of the process.

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 View Composer if it is in use. If necessary, restore the View Composer configuration from backup. See Restore a View Composer Database. After you restore the View Composer configuration, you may need to manually resolve inconsistencies if the virtual machines in vCenter Server have changed since the backup of the View Composer configuration.

Restore a View Composer Database

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

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

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

Prerequisites

Verify the location of the View 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`.

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

   The file is located with the View 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 View Composer service.

What to do next

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

Result Codes for Restoring the View Composer Database

When you restore a View Composer database, the `SviConfig restoredata` command displays a result code.

Table 8-2. 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.

Table 8-2. Restoredata Result Codes (Continued)

Code	Description
14	Another application is using the VMware Horizon View Composer 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 View Composer Database

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

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

Prerequisites

By default, Horizon 7 stores the backup files on the `C:` drive of the View 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 View Composer is installed, stop the VMware Horizon View Composer service.
2. Open a Windows command prompt and navigate to the `SviConfig` executable file.

   The file is located with the View Composer application.

   `View-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_View_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 View Composer Database.

Result Codes for Exporting the View Composer Database

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

Table 8-3. 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.

Monitor Horizon 7 Components

You can quickly survey the status of the Horizon 7 and vSphere components in your Horizon 7 deployment by using the Horizon Administrator dashboard.

Horizon Administrator displays monitoring information about Connection Server instances, the event database, security servers, View Composer services, datastores, vCenter Server instances, and domains.

Note Horizon 7 cannot determine status information about Kerberos domains. Horizon Administrator displays Kerberos domain status as unknown, even when a domain is configured and working.

Procedure

1 In Horizon Administrator, click **Dashboard**.

2 In the System Health pane, expand **View components**, **vSphere components**, or **Other components**.

- A green up arrow indicates that a component has no problems.
- A red down arrow indicates that a component is unavailable or not functioning.
- A yellow double arrow indicates that a component is in a warning state.
- A question mark indicates that the status of a component is unknown.

3 Click a component name.

A dialog displays the name, version, status, and other component information.

What to do next

Use vCenter Server to monitor any Virtual SAN clusters and the disks that participate in a Virtual SAN datastore. For more information about monitoring Virtual SAN in vSphere 5.5 Update 1, see the *vSphere Storage* document and the *vSphere Monitoring and Performance* documentation. For more information about monitoring Virtual SAN in vSphere 6 or later, see the *Administering VMware Virtual SAN* document.

Monitor Machine Status

You can quickly survey the status of machines in your Horizon 7 deployment by using the Horizon Administrator dashboard. For example, you can display all disconnected machines or machines that are in maintenance mode.

Prerequisites

Familiarize yourself with the virtual machine status values. For more information about the status of virtual machines, see "Status of vCenter Server Virtual Machines" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

1 In Horizon Administrator, click **Dashboard**.

2 In the Machine Status pane, expand a status folder.

Option	Description
Preparing	Lists the states while the machine is being provisioned, deleted, or in maintenance mode.
Problem Machines	Lists the error states.
Prepared for use	Lists the states when the machine is ready for use.

3 Locate the machine status and click the hyperlinked number next to it.

The **Machines** page displays all machines with the selected status.

What to do next

You can click a machine name to see details about the machine or click the Horizon Administrator back arrow to return to the Dashboard page.

Understanding Horizon 7 Services

The operation of Connection Server instances and security servers depends on several services that run on the system. These systems are started and stopped automatically, but you might sometimes find it necessary to adjust the operation of these services manually.

You use the Microsoft Windows Services tool to stop or start Horizon 7 services. If you stop Horizon 7 services on a Connection Server host or a security server, end users cannot connect to their remote desktops or applications until you restart the services. You might also need to restart a service if it has stopped running or if the Horizon 7 functionality that it controls appears to be unresponsive.

Stop and Start Horizon 7 Services

The operation of Connection Server instances and security servers depends on several services that run on the system. You might sometimes find it necessary to stop and start these services manually when troubleshooting problems with the operation of Horizon 7.

When you stop Horizon 7 services, end users cannot connect to their remote desktops and applications. You should perform such an action at a time that is already scheduled for system maintenance, or warn end users that their desktops and applications will be unavailable temporarily.

Note Stop only the VMware Horizon View Connection Server service on a Connection Server host, or the VMware Horizon View Security Server service on a security server. Do not stop any other component services.

Prerequisites

Familiarize yourself with the services that run on Connection Server hosts and security servers as described in Services on a Connection Server Host and Services on a Security Server.

Procedure

1. Start the Windows Services tool by entering **`services.msc`** at the command prompt.
2. Select the VMware Horizon View Connection Server service on a Connection Server host, or the VMware Horizon View Security Server service on a security server, and click **Stop**, **Restart**, or **Start** as appropriate.
3. Verify that the status of the listed service changes as expected.

Services on a Connection Server Host

The operation of Horizon 7 depends on several services that run on a Connection Server host.

Table 8-4. Horizon Connection Server Host Services

Service Name	Startup Type	Description
VMware Horizon View Blast Secure Gateway	Automatic	Provides secure HTML Access and Blast Extreme services. This service must be running if clients connect to Connection Server through the Blast Secure Gateway.
VMware Horizon View Connection Server	Automatic	Provides connection broker services. This service must always be running. If you start or stop this service, it also starts or stops the Framework, Message Bus, Security Gateway, and Web services. This service does not start or stop the VMwareVDMDS service or the VMware Horizon View Script Host service.
VMware Horizon View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.
VMware Horizon View Message Bus Component	Manual	Provides messaging services between the Horizon 7 components. This service must always be running.
VMware Horizon View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to Connection Server through the PCoIP Secure Gateway.
VMware Horizon View Script Host	Disabled	Provides support for third-party scripts that run when you delete virtual machines. This service is disabled by default. You should enable this service if you want to run scripts.
VMware Horizon View Security Gateway Component	Manual	Provides common gateway services. This service must always be running.
VMware Horizon View Web Component	Manual	Provides web services. This service must always be running.
VMwareVDMDS	Automatic	Provides LDAP directory services. This service must always be running. During upgrades of Horizon 7, this service ensures that existing data is migrated correctly.

Services on a Security Server

The operation of Horizon 7 depends on several services that run on a security server.

Table 8-5. Security Server Services

Service Name	Startup Type	Description
VMware Horizon View Blast Secure Gateway	Automatic	Provides secure HTML Access and Blast Extreme services. This service must be running if clients connect to this security server through the Blast Secure Gateway.
VMware Horizon View Security Server	Automatic	Provides security server services. This service must always be running. If you start or stop this service, it also starts or stops the Framework and Security Gateway services.
VMware Horizon View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.

Table 8-5. Security Server Services (Continued)

Service Name	Startup Type	Description
VMware Horizon View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to this security server through the PCoIP Secure Gateway.
VMware Horizon View Security Gateway Component	Manual	Provides common gateway services. This service must always be running.

Change the Product License Key

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 Administrator to change the product license key.

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 View Composer and published applications, obtain a valid product license key.

Procedure

1 In Horizon Administrator, select **View Configuration > Product Licensing and Usage**.

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

2 Click **Edit License**.

3 Enter the license serial number and click **OK**.

The **Product Licensing** window shows the updated licensing information.

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.

6 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 Product License Usage

In Horizon 7 Administrator, you can monitor the active users who are concurrently connected to Horizon. The **Product Licensing and Usage** page 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 provides two licensing usage models, one for named users and one for concurrent users. Horizon counts the named users and concurrent users in your environment, regardless of your product license edition or usage model agreement.

For named users, Horizon counts the number of unique users that have accessed the Horizon 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 **Product Licensing and Usage** page displays the number of users since your Horizon 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 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 **Product Licensing and Usage** page displays the highest number of concurrent desktop sessions and published desktop and application users since your Horizon 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 Product License Usage Data

In Horizon Administrator, 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 Product License Usage.

Procedure

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

   The highest historical number of named users is reset to 0.

   Note Selecting **Update General User Information** on the **Users and Groups** page also resets the highest historical number of named users to 0.

Update General User Information from Active Directory

You can update Horizon 7 with the current user information that is stored in Active Directory. This feature updates the name, phone, email, user name, and default Windows domain of Horizon 7 users. The trusted external domains are also updated.

Use this feature if you modify the list of trusted external domains in Active Directory, especially if the altered trust relationships between domains affect user permissions in Horizon 7.

This feature scans Active Directory for the latest user information and refreshes the Horizon 7 configuration.

Updating the general user information also resets the number of named users to 0. This number appears on the **Product Licensing and Usage** page in Horizon Administrator. See Reset Product License Usage Data.

You can also use the `vdmadmin` command to update user and domain information. See Updating Foreign Security Principals Using the -F Option.

Prerequisites

Verify that you can log in to Horizon Administrator as an administrator with the **Manage Global Configuration and Policies** privilege.

Procedure

1 In Horizon Administrator, click **Users and Groups**.

2 Choose whether to update information for all users or an individual user.

Option	Action
For all users	Click **Update General User Information**. Updating all users and groups can take a long time.
For an individual user	a Click the user name to update. b Click **Update General User Information**.

Migrate View Composer to Another Machine

In some situations, you might need to migrate a VMware Horizon View Composer service to a new Windows Server virtual or physical machine. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your Horizon 7 deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server machine.

You can migrate View Composer from the vCenter Server machine to a standalone machine or from a standalone machine to the vCenter Server machine.

- Guidelines for Migrating View Composer

  The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

- Migrate View Composer with an Existing Database

  When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

- Migrate View Composer Without Linked-Clone Virtual Machines

  If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

- Prepare a Microsoft .NET Framework for Migrating RSA Keys

  To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

- Migrate the RSA Key Container to the New View Composer Service

  To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

Guidelines for Migrating View Composer

The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

To preserve the linked-clone virtual machines in your deployment, the VMware Horizon View Composer service that you install on the new virtual or physical machine must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new machine.

Whether or not you migrate the View Composer database, the database must be configured on an available machine in the same domain as the new machine on which you install the VMware Horizon View Composer service, or on a trusted domain.

View Composer creates RSA key pairs to encrypt and decrypt authentication information stored in the View Composer database. To make this data source compatible with the new VMware Horizon View Composer service, you must migrate the RSA key container that was created by the original VMware Horizon View Composer service. You must import the RSA key container to the machine on which you install the new service.

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

Note Each instance of the VMware Horizon View Composer service must have its own View Composer database. Multiple VMware Horizon View Composer services cannot share a View Composer database.

Migrate View Composer with an Existing Database

When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server machine to a standalone machine
- From a standalone machine to a vCenter Server machine
- From a standalone machine to another standalone machine
- From a vCenter Server machine to another vCenter Server machine

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server machine that you are migrating as well.

When you install the VMware Horizon View Composer service on the new machine, you must configure the service to connect to the View Composer database.

Prerequisites

- Familiarize yourself with the View Composer migration requirements. See Guidelines for Migrating View Composer.
- Familiarize yourself with the steps for migrating the RSA key container to the new VMware Horizon View Composer service. See Prepare a Microsoft .NET Framework for Migrating RSA Keys and Migrate the RSA Key Container to the New View Composer Service.
- Familiarize yourself with installing the VMware Horizon View Composer service in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring an TLS certificate for View Composer in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring View Composer in Horizon Administrator. See Configure View Composer Settings and Configure View Composer Domains.
- As best practice, verify that the source and destination machines that you use for migrating View Composer are identical and share the same administrator credentials. When you migrate View Composer from a standalone machine to a vCenter Server machine that already has View Composer installed, configuring View Composer might fail if the credentials used on the two machines are different.

Procedure

1. Disable virtual machine provisioning in the vCenter Server instance that is associated with the VMware Horizon View Composer service.
   a. In Horizon Administrator, select **View Configuration > Servers**.
   b. On the **vCenter Servers** tab, select the vCenter Server instance and click **Disable Provisioning**.
2. (Optional) Migrate the View Composer database to a new location.

   If you need to take this step, consult your database administrator for migration instructions.
3. Uninstall the VMware Horizon View Composer service from the current machine.
4. (Optional) Migrate the RSA key container to the new machine.
5. Install the VMware Horizon View Composer service on the new machine.

   During the installation, specify the DSN of the database that was used by the original VMware Horizon View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.

   If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new VMware Horizon View Composer service must have access to the original database information about the linked clones.

6 Configure an SSL server certificate for View Composer on the new machine.

   You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.

7 In Horizon Administrator, configure the new View Composer settings.

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

   b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.

   c In the View Composer Server Settings pane, click **Edit** and provide the new View Composer settings.

      If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

      If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

   d In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.

   e Click **OK**.

Migrate View Composer Without Linked-Clone Virtual Machines

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

Prerequisites

- Familiarize yourself with installing the VMware Horizon View Composer service in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring a TLS certificate for View Composer in the *Horizon 7 Installation* document.
- Familiarize yourself with the steps for removing View Composer from Horizon Administrator. See Remove View Composer from Horizon 7.

  Before you can remove View Composer, verify that it no longer manages any linked-clone desktops. If any linked clones remain, you must delete them.
- Familiarize yourself with configuring View Composer in Horizon Administrator. See Configure View Composer Settings and Configure View Composer Domains.

Procedure

1 In Horizon Administrator, remove View Composer from Horizon Administrator.
   a Select **View Configuration > Servers**.
   b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with the View Composer service and click **Edit**.
   c In the View Composer Server Settings pane, click **Edit**.
   d Select **Do not use View Composer** and click **OK**.
2 Uninstall the VMware Horizon View Composer service from the current machine.
3 Install the VMware Horizon View Composer service on the new machine.

   During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.
4 Configure a TLS server certificate for View Composer on the new machine.

   You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.
5 In Horizon Administrator, configure the new View Composer settings.
   a In Horizon Administrator, select **View Configuration > Servers**.
   b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.
   c In the View Composer Server Settings pane, click **Edit**.
   d Provide the new View Composer settings.

      If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

      If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.
   e In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
   f Click **OK**.

Prepare a Microsoft .NET Framework for Migrating RSA Keys

To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool. Go to http://www.microsoft.com/net.

Procedure

1. Install the .NET Framework on the physical or virtual machine on which the VMware Horizon View Composer service associated with the existing database is installed.
2. Install the .NET Framework on the destination machine on which you want to want to install the new VMware Horizon View Composer service.

What to do next

Migrate the RSA key container to the destination machine. See Migrate the RSA Key Container to the New View Composer Service.

Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

You must perform this procedure before you install the new VMware Horizon View Composer service.

Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination machines. See Prepare a Microsoft .NET Framework for Migrating RSA Keys.

Procedure

1. On the source machine on which the existing VMware Horizon View Composer service resides, open a command prompt and navigate to the `%windir%\Microsoft.NET\Framework\v2.0xxxxx` directory.
2. Type the `aspnet_regiis` command to save the RSA key pair in a local file.

   ```
   aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
   ```

   The ASP.NET IIS registration tool exports the RSA public-private key pair from the `SviKeyContainer` container to the `keys.xml` file and saves the file locally.
3. Copy the `keys.xml` file to the destination machine on which you want to install the new VMware Horizon View Composer service.
4. On the destination machine, open a command prompt and navigate to the `%windir%\Microsoft.NET\Framework\v2.0xxxxx` directory.

5 Type the `aspnet_regiis` command to migrate the RSA key pair data.

`aspnet_regiis –pi "SviKeyContainer" "`*`path`*`\keys.xml" –exp`

where *path* is the path to the exported file.

The `–exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this machine and imported to another machine. If you previously migrated the keys to this machine without using the `–exp` option, you can import the keys again using the `–exp` option so that you can export the keys in the future.

The registration tool imports the key pair data into the local key container.

What to do next

Install the new VMware Horizon View Composer service on the destination machine. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original VMware Horizon View Composer service. For installation instructions, see "Installing View Composer" in the *Horizon 7 Installation* document.

Complete the steps to migrate View Composer to a new machine and use the same database. See Migrate View Composer with an Existing Database.

Update the Certificates on a Connection Server Instance, Security Server, or View Composer

When you receive updated server TLS certificates or intermediate certificates, you import the certificates into the Windows local computer certificate store on each Connection Server, security server, or View Composer host.

Typically, server certificates expire after 12 months. Root and intermediate certificates expire after 5 or 10 years.

For detailed information about importing server and intermediate certificates, see "Configure Horizon Connection Server, Security Server, or View Composer to Use a New TLS Certificate" in the *Horizon 7 Installation* document.

Prerequisites

- Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.
- Verify that the Certificate snap-in was added to MMC on the Windows Server on which the Connection Server instance, security server, or VMware Horizon View Composer service was installed.

Procedure

1. Import the signed TLS server certificate into the Windows local computer certificate store on the Windows Server host.
   a. In the Certificate snap-in, import the server certificate into the **Certificates (Local Computer) > Personal > Certificates** folder.
   b. Select **Mark this key as exportable**.
   c. Click **Next** and click **Finish**.
2. For Connection Server or security server, delete the certificate Friendly name, **vdm**, from the old certificate that was issued to the Horizon 7 server.
   a. Right-click the old certificate and click **Properties**
   b. On the General tab, delete the Friendly name text, **vdm**.
3. For Connection Server or security server, add the certificate Friendly name, **vdm**, to the new certificate that is replacing the previous certificate.
   a. Right-click the new certificate and click **Properties**
   b. On the General tab, in the Friendly name field, type **vdm**.
   c. Click **Apply** and click **OK**.
4. For a server certificate that is issued to View Composer, run the `SviConfig ReplaceCertificate` utility to bind the new certificate to the port used by View Composer.

   This utility replaces the old certificate binding with the new certificate binding.
   a. Stop the VMware Horizon View Composer service.
   b. Open a Windows command prompt and navigate to the `SviConfig` executable file.

      The file is located with the View Composer application. The default path is `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.
   c. Type the `SviConfig ReplaceCertificate` command. For example:

      ```
      sviconfig –operation=ReplaceCertificate
                –delete=false
      ```

      The utility displays a numbered list of TLS certificates that are available in the Windows local computer certificate store.
   d. To select a certificate, type the number of the certificate and press Enter.
5. If intermediate certificates are issued to a Connection Server, security server, or View Composer host, import the most recent update to the intermediate certificates into the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder in the Windows certificate store.
6. Restart the VMware Horizon View Connection Server service, VMware Horizon View Security Server service, or VMware Horizon View Composer service to make your changes take effect.

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 Administrator, select **View Configuration > Product Licensing and Usage**.
2. In the **Customer Experience Program** panel, 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. Click **OK**.

Managing ThinApp Applications in Horizon Administrator

9

You can use Horizon Administrator to distribute and manage applications packaged with VMware ThinApp. Managing ThinApp applications in Horizon Administrator involves capturing and storing application packages, adding ThinApp applications to Horizon Administrator, and assigning ThinApp applications to machines and desktop pools.

You must have a license to use the ThinApp management feature in Horizon Administrator.

Important If, instead of distributing ThinApps by assigning them to machines and desktop pools, you would rather assign ThinApps to Active Directory users and groups, you can use VMware Identity Manager.

This chapter includes the following topics:

Horizon 7 Requirements for ThinApp Applications

When capturing and storing ThinApp applications that will be distributed to remote desktops in Horizon Administrator, you must meet certain requirements.

- You must package your applications as Microsoft Installation (MSI) packages.
- You must use ThinApp version 4.6 or later to create or repackage the MSI packages.
- You must store the MSI packages on a Windows network share that resides in an Active Directory domain that is accessible to your Connection Server host and remote desktops. The file server must support authentication and file permissions that are based on computer accounts.

- You must configure the file and sharing permissions on the network share that hosts the MSI packages to give Read access to the built-in Active Directory group Domain Computers. If you plan to distribute ThinApp applications to domain controllers, you must also give Read access to the built-in Active Directory group Domain Controllers.
- To allow users access to streaming ThinApp application packages, you must set the NTFS permission of the network share that hosts the ThinApp packages to `Read&Execute` for users.
- Make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the MSI packages. A disjoint namespace occurs when an Active Directory domain name is different from the DNS namespace that is used by machines in that domain. See VMware Knowledge Base (KB) article 1023309 for more information.
- To run streamed ThinApp applications on remote desktops, users must have access to the network share that hosts the MSI packages.

Capturing and Storing Application Packages

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package.

To manage ThinApp applications in Horizon Administrator, you must use the ThinApp **Setup Capture** wizard to capture and package your applications in MSI format and store the MSI packages in an application repository.

An application repository is a Windows network share. You use Horizon Administrator to register the network share as an application repository. You can register multiple application repositories.

Note If you have multiple application repositories, you can use third-party solutions to manage load balancing and availability. Horizon 7 does not include load balancing or availability solutions.

See the *Introduction to VMware ThinApp* and the *ThinApp User's Guide* for complete information on ThinApp features and how to use the ThinApp **Setup Capture** wizard.

1 Package Your Applications

   You use the ThinApp **Setup Capture** wizard to capture and package your applications.

2 Create a Windows Network Share

   You must create a Windows network share to host the MSI packages that are distributed to remote desktops and pools in Horizon Administrator.

3 Register an Application Repository

   You must register the Windows network share that hosts your MSI packages as an application repository in Horizon Administrator.

4 Add ThinApp Applications to Horizon Administrator

   You add ThinApp applications to Horizon Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to Horizon Administrator, you can assign it to machines and desktop pools.

5 Create a ThinApp Template

You can create a template in Horizon Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

Package Your Applications

You use the ThinApp **Setup Capture** wizard to capture and package your applications.

Prerequisites

- Download the ThinApp software from http://www.vmware.com/products/thinapp and install it on a clean computer. View supports ThinApp version 4.6 and later.
- Familiarize yourself with the ThinApp software requirements and application packaging instructions in the *ThinApp User's Guide*.

Procedure

1. Start the ThinApp **Setup Capture** wizard and follow the prompts in the wizard.
2. When the ThinApp **Setup Capture** wizard prompts you for a project location, select **Build MSI package**.
3. If you plan to stream the application to remote desktops, set the MSIStreaming property to 1 in the `package.ini` file.

```
MSIStreaming=1
```

The ThinApp **Setup Capture** wizard encapsulates the application, all of the necessary components to run the application, and the application itself into an MSI package.

What to do next

Create a Windows network share to store the MSI packages.

Create a Windows Network Share

You must create a Windows network share to host the MSI packages that are distributed to remote desktops and pools in Horizon Administrator.

Prerequisites

- Use the ThinApp **Setup Capture** wizard to package the applications.
- Verify that the network share meets Horizon 7 requirements for storing ThinApp applications. See Horizon 7 Requirements for ThinApp Applications for more information.

Procedure

1. Create a shared folder on a computer in an Active Directory domain that it accessible to both your Connection Server host and remote desktops.

2 Configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.

3 If you plan to assign ThinApp applications to domain controllers, give Read access to the built-in Active Directory group Domain Controllers.

4 If you plan to use streaming ThinApp application packages, set the NTFS permission of the network share that hosts the ThinApp packages to `Read&Execute` for users.

5 Copy your MSI packages to the shared folder.

What to do next

Register the Windows network share as an application repository in Horizon Administrator.

Register an Application Repository

You must register the Windows network share that hosts your MSI packages as an application repository in Horizon Administrator.

You can register multiple application repositories.

Prerequisites

Create a Windows network share.

Procedure

1 In Horizon Administrator, select **View Configuration > ThinApp Configuration** and click **Add Repository**.

2 Type a display name for the application repository in the **Display name** text box.

3 Type the path to the Windows network share that hosts your application packages in the **Share path** text box.

The network share path must be in the form *ServerComputerName**ShareName* where *ServerComputerName* is the DNS name of the server computer. Do not specify an IP address.

For example: `\\server.domain.com\MSIPackages`

4 Click **Save** to register the application repository with Horizon Administrator.

Add ThinApp Applications to Horizon Administrator

You add ThinApp applications to Horizon Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to Horizon Administrator, you can assign it to machines and desktop pools.

Prerequisites

Register an application repository with Horizon Administrator.

Procedure

1. In Horizon Administrator, select **Catalog > ThinApps**.
2. On the **Summary** tab, click **Scan New ThinApps**.
3. Select an application repository and a folder to scan and click **Next**.

   If the application repository contains subfolders, you can expand the root folder and select a subfolder.
4. Select the ThinApp applications that you want to add to Horizon Administrator.

   You can press Ctrl+click or Shift+click to select multiple ThinApp applications.
5. Click **Scan** to begin scanning the MSI packages that you selected.

   You can click **Stop Scan** if you need to stop the scan.

   Horizon Administrator reports the status of each scanning operation and the number of ThinApp applications that were added to Horizon Administrator. If you select an application that is already in Horizon Administrator, it is not added again.
6. Click **Finish**.

   The new ThinApp applications appear on the **Summary** tab.

What to do next

(Optional) Create ThinApp templates.

Create a ThinApp Template

You can create a template in Horizon Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

With ThinApp templates, you can streamline the distribution of multiple applications. When you assign a ThinApp template to a machine or desktop pool, Horizon Administrator installs all of the applications that are currently in the template.

Creating ThinApp templates is optional.

Note If you add an application to a ThinApp template after assigning the template to a machine or desktop pool, Horizon Administrator does not automatically assign the new application to the machine or desktop pool. If you remove an application from a ThinApp template that was previously assigned to a machine or desktop pool, the application remains assigned to the machine or desktop pool.

Prerequisites

Add selected ThinApp applications to Horizon Administrator.

Procedure

1. In Horizon Administrator, select **Catalog > ThinApps** and click **New Template**.

2 Type a name for the template and click **Add**.

All of the available ThinApp applications appear in the table.

3 To find a particular ThinApp application, type the name of the application in the **Find** text box and click **Find**.

4 Select the ThinApp applications that you want to include in the template and click **Add**.

You can press Ctrl+click or Shift+click to select multiple applications.

5 Click **OK** to save the template.

Assigning ThinApp Applications to Machines and Desktop Pools

To install a ThinApp application on a remote desktop, you use Horizon Administrator to assign the ThinApp application to a machine or desktop pool.

When you assign a ThinApp application to a machine, Horizon Administrator begins installing the application on the virtual machine a few minutes later. When you assign a ThinApp application to a desktop pool, Horizon Administrator begins installing the application the first time a user logs in to a remote desktop in the pool.

Streaming	Horizon Administrator installs a shortcut to the ThinApp application on the remote desktop. The shortcut points to the ThinApp application on the network share that hosts the repository. Users must have access to the network share to run streamed ThinApp applications.
Full	Horizon Administrator installs the full ThinApp application on the local file system.

The amount of time it takes to install a ThinApp application depends on the size of the application.

Important You can assign ThinApp applications to virtual machine-based desktops and automated desktop pools or manual pools that contains vCenter Server virtual machines. You cannot assign ThinApp applications to published desktops or traditional PCs.

- Best Practices for Assigning ThinApp Applications

  Follow best practices when you assign ThinApp applications to machines and desktop pools.
- Assign a ThinApp Application to Multiple Machines

  You can assign a particular ThinApp to one or more machines.
- Assign Multiple ThinApp Applications to a Machine

  You can assign one or more ThinApp applications to a particular machine.
- Assign a ThinApp Application to Multiple Desktop Pools

  You can assign a particular ThinApp application to one or more desktop pools.

- Assign Multiple ThinApp Applications to a Desktop Pool

  You can assign one more ThinApp applications to a particular desktop pool.

- Assign a ThinApp Template to a Machine or Desktop Pool

  You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a machine or desktop pool.

- Review ThinApp Application Assignments

  You can review all of the machines and desktop pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular machine or desktop pool.

- Display MSI Package Information

  After you add a ThinApp application to Horizon Administrator, you can display information about its MSI package.

Best Practices for Assigning ThinApp Applications

Follow best practices when you assign ThinApp applications to machines and desktop pools.

- To install a ThinApp application on a particular remote desktop, assign the application to the virtual machine that hosts the desktop. If you use a common naming convention for your machines, you can use machine assignments to quickly distribute applications to all of the machines that use that naming convention.
- To install a ThinApp application on all of the machines in a desktop pool, assign the application to the desktop pool. If you organize your desktop pools by department or user type, you can use desktop pool assignments to quickly distribute applications to specific departments or users. For example, if you have a desktop pool for your accounting department users, you can distribute the same application to all of the users in your accounting department by assigning the application to the accounting pool.
- To streamline the distribution of multiple ThinApp applications, include the applications in a ThinApp template. When you assign a ThinApp template to a machine or desktop pool, Horizon Administrator installs all of the applications currently in the template.
- Do not assign a ThinApp template to a machine or desktop pool if the template contains a ThinApp application that is already assigned to that machine or desktop pool. Also, do not assign a ThinApp template to the same machine or desktop pool more than once with a different installation type. Horizon Administrator will return ThinApp assignment errors in both of these situations.

Assign a ThinApp Application to Multiple Machines

You can assign a particular ThinApp to one or more machines.

Prerequisites

Scan an application repository and add selected ThinApp applications to Horizon Administrator. See Add ThinApp Applications to Horizon Administrator.

Procedure

1. In Horizon Administrator, select **Catalog > ThinApps** and select the ThinApp application.
2. Select **Assign Machines** from the **Add Assignment** drop-down menu.

   The machines that the ThinApp application is not already assigned to appear in the table.

Option	Action
Find a specific machine	Type the name of the machine in the **Find** text box and click **Find**.
Find all of the machines that follow the same naming convention	Type a partial machine name in the **Find** text box and click **Find**.

3. Select the machines that you want to assign the ThinApp application to and click **Add**.

   You can press Ctrl+click or Shift+click to select multiple machines.
4. Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

   Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

Horizon Administrator begins installing the ThinApp application a few minutes later. After the installation is finished, the application is available to all of the users of the desktops hosted by the virtual machines.

Assign Multiple ThinApp Applications to a Machine

You can assign one or more ThinApp applications to a particular machine.

Prerequisites

Scan an application repository and add selected ThinApp applications to Horizon Administrator. See Add ThinApp Applications to Horizon Administrator.

Procedure

1. In Horizon Administrator, select **Resources > Machines** and double-click the name of the machine in the Machine column.
2. On the **Summary** tab, click **Add Assignment** in the ThinApps pane.

   The ThinApp applications that are not already assigned to the machine appear in the table.
3. To find a particular application, type the name of the application in the **Find** text box and click **Find**.
4. Select a ThinApp application to assign to the machine and click **Add**.

   Repeat this step to add multiple applications.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

Horizon Administrator begins installing the ThinApp applications a few minutes later. After the installation is finished, the applications are available to all of the users of the desktop that is hosted by the virtual machine.

Assign a ThinApp Application to Multiple Desktop Pools

You can assign a particular ThinApp application to one or more desktop pools.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, Horizon Administrator reinstalls the application for you. You do not have to manually reinstall the application.

Prerequisites

Scan an application repository and add selected ThinApp applications to Horizon Administrator. See Add ThinApp Applications to Horizon Administrator.

Procedure

1 In Horizon Administrator, select **Catalog > ThinApps** and select the ThinApp application.

2 Select **Assign Desktop Pools** from the **Add Assignment** drop-down menu.

The desktop pools that the ThinApp application is not already assigned to appear in the table.

Option	Action
Find a specific desktop pool	Type the name of the desktop pool in the **Find** text box and click **Find**.
Find all of the desktop pools that follow the same naming convention	Type a partial desktop pool name in the **Find** text box and click **Find**.

3 Select the desktop pools that you want to assign the ThinApp application to and click **Add**.

You can press Ctrl+click or Shift+click to select multiple desktop pools.

4 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

Horizon Administrator begins installing the ThinApp application the first time a user logs in to a desktop in the pool. After the installation is finished, the application is available to all of the users of the desktop pool.

Assign Multiple ThinApp Applications to a Desktop Pool

You can assign one more ThinApp applications to a particular desktop pool.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, Horizon Administrator reinstalls the application for you. You do not have to manually reinstall the application.

Prerequisites

Scan an application repository and add selected ThinApp applications to Horizon Administrator. See Add ThinApp Applications to Horizon Administrator.

Procedure

1 In Horizon Administrator, select **Catalog > Desktop Pools** and double-click the pool ID.

2 On the **Inventory** tab, click **ThinApps** and then click **Add Assignment**.

The ThinApp applications that are not already assigned to the pool appear in the table.

3 To find a particular application, type the name of the ThinApp application in the **Find** text box and click **Find**.

4 Select a ThinApp application to assign to the pool and click **Add**.

Repeat this step to select multiple applications.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

Horizon Administrator begins installing the ThinApp applications the first time a user logs in to a desktop in the pool. After the installation is finished, the applications are available to all of the users of the desktop pool.

Assign a ThinApp Template to a Machine or Desktop Pool

You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a machine or desktop pool.

When you assign a ThinApp template to a machine or desktop pool, Horizon Administrator installs the ThinApp applications currently in the template.

Prerequisites

Create a ThinApp template. See Create a ThinApp Template.

Procedure

1 In Horizon Administrator, select **Catalog > ThinApps**.

2 Select the ThinApp template.

3 Select **Assign Machines** or **Assign Desktop Pools** from the **Add Assignment** drop-down menu.

All machines or desktop pools appear in the table.

Option	Action
Find a specific machine or desktop pool	Type the name of the machine or desktop pool in the **Find** text box and click **Find**.
Find all of the machines or desktop pools that follow the same naming convention	Type a partial machine or desktop pool name in the **Find** text box and click **Find**.

4 Select the machines or desktop pools that you want to assign the ThinApp template to and click **Add**.

Repeat this step to select multiple machines or desktop pools.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

When you assign a ThinApp template to a machine, Horizon Administrator begins installing the applications in the template a few minutes later. When you assign a ThinApp template to a desktop pool, Horizon Administrator begins installing the applications in the template the first time a user logs in to a remote desktop in the desktop pool. After the installation is finished, the applications are available to all of the users of the machine or desktop pool.

Horizon Administrator returns an application assignment error if a ThinApp template contains an application that is already assigned to the machine or desktop pool.

Review ThinApp Application Assignments

You can review all of the machines and desktop pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular machine or desktop pool.

Prerequisites

Familiarize yourself with the ThinApp installation status values in ThinApp Application Installation Status Values.

Procedure

- Select the ThinApp application assignments that you want to review.

Option	Action
Review all of the machines and desktop pools that a particular ThinApp application is assigned to	Select **Catalog > ThinApps** and double-click the name of the ThinApp application. The **Assignments** tab shows the machines and desktop pools that the application is currently assigned to, including the installation type. The **Machines** tab shows the machines that are currently associated with the application, including installation status information. **Note** When you assign a ThinApp application to a pool, machines in the pool appear on the **Machines** tab only after the application is installed.
Review all of the ThinApp applications that are assigned to a particular machine	Select **Resources > Machines** and double-click the name of the machine in Machine column. The ThinApps pane on **Summary** tab shows each application that is currently assigned to the machine, including the installation status.
Review all of the ThinApp applications that are assigned to a particular desktop pool	Select **Catalog > Desktop Pools**, double-click the pool ID, select the **Inventory** tab, and click **ThinApps**. The ThinApp Assignments pane shows each application that is currently assigned to the desktop pool.

ThinApp Application Installation Status Values

After you assign a ThinApp application to a machine or pool, Horizon Administrator indicates the status of the installation.

The following table describes each status value.

Table 9-1. ThinApp Application Installation Status

Status	Description
Assigned	The ThinApp application is assigned to the machine.
Install Error	An error occurred when Horizon Administrator attempted to install the ThinApp application.
Uninstall Error	An error occurred when Horizon Administrator attempted to uninstall the ThinApp application.
Installed	The ThinApp application is installed.
Pending Install	Horizon Administrator is attempting to install the ThinApp application. You cannot unassign an application that has this status. **Note** This value does not appear for machines in desktop pools.
Pending Uninstall	Horizon Administrator is attempting to uninstall the ThinApp application.

Display MSI Package Information

After you add a ThinApp application to Horizon Administrator, you can display information about its MSI package.

Procedure

1. In Horizon Administrator, select **Catalog > ThinApps**.

   The **Summary** tab lists the applications that are currently available and shows the number of full and streaming assignments.
2. Double-click the name of the application in the ThinApp column.
3. Select the **Summary** tab to see general information about the MSI package.
4. Click **Package Info** to see detailed information about the MSI package.

Maintaining ThinApp Applications in Horizon Administrator

Maintaining ThinApp applications in Horizon Administrator involves tasks such as removing ThinApp application assignments, removing ThinApp applications and application repositories, and modifying and deleting ThinApp templates.

Note To upgrade a ThinApp application, you must unassign and remove the older version of the application and add and assign the newer version.

- Remove a ThinApp Application Assignment from Multiple Machines

  You can remove an assignment to a particular ThinApp application from one or more machines.
- Remove Multiple ThinApp Application Assignments from a Machine

  You can remove assignments to one or more ThinApp applications from a particular machine.
- Remove a ThinApp Application Assignment from Multiple Desktop Pools

  You can remove an assignment to a particular ThinApp application from one or more desktop pools.

- Remove Multiple ThinApp Application Assignments from a Desktop Pool

  You can remove one or more ThinApp application assignments from a particular desktop pool.
- Remove a ThinApp Application from Horizon Administrator

  When you remove a ThinApp application from Horizon Administrator, you can no longer assign the application to machinse and desktop pools.
- Modify or Delete a ThinApp Template

  You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.
- Remove an Application Repository

  You can remove an application repository from Horizon Administrator.

Remove a ThinApp Application Assignment from Multiple Machines

You can remove an assignment to a particular ThinApp application from one or more machines.

Prerequisites

Notify the users of the remote desktops that are hosted by the machines that you intend to remove the application.

Procedure

1. In Horizon Administrator, select **Catalog > ThinApps** and double-click the name of the ThinApp application.
2. On the **Assignments** tab, select a machine and click **Remove Assignment**.

   You can press Ctrl+click or Shift+click to select multiple machines.

Horizon Administrator uninstalls the ThinApp application a few minutes later.

Important If an end user is using the ThinApp application at the time when Horizon Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the machine and then click **Remove App Status for Desktop** in Horizon Administrator.

Remove Multiple ThinApp Application Assignments from a Machine

You can remove assignments to one or more ThinApp applications from a particular machine.

Prerequisites

Notify the users of the remote desktop that is hosted by the machine that you intend to remove the applications.

Procedure

1 In Horizon Administrator, select **Resources > Machines** and double-click the name of the machine in the Machine column.

2 On the **Summary** tab, select the ThinApp application and click **Remove Assignment** in the ThinApps pane.

Repeat this step to remove another application assignment.

Horizon Administrator uninstalls the ThinApp application a few minutes later.

Important If an end user is using the ThinApp application at the time when Horizon Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the machine and then click **Remove App Status For Desktop** in Horizon Administrator.

Remove a ThinApp Application Assignment from Multiple Desktop Pools

You can remove an assignment to a particular ThinApp application from one or more desktop pools.

Prerequisites

Notify the users of the remote desktops in the pools that you intend to remove the application.

Procedure

1 In Horizon Administrator, select **Catalog > ThinApps** and double-click the name of the ThinApp application.

2 On the **Assignments** tab, select a desktop pool and click **Remove Assignment**.

You can press Ctrl+click or Shift+click to select multiple desktop pools.

Horizon Administrator uninstalls the ThinApp application the first time a user logs in to a remote desktop in the pool.

Remove Multiple ThinApp Application Assignments from a Desktop Pool

You can remove one or more ThinApp application assignments from a particular desktop pool.

Prerequisites

Notify the users of the remote desktops in the pool that you intend to remove the applications.

Procedure

1 In Horizon Administrator, select **Catalog > Desktop Pools** and double-click the pool ID.

2 On the **Inventory** tab, click **ThinApps**, select the ThinApp application, and click **Remove Assignment**.

Repeat this step to remove multiple applications.

Horizon Administrator uninstalls the ThinApp applications the first time a user logs in to a remote desktop in the pool.

Remove a ThinApp Application from Horizon Administrator

When you remove a ThinApp application from Horizon Administrator, you can no longer assign the application to machinse and desktop pools.

You might need to remove a ThinApp application if your organization decides to replace it with a different vendor's application.

Note You cannot remove a ThinApp application if it is already assigned to a machine or desktop pool or if it is in the Pending Uninstall state.

Prerequisites

If a ThinApp application is currently assigned to a machine or desktop pool, remove the assignment from the machine or desktop pool.

Procedure

1 In Horizon Administrator, select **Catalog > ThinApps** and select the ThinApp application.

2 Click **Remove ThinApp**.

3 Click **OK**.

Modify or Delete a ThinApp Template

You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.

If you add an application to a ThinApp template after assigning the template to a machine or desktop pool, Horizon Administrator does not automatically assign the new application to the machine or desktop pool. If you remove an application from a ThinApp template that was previously assigned to a machine or desktop pool, the application remains assigned to the machine or desktop pool.

Procedure

◆ In Horizon Administrator, select **Catalog > ThinApps** and select the ThinApp template.

Option	Action
Add or remove ThinApp applications from the template	Click **Edit Template**.
Delete the template	Click **Remove Template**.

Remove an Application Repository

You can remove an application repository from Horizon Administrator.

You might need to remove an application repository if you no longer need the MSI packages that it contains, or if you need to move the MSI packages to a different network share. You cannot edit the share path of an application repository in Horizon Administrator.

Procedure

1. In Horizon Administrator, select **View Configuration > ThinApp Configuration** and select the application repository.
2. Click **Remove Repository**.

Monitoring and Troubleshooting ThinApp Applications in Horizon Administrator

Horizon Administrator logs events that are related to ThinApp application management to the Events and Reporting database. You can view these events on the **Events** page in Horizon Administrator.

An event appears on the **Events** page when the following situations occur.

- A ThinApp application is assigned or an application assignment is removed
- A ThinApp application is installed or uninstalled on a machine
- A ThinApp application cannot be installed or uninstalled
- A ThinApp application repository is registered, modified, or removed from Horizon Administrator
- A ThinApp application is added to Horizon Administrator

Troubleshooting tips are available for common ThinApp application management problems.

Cannot Register an Application Repository

You cannot register an application repository in Horizon Administrator.

Problem

You receive an error message when you attempt to register an application repository in Horizon Administrator.

Cause

The Connection Server host cannot access the network share that hosts the application repository. The network share path that you typed in the **Share path** text box might be incorrect, the network share that hosts the application repository is in a domain that is not accessible from the Connection Server host, or the network share permissions have not been set up properly.

Solution

- If the network share path is incorrect, type the correct network share path. Network share paths that contain IP addresses are not supported.
- If the network share is not in an accessible domain, copy your application packages to a network share in a domain that is accessible from the Connection Server host.
- Verify that the file and sharing permissions on the shared folder give Read access to the built-in Active Directory group Domain Computers. If you plan to assign ThinApps to domain controllers, verify that the file and sharing permissions also give Read access to the built-in Active Directory group Domain Controllers. After you set or change permissions, it can take up to 20 minutes for the network share to become accessible.

Cannot Add ThinApp Applications to Horizon Administrator

Horizon Administrator cannot add ThinApp applications to Horizon Administrator.

Problem

No MSI packages are available when you click **Scan New ThinApps** in Horizon Administrator.

Cause

Either the application packages are not in MSI format or the Connection Server host cannot access the directories in the network share.

Solution

- Verify that the application packages in the application repository are in MSI format.
- Verify that the network share meets Horizon 7 requirements for ThinApp applications. See Horizon 7 Requirements for ThinApp Applications for more information.
- Verify that the directories in the network share have the proper permissions. See Cannot Register an Application Repository for more information.

Messages appear in the Connection Server debug log file when an application repository is scanned. Connection Server log files are located on the Connection Server host in the *drive*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` directory.

Cannot Assign a ThinApp Template

You cannot assign a ThinApp template to a machine or desktop pool.

Problem

Horizon Administrator returns an assignment error when you attempt to assign a ThinApp template to a machine or desktop pool.

Cause

Either the ThinApp template contains an application that is already assigned to the machine or desktop pool, or the ThinApp template was previously assigned to the machine or desktop pool with a different installation type.

Solution

If the template contains a ThinApp application that is already assigned to the machine or desktop pool, create a new template that does not contain the application or edit the existing template and remove the application. Assign the new or modified template to the machine or desktop pool.

To change the installation type of a ThinApp application, you must remove the existing application assignment from the machine or desktop pool. After the ThinApp application is uninstalled, you can assign it to the machine or desktop pool with a different installation type.

ThinApp Application Is Not Installed

Horizon Administrator cannot install a ThinApp application.

Problem

The ThinApp application installation status shows either Pending Install or Install Error.

Cause

Common causes for this problem include the following:

- There was not enough disk space on the machine to install the ThinApp application.
- Network connectivity was lost between the Connection Server host and the machine or between the Connection Server host and the application repository.
- The ThinApp application was not accessible in the network share.
- The ThinApp application was previously installed or the directory or file already exists on the machine.

You can see the Horizon Agent and Connection Server log files for more information about the cause of the problem.

Horizon Agent log files are located on the machine in *drive*:\ProgramData\VMware\VDM\logs.

Connection Server log files are located on the Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

Solution

1. In Horizon Administrator, select **Catalog > ThinApps**.
2. Click the name of the ThinApp application.
3. On the **Machines** tab, select the machine and click **Retry Install** to reinstall the ThinApp application.

ThinApp Application Is Not Uninstalled

Horizon Administrator cannot uninstall a ThinApp application.

Problem

The ThinApp application installation status shows Uninstall Error.

Cause

Common causes for this error include the following:

- The ThinApp application was busy when Horizon Administrator tried to uninstall it.
- Network connectivity was lost between the Connection Server host and the machine.

You can see the Horizon Agent and Connection Server log files for more information about the cause of the problem.

Horizon Agent log files are located on the machine in *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs for Windows XP systems and *drive*:\ProgramData\VMware\VDM\logs for Windows 7 systems.

Connection Server log files are located on the Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

Solution

1. In Horizon Administrator, select **Catalog > ThinApps**.
2. Click the name of the ThinApp application.
3. Click the **Machines** tab, select the machine, and click **Retry Uninstall** to retry the uninstall operation.
4. If the uninstall operation still fails, manually remove the ThinApp application from the machine and then click **Remove App Status For Desktop**.

   This command clears the ThinApp application assignment in Horizon Administrator. It does not remove any files or settings in the machine.

   Important Use this command only after manually removing the ThinApp application from the machine.

MSI Package Is Invalid

Horizon Administrator reports an invalid MSI package in an application repository.

Problem

Horizon Administrator reports that an MSI package is invalid during a scanning operation.

Cause

Common causes of this problem include the following:

- The MSI file is corrupted.
- The MSI file was not created with ThinApp.
- The MSI file was created or repackaged with an unsupported version of ThinApp. You must use ThinApp version 4.6 or later.

Solution

See the *ThinApp User's Guide* for information on troubleshooting problems with MSI packages.

ThinApp Configuration Example

The ThinApp configuration example takes you step-by-step through a typical ThinApp configuration, beginning with capturing and packaging applications and ending with checking the status of an installation.

Prerequisites

See these topics for complete information about how to perform the steps in this example.

- Capturing and Storing Application Packages
- Assigning ThinApp Applications to Machines and Desktop Pools

Procedure

1. Download the ThinApp software from http://www.vmware.com/products/thinapp and install it on a clean computer.

   Horizon 7 supports ThinApp version 4.6 and later.
2. Use the ThinApp **Setup Capture** wizard to capture and package your applications in MSI format.
3. Create a shared folder on a computer in an Active Directory domain that it accessible to both your Connection Server host and your remote desktops and configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.

   If you plan to assign ThinApp applications to domain controllers, also give Read access to the built-in Active Directory group Domain Controllers.
4. Copy your MSI packages to the shared folder.
5. Register the shared folder as an application repository in Horizon Administrator.
6. In Horizon Administrator, scan the MSI packages in the application repository and add selected ThinApp applications to Horizon Administrator.

7 Decide whether to assign the ThinApp applications to machines or desktop pools.

If you use a common naming convention for your machines, you can use machine assignments to quickly distribute applications to all of the machines that use that naming convention. If you organize your desktop pools by department or user type, you can use desktop pool assignments to quickly distribute applications to specific departments or users.

8 In Horizon Administrator, select the ThinApp applications to assign to your machines or desktop pools and specify the installation method.

Option	Action
Streaming	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the machine's local file system.

9 In Horizon Administrator, check the installation status of the ThinApp applications.

Setting Up Clients in Kiosk Mode

10

You can set up unattended clients that can obtain access to their desktops from Horizon 7.

A client in kiosk mode is a thin client or a lock-down PC that runs Horizon Client to connect to a Connection Server instance and launch a session. End users do not typically need to log in to access the client device, although the published desktop might require them to provide authentication information for some applications. Sample applications include medical data entry workstations, airline check-in stations, customer self-service points, and information terminals for public access.

You should ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

Clients in kiosk mode support the standard features for remote access such as automatic redirection of USB devices to the remote session and location-based printing.

Horizon 7 uses the Flexible Authentication feature in Horizon 7 4.5 and later to authenticate a client device in kiosk mode rather than the end user. You can configure a Connection Server instance to authenticate clients that identify themselves by their MAC address or by a user name that starts with the characters "custom-" or with an alternate prefix string that you have defined in ADAM. If you configure a client to have an automatically generated password, you can run Horizon Client on the device without specifying a password. If you configure an explicit password, you must specify this password to Horizon Client. As you would usually run Horizon Client from a script, and the password would appear in clear text, you should take precautions to make the script unreadable by unprivileged users.

Only Connection Server instances that you enable to authenticate clients in kiosk mode can accept connections from accounts that start with the characters "cm-" followed by a MAC address, or that start with the characters "custom-" or an alternate string that you have defined. Horizon Client in Horizon 7 4.5 and later does not allow the manual entry of user names that take these forms.

As a best practice, use dedicated Connection Server instances to handle clients in kiosk mode, and to create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice not only partitions these systems against unwarranted intrusion, but also makes it easier to configure and administer the clients.

Configure Clients in Kiosk Mode

To configure Active Directory and Horizon 7 to support clients in kiosk mode, you must perform several tasks in sequence.

Prerequisites

Verify that you have the privileges required to perform the configuration tasks.

- **Domain Admins** or **Account Operators** credentials in Active Directory to make changes to the accounts of users and groups in a domain.
- **Administrators**, **Inventory Administrators**, or an equivalent role to use Horizon Administrator to entitle users or groups to remote desktops.
- **Administrators** or an equivalent role to run the `vdmadmin` command.

Procedure

1 Prepare Active Directory and Horizon 7 for Clients in Kiosk Mode

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

2 Set Default Values for Clients in Kiosk Mode

You can use the `vdmadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

3 Display the MAC Addresses of Client Devices

If you want to create an account for a client that is based on its MAC address, you can use Horizon Client to discover the MAC address of the client device.

4 Add Accounts for Clients in Kiosk Mode

You can use the `vdmadmin` command to add accounts for clients to the configuration of a Connection Server group. After you add a client, it is available for use with a Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

5 Enable Authentication of Clients in Kiosk Mode

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their remote desktops via a Connection Server instance.

6 Verify the Configuration of Clients in Kiosk Mode

You can use the `vdmadmin` command to display information about clients in kiosk mode and Connection Server instances that are configured to authenticate such clients.

7 Connect to Remote Desktops from Clients in Kiosk Mode

You can run the client from the command line or use a script to connect a client to a remote session.

Prepare Active Directory and Horizon 7 for Clients in Kiosk Mode

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

As a best practice, create a separate organizational unit and group to help minimize your work in administering clients in kiosk mode. You can add individual accounts for clients that do not belong to any group, but this creates a large administrative overhead if you configure more than a small number of clients.

Procedure

1 In Active Directory, create a separate organizational unit and group to use with clients in kiosk mode.

You must specify a pre-Windows 2000 name for the group. You use this name to identify the group to the `vdmadmin` command.

2 Create the image or template for the guest virtual machine.

You can use a virtual machine that is managed by vCenter Server as a template for an automated pool, as a parent for a linked-clone pool, or as a virtual machine in a manual desktop pool. You can also install and configure applications on the guest operating system.

3 Configure the guest operating system so that the clients are not locked when they are left unattended.

Horizon 7 suppresses the pre-login message for clients that connect in kiosk mode. If you require an event to unlock the screen and display a message, you can configure a suitable application on the guest operating system.

4 In Horizon Administrator, create the desktop pool that the clients will use and entitle the group to this pool.

For example, you might choose to create a floating-assignment, linked-clone desktop pool as being most suitable for the requirements of your client application. You might also associate one or more ThinApp applications with the desktop pool.

Important Do not entitle a client or a group to more than one desktop pool. If you do, Horizon 7 assigns a remote desktop at random from the pools to which a client is entitled, and generates a warning event.

5 If you want to enable location-based printing for the clients, configure the Active Directory group policy setting `AutoConnect Location-based Printing for VMware View`, which is located in the Microsoft Group Policy Object Editor in the `Software Settings` folder under `Computer Configuration`.

6 Configure other policies that you need to optimize and secure the remote desktops of the clients.

For example, you might want to override the policies that connect local USB devices to the remote desktop when it is launched or when the devices are plugged in. By default, Horizon Client for Windows enables these policies for clients in kiosk mode.

Example: Preparing Active Directory for Clients in Kiosk Mode

A company intranet has a domain MYORG, and its organizational unit has the distinguished name OU=myorg-ou,DC=myorg,DC=com. In Active Directory, you create the organizational unit kiosk-ou with the distinguished name OU=kiosk-ou,DC=myorg,DC=com and the group kc-grp for use with clients in kiosk mode.

What to do next

Set default values for the clients.

Set Default Values for Clients in Kiosk Mode

You can use the `vdmadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients will use to connect to their published desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all Connection Server instances in a group.

Procedure

- Set the default values for clients.

```
vdmadmin –Q –clientauth –setdefaults [–b authentication_arguments] [–ou DN] [ –expirepassword |
–noexpirepassword ] [–group group_name | –nogroup]
```

Option	Description
–expirepassword	Specifies that the expiry time for passwords on the client accounts is the same as for the Connection Server group. If no expiry time is defined for the group, passwords do not expire.
–group *group_name*	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.
–noexpirepassword	Specifies that passwords on client accounts do not expire.
–nogroup	Clears the setting for the default group.
–ou *DN*	Specifies the distinguished name of the default organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com **Note** You cannot use the command to change the configuration of an organizational unit.

The command updates the default values for clients in the Connection Server group.

Example: Setting Default Values for Cients in Kiosk Mode

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group kc–grp
```

What to do next

Find out the MAC addresses of client devices that use their MAC address for authentication.

Display the MAC Addresses of Client Devices

If you want to create an account for a client that is based on its MAC address, you can use Horizon Client to discover the MAC address of the client device.

Prerequisites

Log in on the console of the client.

Procedure

- To display the MAC address, type the appropriate command for your platform.

Option	Action
Windows	Enter **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo** The client uses the default Connection Server instance that you configured for it. If you have not configured a default value, the client prompts you for the value. The command displays the IP address, MAC address, and machine name of the client device.
Linux	Enter **vmware-view --printEnvironmentInfo -s *connection_server*** You must specify the IP address or FQDN of the Connection Server instance that the client will use to connect to the desktop. The command displays the IP address, MAC address, machine name, domain, name and domain of any logged-on user, and time zone of the client device.

What to do next

Add accounts for the clients.

Add Accounts for Clients in Kiosk Mode

You can use the `vdmadmin` command to add accounts for clients to the configuration of a Connection Server group. After you add a client, it is available for use with a Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients will use to connect to their published desktops.

When you add a client in kiosk mode, Horizon 7 creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with a recognized prefix string, such as "custom-", or with an alternate prefix string that you have defined in ADAM, and it cannot be more than 20 characters long. If you do not specify a name for a client, Horizon 7 generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with Connection Server instances that you enable to authenticate clients.

Important Do not use a specified name with more than one client device. Future releases might not support this configuration.

Procedure

- Run the `vdmadmin` command using the `-domain` and `-clientid` options to specify the domain and the name or the MAC address of the client.

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name -clientid client_id
[-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group
group_name | -nogroup] [-description "description_text"]
```

Option	Description
-clientid *client_id*	Specifies the name or the MAC address of the client.
-description "*description_text*"	Creates a description of the account for the client device in Active Directory.
-domain *domain_name*	Specifies the domain for the client.
-expirepassword	Specifies that the expiry time for the password on the client's account is the same as for the Connection Server group. If no expiry time is defined for the group, the password does not expire.
-genpassword	Generates a password for the client's account. This is the default behavior if you do not specify either `-password` or `-genpassword`. A generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, use the `-password` option to specify the password.
-group *group_name*	Specifies the name of the group to which the client's account is added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory. If you previously set a default group, client's account is added to this group.
-noexpirepassword	Specifies that the password on the client's account does not expire.
-nogroup	Specifies that the client's account is not added to the default group.
-ou *DN*	Specifies the distinguished name of the organizational unit to which the client's account is added. For example: OU=kiosk-ou,DC=myorg,DC=com
-password "*password*"	Specifies an explicit password for the client's account.

The command creates a user account in Active Directory for the client in the specified domain and group (if any).

Example: Adding Accounts for Clients

Add an account for a client specified by its MAC address to the MYORG domain, using the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Terminal 21"
```

Add an account for a named client, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Kiosk 11"
```

What to do next

Enable authentication of the clients.

Enable Authentication of Clients in Kiosk Mode

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their remote desktops via a Connection Server instance.

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients will use to connect to their remote desktops.

Although you enable authentication for an individual Connection Server instance, all Connection Server instances in a group share all other settings for client authentication. You need only add an account for a client once. In a Connection Server group, any enabled Connection Server instance can authenticate the client.

If you plan to use kiosk mode with a session-based desktop on an RDS host, you must also add the user account to the Remote Desktop Users group.

Procedure

1 Enable authentication of clients on a Connection Server instance.

```
vdmadmin –Q –enable [–b authentication_arguments] –s connection_server [–requirepassword]
```

Option	Description
–requirepassword	Specifies that you require clients to provide passwords. **Important** If you specify this option, the Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a Connection Server instance to specify this option, such clients cannot authenticate themselves and they fail with the error message `Unknown username or bad password`.
–s *connection_server*	Specifies the NetBIOS name of the Connection Server instance on which to enable authentication of clients.

The command enables the specified Connection Server instance to authenticate clients.

2 If the published desktop is provided by a Microsoft RDS host, log in to the RDS host and add the user account to the Remote Desktop Users group.

For example, say that on the Horizon 7 server, you entitle the user account `custom–11` to a session-based desktop on an RDS host. You must then log in to the RDS host, and add the user `custom–11` to the Remote Desktop Users group by going to **Control Panel > System and Security > System > Remote settings > Select users > Add**.

Example: Enabling Authentication of Clients in Kiosk Mode

Enable authentication of clients for the Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

What to do next

Verify the configuration of the Connection Server instances and the clients.

Verify the Configuration of Clients in Kiosk Mode

You can use the `vdmadmin` command to display information about clients in kiosk mode and Connection Server instances that are configured to authenticate such clients.

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients will use to connect to their remote desktops.

Procedure

- Display information about clients in kiosk mode and client authentication.

  ```
  vdmadmin –Q –clientauth –list [–b authentication_arguments] [–xml]
  ```

  The command displays information about clients in kiosk mode and the Connection Server instances on which you have enabled client authentication.

Example: Displaying Information for Clients in Kiosk Mode

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password and requires the end user to provide this. The Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

What to do next

Verify that the clients can connect to their remote desktops.

Connect to Remote Desktops from Clients in Kiosk Mode

You can run the client from the command line or use a script to connect a client to a remote session.

You would usually use a command script to run Horizon Client on a deployed client device.

Note On a Windows or Mac client, by default USB devices on the client are not forwarded automatically if they are in use by another application or service when the remote desktop session starts. On all clients, human interface devices (HIDs) and smart card readers are not forwarded by default.

Procedure

- To connect to a remote session, type the appropriate command for your platform.

Option	Description	
Windows	Enter **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL *connection_server*] [-userName *user_name*] [-password *password*]**	
	-password *password*	Specifies the password for the client's account. If you defined a password for the account, you must specify this password.
	-serverURL *connection_server*	Specifies the IP address or FQDN of the Connection Server instance that Horizon Client will use to connect to its remote desktop. If you do not specify the IP address or FQDN of the Connection Server instance that the client will use to connect to its remote desktop, the client uses the default Connection Server instance that you configured for it.
	-userName *user_name*	Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.
Linux	Enter **vmware-view --unattended -s *connection_server* [--once] [-u *user_name*] [-p *password*]**	
	--once	Specifies that you do not want Horizon Client to retry connecting in the case of an error occurring. **Important** You should usually specify this option, and use the exit code to handle the error. Otherwise, you might find it difficult to kill the `vmware-view` process remotely.
	-p *password*	Specifies the password for the client's account. If you defined a password for the account, you must specify this password.
	-s *connection_server*	Specifies the IP address or FQDN of the Connection Server instance that the client will use to connect to its desktop.
	-u *user_name*	Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.

If the server authenticates the kiosk client and a remote desktop is available, the command starts the remote session.

Example: Running Horizon Client on Clients in Kiosk Mode

Run Horizon Client on a Windows client whose account name is based on its MAC address, and which has an automatically generated password.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL
consvr2.myorg.com
```

Run Horizon Client on a Linux client using an assigned name and password.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Troubleshooting Horizon 7

11

You can use a variety of procedures for diagnosing and fixing problems that you might encounter when using Horizon 7. You can use Horizon Help Desk Tool for troubleshooting, use other troubleshooting procedures to investigate and correct problems, or obtain assistance from VMware Technical Support.

For information about troubleshooting desktops and desktop pools, see the *Setting Up Virtual Desktops in Horizon 7* document.

This chapter includes the following topics:

Using Horizon Help Desk Tool

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 Verify Horizon Help Desk Tool License.

- 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, Configure Role-Based Access for Horizon Help Desk Tool
- 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}
  ```

Note When used in Horizon Administrator, Horizon Help Desk Tool does not support Linux desktops. Use Horizon Help Desk Tool in Horizon Console to get the status of Horizon 7 user sessions on Linux desktop sessions.

Verify Horizon Help Desk Tool License

If you do not have a valid product license key, you cannot log in to Horizon Help Desk Tool. You can verify the product license key in Horizon Administrator and apply a valid license.

Prerequisites

- Obtain a valid product license key for the Horizon Enterprise edition license or the Horizon Apps Advanced edition license.

Procedure

1. In Horizon Administrator, select **View Configuration > Product Licensing and Usage**.

   The first and last five characters of the current license key are displayed in the **Licensing** panel.
2. Verify the license status for the **Help Desk license** field.

Option	Description
Disabled	The product license key is not valid. You cannot log in to Horizon Help Desk Tool.
Enabled	The product license key is valid. You can log in to Horizon Help Desk Tool.

3. (Optional) If the product license key is not valid, click **Edit License** and enter the valid license serial number and click **OK** and refresh the Horizon Administrator URL.

   The **Product Licensing** window shows the updated licensing information.

What to do next

Log in to Horizon Help Desk Tool.

Configure Role-Based Access for Horizon Help Desk Tool

You can assign predefined administrator roles to Horizon Help Desk Tool administrators to delegate the troubleshooting tasks between administrator users. You can also create custom roles and add privileges based on the predefined administrator roles.

You can assign the following predefined administrator roles to Horizon Help Desk Tool administrators:

- Help Desk Administrator
- Help Desk Administrator (Read Only)

If you create a custom role for a Horizon Help Desk Tool administrator, you must assign the Manage Help Desk (Read Only) privilege along with any other privileges based on the Help Desk Administrator role or Help Desk Administrator (Read Only) role.

Prerequisites

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

Procedure

1. In Horizon Administrator, select **View Configuration > Administrators** and click the **Roles** tab.
2. On the **Roles** tab, click **Add Role** and select either the Help Desk Administrator role or the Help Desk Administrator (Read Only) role, and click **OK**.
   a. (Optional) To add a custom role, on the **Roles** tab, click **Add Role** and select the Manage Help Desk (Read Only) privilege, select any privileges based on the Help Desk Administrator role or the Help Desk Administrator (Read Only) role, and click **OK**.

Log In to Horizon Help Desk Tool

Horizon Help Desk Tool is integrated into Horizon Console. Starting from Horizon 7 version 7.5, you can no longer use the Horizon Help Desk Tool URL to log in to Horizon Help Desk Tool.

Procedure

1. To log in to Horizon Help Desk Tool from Horizon Administrator, click **Horizon Console** on the top right panel. This is a single sign-on to the Horizon Console Web interface.
2. 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.
3. 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 phone number to open a Skype for Business session to call the user to collaborate with the user on a troubleshooting task.

You can also click the email to send a message to the user.

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 11-1. 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. ■ G, if the session is running in a different pod in the pod federation.
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. See Session Details for Horizon Help Desk Tool. ■ The **Processes** tab displays information about CPU and memory related processes. See Session Processes for Horizon Help Desk Tool. ■ The **Applications** tab displays the details about the applications that are running. See Application Status for Horizon Help Desk Tool.
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.

Desktop Entitlements

The **Desktop Entitlements** tab displays information about the published desktops or virtual desktops that the user is entitled to use.

Table 11-2. Desktop Entitlements

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.
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.

Table 11-2. Desktop Entitlements (Continued)

Option	Description
Type	Displays information about the type of desktop entitlement. ■ Local, for a local entitlement. ■ Global, for a global 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.

Application Entitlements

The **Application Entitlements** tab displays information about the published applications that the user is entitled to use.

Table 11-3. Application Entitlements

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** In the case of 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. ■ Global, for a global 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 CPA environment.

Table 11-4. 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 user 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 11-5. VM Details

Option	Description
Computer Name	Name of the desktop or application session.
Agent Version	Horizon Agent version.
Session State	State of the desktop or application session.
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.
Session Duration	The time the session remained connected to Connection Server.

Table 11-5. VM Details (Continued)

Option	Description
Connection Server	The Connection Server that the session connects to.
Unifted Access Gateway Name	Name of the Unified Access Gateway appliance. This information might take 30 seconds to 60 seconds to display after connecting to the session.
Unified Access Gateway IP	IP address of the Unified Access Gateway appliance. This information might take 30 seconds to 60 seconds to display after connecting to the session.
Pool	Name of the desktop or application pool.
Farm	The farm of RDS hosts for the published desktop or application session.
vCenter	IP address of vCenter Server.

Show Blast Metrics

Displays performance details for a virtual or published desktop session that uses the VMware Blast display protocol. To view these performance details, click **Show Blast Metrics**.

Table 11-6. Blast Display Protocol Details

Option	Description
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, Memory, and Latency

Displays charts for CPU and memory usage of the virtual or published desktop or application and the latency for the PCoIP or Blast display protocol.

Table 11-7. CPU, Memory, and Latency Details

Option	Description
Session CPU	CPU usage of the current session.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Session Memory	Memory usage of the current session.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Session Latency	Displays a chart for the latency for the PCoIP or Blast display protocol. 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**.

Session Logon Segments

Displays the logon duration and usage segments that are created during logon.

Table 11-8. 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. ■ **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. The **GPO Load** logon segment time is 0 if no global policy is configured.
- 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 should appear for new sessions. If these logon segments do not appear for new sessions, you must restart the RDS host.

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.

Table 11-9. 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.

Application Status for Horizon Help Desk Tool

You can view the status and details of an application on the **Applcations** tab when you click a user name in the **Computer Name** option on the **Sessions** tab.

Applications

For each application, you can view the current status and other details.

Table 11-10. Application Details

Option	Description
Application	Name of the application.
Description	Description of the application.

Table 11-10. Application Details (Continued)

Option	Description
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. 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.

Using the VMware Logon Monitor

VMware Logon Monitor monitors Windows user logons and reports performance metrics intended to help administrators, support staff, and developers to troubleshoot slow logon performance.

Metrics include logon time, logon script time, CPU/memory usage, and network connection speed. Logon Monitor can also receive metrics from other VMware products to provide more information on the logon process.

Supported Platforms

Logon Monitor supports the same Windows platforms as the Horizon Agent.

Key Features

Logon Monitor provides the following features:

- Installed as part of Horizon Agent and enabled by default.
- Integrates with Horizon Help Desk Tool timing profiler. Logon-related metrics are aggregated and sent to the Horizon Agent events database.
- Enables customers to upload logs to a file server for easier access.
- Integrates with other VMware products, such as Horizon Persona Management, App Volumes, UEM, and the Horizon Agent that send logon-related events to Logon Monitor. Logon Monitor logs the events as they occur to show the events in the logon flow and how long they are taking.
- Monitors concurrent logons on the same machine.

Logs

Logon Monitor writes log files for service status messages and for a user session. By default, all log files are written to `C:\ProgramData\VMware\VMware Logon Monitor\Logs`.

- Main Log: The main log file, `vmlm.txt`, contains all status messages for the vmlm service and session events that come in before and after monitoring the logon. Check this log to determine if the Logon Monitor is running correctly.
- Session Log: The session log contains all events related to a user logon session. Events start in this log when the logon begins and only apply to a single user session. A summary written at the end of the log provides an overview of the most important metrics. Check this log to troubleshoot slow logons. When the logon is complete, no further events are written to the session log.

Logon Monitor Metrics

Logon Monitor computes metrics related to logon, group policy, user profile, and performance. These metrics provide administrators a detailed view of end user systems during logon time to help determine the root cause of performance bottlenecks.

Table 11-11. Logon Monitor Metrics

Metric	Parameters	Description
Logon time	■ Start ■ End ■ Total Time	Metrics include the time logon starts on the guest, logon is completed and the profile is loaded and the desktop is visible, and the total time spent processing logon on the guest. Excludes any time spent outside of the guest.
Session start to logon start time	Total time	Time from when Windows created a user session until logon began.
Profile sync time	Total time	Time Windows spent reconciling user profile during logon.
Shell load	■ Start ■ End ■ Total Time	Windows provides the start time of the user shell load. The end time is when the explorer window is created.
Logon to hive load time	Total time	Metrics provide total time from when the logon starts to when the user registry hive is loaded.
Windows folder redirection	■ Start ■ End ■ Total Time	Metrics related to the time Windows folder redirection starts and is fully applied, as well as the total time to enable Windows folder redirection. This time can be high for the first time folder redirection has been applied or if new files are being uploaded to the redirected share.
Group policy time	■ User group policy apply time ■ Machine group policy apply time	Metrics related to applying group policy to the guest include the time it took to apply user group policy and machine group policy.
Profile metrics	■ Profile type: local, roaming, temporary ■ Profile size: number of files, number of folders, total megabytes	Metrics related to the user profile indicate the type of user profile and whether it is stored on the local machine, on a central profile store, or deleted after logoff. The profile size includes metrics on the number of files, the total number of folders, and the total size in MB of the user profile.
Profile size distribution	■ Number of Files Between 0 and 1MB ■ Number of Files Between 1MB and 10MB ■ Number of Files Between 10MB and 100MB ■ Number of Files Between 100MB and 1GB ■ Number of Files Between 1GB and 10GB	A count of the number of files in various size ranges in the user profile.

Table 11-11. Logon Monitor Metrics (Continued)

Metric	Parameters	Description
Processes started during logon	■ Name ■ Process ID ■ Parent process ID ■ Session ID	These values are logged for each process that starts from the time the session starts until the logon is complete.
Group policy logon script time	Total time	Metrics related to executing group policy logon scripts report total time spent executing group policy logon scripts.
Group policy power shell script time	Total time	Metrics related to executing group policy power shell scripts indicate time spent executing group policy power shell scripts.
Memory usage	■ Available bytes: min, max, avg ■ Committed bytes: min, max, avg ■ Paged Pool: min, max, avg	WMI metrics related to memory usage during logon. Samplings are takings until logon is complete. Disabled by default.
CPU usage	■ Idle CPU: min, max, avg ■ User CPU: min, max, avg ■ Kernel CPU: min, max, avg	WMI metrics related to CPU usage during logon. Samplings are taken until logon is complete. Disabled by default.
Are logon scripts synchronous?		Reports whether group policy logon scripts are executed synchronously or asynchronously to the logon.
Network connection status	■ Dropped ■ Restored	Reports whether the network connection is alive or disconnected.
Group Policy Software Installation	■ Asynchronous: True/False ■ Error Code ■ Total Time	Metrics related to group policy software installation indicate whether the installations are synchronous or asynchronous to the logon, if the installations succeeded or failed, and the total time spent installing software using group policy.
Disk Usage For Profile Volume	■ Disc space available for user ■ Free disk space ■ Total disk space	Metrics related to the disk usage on the volume where the user profile is stored.
Domain Controller Discovery	■ Error code ■ Total time	Domain controller related metrics. Error code indicates if there is a failure reaching the domain controller.
Estimated network bandwidth	Bandwidth	Value collected from Event ID 5327.
Network connection details	■ Bandwidth ■ Slow link threshold ■ Slow link detected: True/False	Values collected from Event ID 5314.

Table 11-11. Logon Monitor Metrics (Continued)

Metric	Parameters	Description
Settings that can affect logon time	■ Computer\Administrative Templates\Logon\Always wait for network at computer startup and logon ■ Computer\Administrative Templates\Logon\Run these programs at user logon ■ Computer\Administrative Templates\User Profiles\Wait for roaming user profile ■ Computer\Administrative Templates\User Profiles\Set maximum wait time for network if a user has a roaming profile or remote home directory ■ Computer\Administrative Templates\Group Policy\Configure Logon Script Delay ■ User\Admin Templates\System\Logon\Run these programs at user logon ■ User\Admin Templates\System\User Profiles\Specify network directories to sync at logon, logoff time only	
Metrics from Horizon Agent, Persona Management, App Volumes		VMware products that interact with Logon Monitor report custom metrics in the Logon Monitor logs. These metrics can help determine if one of these products might be contributing in a negative way to the logon time.

Logon Monitor Configuration Settings

You can configure Logon Monitor settings using Windows Registry values.

Registry Settings

To change the configuration settings, navigate to the registry key `HKLM\Software\VMware, Inc.\VMware Logon Monitor`.

Table 11-12. Logon Monitor Configuration Values

Registry Key	Type	Description
RemoteLogPath	REG_SZ	Path to remote share to upload logs. When logs are copied to remote log share they are placed in folders specified by the RemoteLogPath registry key. Example: `\\server\share\%username%.%userdomain%`. Logon Monitor creates the folders as needed. Disabled by default. ■ UNC Path to remote log FOLDER ■ Optional; if not configured, log is not uploaded. ■ Optional local environment variables supported.
Flags	REG_DWORD	This value is a bitmask to influence the behavior of the logon monitor. ■ The value to set or remove to enable or disable CPU and memory metrics is 0x4. Disabled by default. ■ The value to set or remove to enable process events and logon script metrics is 0x8. Disabled by default. ■ The value to set to enable or disable integration with Horizon 7 is 0x2. Enabled by default. ■ The value to set to disable crash dumps is 0x1. Dumps are written to `C:\ProgramData\VMware\VMware Logon Monitor\Data`. Disabled by default.
LogMaxSizeMB	REG_DWORD	Maximum size of the main log in MB. Default is 100 MB.
LogKeepDays	REG_DWORD	Maximum number of days to keep the main log before rolling it. Default is 7 days.

Timing Profiler Settings

Logon Monitor integrates with Horizon Help Desk timing profiler. The timing profiler is off by default.

- To enable Logon Monitor to use the timing profiler to write events to the event database, run `vdmadmin –I –timingProfiler –enable`.
- To disable Logon Monitor to use the timing profiler, run `vdmadmin –I –timingProfiler –disable`.

Using VMware Horizon Performance Tracker

VMware Horizon Performance Tracker is a utility that runs in a remote desktop and monitors the performance of the display protocol and system resource usage. You can also create an application pool and run Horizon Performance Tracker as a published application.

Configuring VMware Horizon Performance Tracker

You can run Horizon Performance Tracker in a remote desktop. You can also run Horizon Performance Tracker as a published application.

Horizon Performance Tracker Features

Horizon Performance Tracker displays critical data of the following features:

Table 11-13. Horizon Performance Tracker Features

Performance Monitoring	Details

Protocol specific data	■ Encoder Name: The name of encoder used in display protocol
	■ Bandwidth Used: Overall bandwidth for incoming and outgoing bandwidth averaged over the sampling period for display protocol, PCoIP or Blast
	■ Frame rate per second: Number of imaging frames that were encoded over a one-second sampling period
	■ Audio On: Whether the Audio feature is on
	■ Audio Started: Whether the Audio feature is started
	■ CPU usage:
	  ■ Encoder CPU: CPU usage of the display protocol encoder in current user session
	  ■ System CPU: Total CPU usage of system

Transport type	■ Client to Remote Session: UDP or TCP protocol transport package used from client to remote peer ■ Remote Session to Client: UDP or TCP protocol transport package used from remote peer to client ■ Horizon Connection Server: UDP or TCP protocol transport package used to connect to a Connection Server instance
System health status	■ Estimated Bandwidth: Overall estimated bandwidth available between Horizon Client and Horizon Agent ■ Round Trip: Round trip latency in milliseconds between the Horizon Agentand the Horizon Client
Session context	■ Server details, such as DNS name, domain name, whether it is tunneled, URL, remote IP address ■ Client machine details, such as display number, IP address, keyboard and mouse layout, language, time zone
Realtime protocol switch	

Note Horizon Performance Tracker only collects and displays data when Horizon Agent is running in a virtual desktop session.

System Requirements for Horizon Performance Tracker

Horizon Performance Tracker supports these configurations.

Table 11-14. Horizon Performance Tracker System Requirements

System	Requirements
Virtual desktop operating systems	All operating systems that support Horizon Agent
Client machine operating systems	All Horizon Client versions are supported, except Horizon Client for Linux and Horizon Client for Windows 10 UWP as published applications are not supported.
Display protocols	VMware Blast and PCoIP

Installing Horizon Performance Tracker

Horizon Performance Tracker is a custom setup option in the Horizon Agent installer. You must select the option, as it is not selected by default. Horizon Performance Tracker is available for both IPv4 and IPv6.

You can install Horizon Performance Tracker on a virtual desktop or on an RDS host. If you install it on an RDS host, you can publish it as published application and run the published application from Horizon Client. See *Setting Up Published Desktops and Applications in Horizon 7* document.

The installation creates a shortcut on the desktop.

Configuring Horizon Performance Tracker Group Policy Settings

You can configure group policy settings to change the default settings. See VMware Horizon Performance Tracker Policy Settings.

VMware Horizon Performance Tracker Policy Settings

The Horizon Performance Tracker ADMX template file (`perf_tracker.admx`) contains policy settings related to Horizon Performance Tracker.

When you install Horizon Performance Tracker, the `perf_tracker.admx` file is installed in the `C:\Program Files\vmware\Horizon Performance Tracker\admx` directory on the agent machine. The associated ADML file is in a subfolder in the same directory. To edit policy settings, use `gpedit.msc` on the agent machine.

Procedure

1. Copy the files from `C:\Program Files\vmware\Horizon Performance Tracker\admx` to `C:\Windows\PolicyDefinitions` on the agent machine.
2. Run `gpedit.msc`.
3. Navigate to **Computer Configuration > Administrative Templates > Vmware Horizon Performance Tracker** to edit the settings.

   Table 11-15. Horizon Performance Tracker Policy Settings

Setting	Description
Horizon Performance Tracker basic setting	When enabled, you can set the frequency in seconds at which Horizon Performance Tracker collects data.
Enable Horizon Performance Tracker auto start in remote desktop connection	When enabled, Horizon Performance Tracker automatically starts when a user logs on to a remote desktop connection. To clear this preference GPO setting, select **Disable**.
Enable Horizon Performance Tracker auto start in remote application connection	When enabled, Horizon Performance Tracker automatically starts when a user logs on to a remote application connection. To clear this preference GPO setting, select **Disable**.

4. Restart Horizon Performance Tracker for the changes to take effect.

Run Horizon Performance Tracker

You can use Horizon Client to run Horizon Performance Tracker inside a remote desktop or as a published application.

If the Horizon Client platform that you are using supports multiple sessions, you can run multiple Horizon Performance Tracker published applications from different farms. On Windows and Mac clients, which support multiple sessions, the machine name in the overview window identifies the farm from which the published application originates. On Android and iOS clients, and in HTML Access, only one open session is supported at a time. If you open a second session from another farm, the first session closes.

Prerequisites

- Install and configure Horizon Performance Tracker. See Configuring VMware Horizon Performance Tracker.
- Configure the Horizon Performance Tracker group policy settings. See VMware Horizon Performance Tracker Policy Settings.

Procedure

- To run Horizon Performance Tracker in a remote desktop, use Horizon Client or HTML Access to connect to the server and start the remote desktop.

  If Horizon Performance Tracker does not start automatically when the remote desktop opens, you can double-click the **VMware Horizon Performance Tracker** shortcut on the Windows desktop, or start Horizon Performance Tracker in the same way that you start any Windows application.

  To select options to show the overview window or floating bar and exit the application, right-click the VMware Horizon Performance Tracker icon in the system tray in the remote desktop.
- To run Horizon Performance Tracker as a published application, use Horizon Client or HTML Access to connect to the server and start the Horizon Performance Tracker published application.

  How you use the Horizon Performance Tracker published application depends on the type of client that you are using. You cannot use Horizon Client for Linux or Horizon Client for Windows 10 UWP to run Horizon Performance Tracker as a published application.

  - With Horizon Client for Windows, the VMware Horizon Performance Tracker icon appears in the system tray on the Windows client system. You can double-click this icon to open Horizon Performance Tracker on the Windows client. You can right-click this icon to select options to show the overview window or floating bar and exit the application.
  - With Horizon Client for Mac, the VMware Horizon Performance Tracker icon appears in the menu bar on the Mac client system. You can double-click this icon to open Horizon Performance Tracker on the Mac client. You can also right-click this icon to select options to show the overview window or floating bar and exit the application.

- With Horizon Client for Android or Horizon Client for iOS, the VMware Horizon Performance Tracker icon appears in the Unity Touch sidebar in Horizon Client. You can touch and hold this icon and select options to show the overview window and floating bar and exit the application.
- With HTML Access, the VMware Horizon Performance Tracker icon appears in the HTML Access sidebar. You can right-click this icon and select options to show the overview window or floating bar and exit the application.

What to do next

For information about the data that Horizon Performance Tracker displays, see Configuring VMware Horizon Performance Tracker.

Monitoring System Health

You can use the system health dashboard in Horizon Administrator to quickly see problems that might affect the operation of Horizon 7 or access to remote desktops by end users.

The system health dashboard in the top left of the Horizon Administrator display provides a number of links that you can use to view reports about the operation of Horizon 7:

Sessions	Provides a link to the Sessions screen, which displays information about the status of remote desktop and application sessions.
Problem vCenter VMs	Provides a link to the Machines screen, which displays information about vCenter virtual machines, RDS hosts, other machines that Horizon 7 has flagged as having problems.
Problem RDS Hosts	Provides a link to the **RDS Hosts** tab on the Machines screen, which displays information about RDS hosts that Horizon 7 has flagged as having problems.
Events	Provides links to the Events screen filtered for error events and for warning events.
System Health	Provides links to the Dashboard screen, which displays summaries of the status of Horizon 7 components, vSphere components, domains, desktops, and datastore usage.

The system health dashboard displays a numbered link against each item. This value indicates the number of items that the linked report provides details about.

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 Administrator, and notifies you of the number of events on the dashboard. You can examine the events in detail on the Events screen.

Note Events are listed in the Horizon Administrator 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 Administrator interface.

In addition to monitoring events in Horizon Administrator, you can generate Horizon 7 events in `Syslog` format so that the event data can be accessible to analytics software. See Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option and "Configure Event Logging for Syslog Servers" in the *Horizon 7 Installation* document.

Prerequisites

Create and configure the event database as described in the *Horizon 7 Installation* document.

Procedure

1. In Horizon Administrator, select **Monitoring > Events**.
2. (Optional) In the Events window, 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.

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 11-16. 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.

Collecting Diagnostic Information for Horizon 7

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with Horizon 7.

You can collect diagnostic information for various components of Horizon 7. How you collect this information varies depending on the Horizon 7 component.

- Create a Data Collection Tool Bundle for Horizon Agent

  To assist VMware Technical Support in troubleshooting Horizon Agent, you might need to use the `vdmadmin` command to create a Data Collection Tool (DCT) bundle. You can also obtain the DCT bundle manually, without using `vdmadmin`.

- Save Diagnostic Information for Horizon Client

  If you encounter problems using Horizon Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

- Collect Diagnostic Information for View Composer Using the Support Script

  You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

- Collect Diagnostic Information for Horizon Connection Server

  You can use the support tool to set logging levels and generate log files for Horizon Connection Server.

- Collect Diagnostic Information for Horizon Agent, Horizon Client, or Horizon Connection Server from the Console

  If you have direct access to the console, you can use the support scripts to generate log files for Connection Server, Horizon Client, or remote desktops that are running Horizon Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

Create a Data Collection Tool Bundle for Horizon Agent

To assist VMware Technical Support in troubleshooting Horizon Agent, you might need to use the `vdmadmin` command to create a Data Collection Tool (DCT) bundle. You can also obtain the DCT bundle manually, without using `vdmadmin`.

For your convenience, you can use the `vdmadmin` command on a Connection Server instance to request a DCT bundle from a remote desktop. The bundle is returned to Connection Server.

You can alternatively log in to a specific remote desktop and run a `support` command that creates the DCT bundle on that desktop. If User Account Control (UAC) is turned on, you must obtain the DCT bundle in this fashion.

Procedure

1 Log in as a user with the required privileges.

Option	Action
On View Connection Server, using vdmadmin	Log in to a standard or replica instance Connection Server as a user with the **Administrators** role.
On the remote desktop	Log in to the remote desktop as a user with administrative privileges.

2 Open a command prompt and run the command to generate the DCT bundle.

Option	Action
On View Connection Server, using vdmadmin	To specify the names of the output bundle file, desktop pool, and machine, use the `–outfile`, `–d`, and `–m` options with the `vdmadmin` command. `vdmadmin –A [–b authentication_arguments] –getDCT –outfile local_file –d desktop –m machine`
On the remote desktop	Change directories to `c:\Program Files\VMware\VMware View\Agent\DCT` and run the following command: `support`

The command writes the bundle to the specified output file.

Example: Using vdmadmin to Create a Bundle File for Horizon Agent

Create the DCT bundle for the machine machine1 in the desktop pool dtpool2 and write it to the zip file `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

What to do next

If you have an existing support request, you can update it by attaching the DCT bundle file.

Save Diagnostic Information for Horizon Client

If you encounter problems using Horizon Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

You can attempt to resolve connection problems for Horizon Client before saving the diagnostic information and contacting VMware Technical Support. For more information, see "Connection Problems Between Horizon Client and Horizon Connection Server" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

1 In Horizon Client, click **Support Information**, or, on the remote desktop menu, select **Options > Support Information**.

2 In the **Support Information** window, click **Collect Support Data** and click **Yes** when prompted.

   A command window shows the progress of gathering the information. This process can take several minutes.

3 In the command window, respond to the prompts by entering the URLs of the Horizon Connection Server instances against which you want to test the configuration of Horizon Client, and, if required, selecting to generate diagnostic dumps of the Horizon 7 processes.

   The information is written to a zip file in a folder on the client machine's desktop.

4 File a support request on the Support page of the VMware Web site, and attach the output zip file.

Collect Diagnostic Information for View Composer Using the Support Script

You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

Prerequisites

Log in to the computer on which View Composer is installed.

Because you must use the Windows Script Host utility (`cscript`) to run the support script, familiarize yourself with using `cscript`. See http://technet.microsoft.com/library/bb490887.aspx.

Procedure

1 Open a command prompt window and change to the `C:\Program Files\VMware\VMware View Composer` directory.

   If you did not install the software in the default directories, substitute the appropriate drive letter and path.

2 Type the command to run the `svi-support` script.

```
cscript ".\svi-support.wsf" /zip
```

   You can use the `/?` option to display information about other command options that are available with the script.

   When the script finishes, it informs you of the name and location of the output file.

3 File a support request on the Support page of the VMware Web site and attach the output file.

Collect Diagnostic Information for Horizon Connection Server

You can use the support tool to set logging levels and generate log files for Horizon Connection Server.

The support tool collects logging data for Connection Server. This information helps VMware Technical Support diagnose any issues that arise with Connection Server. The support tool is not intended to collect diagnostic information for Horizon Client or Horizon Agent. You must instead use the support script. See Collect Diagnostic Information for Horizon Agent, Horizon Client, or Horizon Connection Server from the Console.

Prerequisites

Log in to a standard or replica instance of the Connection Server as a user in the **Administrators** role.

Procedure

1 Select **Start > All Programs > VMware > Set View Connection Server Log Levels**.

2 In the **Choice** text box, type a numeric value to set the logging level and press Enter.

Option	Description
0	Resets the logging level to the default value.
1	Selects a normal level of logging.
2	Selects a debug level of logging (default).
3	Selects full logging.

The system starts recording log information with the level of detail that you have selected.

3 When you have collected enough information about the behavior of Connection Server, select **Start > All Programs > VMware > Generate View Connection Server Log Bundle**.

The support tool writes the log files to a folder called `vdm-sdct` on the desktop of the Connection Server instance.

4 File a support request on the Support page of the VMware Web site and attach the output files.

Collect Diagnostic Information for Horizon Agent , Horizon Client, or Horizon Connection Server from the Console

If you have direct access to the console, you can use the support scripts to generate log files for Connection Server, Horizon Client, or remote desktops that are running Horizon Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

Prerequisites

Log in to the system that you want to collect information for. You must log in as a user with administrator privileges.

- For Horizon Agent, log in to the virtual machine that has Horizon Agent installed.
- For Horizon Client, log in to the system with Horizon Client installed.
- For Connection Server, log in to the Connection Server host.

Procedure

1 Open a command prompt window and change to the appropriate directory for the Horizon 7 component that you want to collect diagnostic information for.

Option	Description
Horizon Agent	Change to the `C:\Program Files\VMware View\Agent\DCT` directory.
Horizon Client	Change to the `C:\Program Files\VMware View\Client\DCT` directory.
View Connection Server	Change to the `C:\Program Files\VMware View\Server\DCT` directory.

If you did not install the software in the default directories, substitute the appropriate drive letter and path.

2 Type the command to run the support script.

```
.\support.bat [loglevels]
```

If you want to enable advanced logging, specify the `loglevels` option and enter the numeric value for the logging level when prompted.

Option	Description
0	Resets the logging level to the default value.
1	Selects a normal level of logging.
2	Selects a debug level of logging (default).
3	Selects full logging.
4	Selects informational logging for PCoIP (Horizon Agent and Horizon Client only).
5	Selects debug logging for PCoIP (Horizon Agent and Horizon Client only).
6	Selects informational logging for virtual channels (Horizon Agent and Horizon Client only).
7	Selects debug logging for virtual channels (Horizon Agent and Horizon Client only).
8	Selects trace logging for virtual channels (Horizon Agent and Horizon Client only).

The script writes the zipped log files to the folder `vdm-sdct` on the desktop.

3 You can find the View Composer guest agent logs in the `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support` directory.

4 File a support request on the Support page of the VMware Web site and attach the output file.

Update Support Requests

You can update your existing support request at the Support Web site.

After you file a support request, you might receive an email request from VMware Technical Support asking for the output file from the `support` or `svi-support` scripts. When you run the scripts, they inform you of the name and location of the output file. Reply to the email message and attach the output file to the reply.

If the output file is too large to include as an attachment (10MB or more), contact VMware Technical Support, tell them the number of your support request, and request FTP upload instructions. Alternatively, you can attach the file to your existing support request at the Support Web site.

Procedure

1. Visit the Support page at the VMware Web site and log in.
2. Click **Support Request History** and find the applicable support request number.
3. Update the support request and attach the output that you obtained by running the `support` or `svi-support` script.

Troubleshooting an Unsuccessful Security Server Pairing with Horizon Connection Server

A security server might not be working if it failed to pair successfully with a Connection Server instance.

Problem

The following security server issues might occur if a security server failed to pair with Connection Server:

- When you try to install the security server a second time, the security server cannot connect to Connection Server.
- Horizon Client cannot connect to Horizon 7. The following error message appears: `The View Connection Server authentication failed. No gateway is available to provide a secure connection to a desktop. Contact your network administrator.`
- The security server is displayed in the Horizon Administrator dashboard as `Down`.

Cause

This problem can occur if you started to install a security server and the attempt was cancelled or otherwise aborted after you entered a security server pairing password.

Solution

If you intend to keep the security server in your Horizon 7 environment, take these steps:

1. In Horizon Administrator, select **View Configuration > Servers**.
2. On the **Security Servers** tab, select a security server, select **Prepare for Upgrade or Reinstallation** from the **More Commands** drop-down menu, and click **OK**.
3. On the **Connection Servers** tab, select the Connection Server instance that you want to pair with the security server, select **Specify Security Server Pairing Password** from the **More Commands** drop-down menu, type a password, and click **OK**.
4. Install the security server again.

If you intend to remove the security server entry from your Horizon 7 environment, run the `vdmadmin -S` command.

For example: **`vdmadmin -S -r -s`** ***`security_server_name`***

Troubleshooting Horizon 7 Server Certificate Revocation Checking

A security server or a Connection Server instance that is used for secure Horizon Client connections might show as red in View Administrator if certificate revocation checking cannot be performed on the server's TLS certificate.

Problem

A security server or Connection Server icon is red on the Horizon Administrator dashboard. The Horizon 7 server's status shows the following message: `Server's certificate cannot be checked`.

Cause

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a Connection Server instance cannot reach the servers that provide revocation checking because of firewalls or other controls.

A Connection Server instance performs certificate revocation checking on its own certificate and on those of the security servers paired to it. By default, the VMware Horizon View Connection Server service is started with the `LocalSystem` account. When it runs under `LocalSystem`, a Connection Server instance cannot use the proxy settings configured in Internet Explorer to access the CRL DP URL or OCSP responder to determine the revocation status of the certificate.

You can use Microsoft `Netshell` commands to import the proxy settings to the Connection Server instance so that the server can access the certificate revocation checking sites on the Internet.

Solution

1. On the Connection Server computer, open a command-line window with the **Run as administrator** setting.

   For example, click **Start**, type **`cmd`**, right-click the `cmd.exe` icon, and select **Run as administrator**.
2. Type **`netsh`** and press Enter.
3. Type **`winhttp`** and press Enter.
4. Type **`show proxy`** and press Enter.

   `Netshell` shows that the proxy was set to DIRECT connection. With this setting, the Connection Server computer cannot connect to the Internet if a proxy is in use in your organization.
5. Configure the proxy settings.

   For example, at the `netsh winhttp>` prompt, type **`import proxy source=ie`**.

   The proxy settings are imported to the Connection Server computer.

6 Verify the proxy settings by typing **`show proxy`**.

7 Restart the VMware Horizon View Connection Server service.

8 On the Horizon Administrator dashboard, verify that the security server or Connection Server icon is green.

Troubleshooting Smart Card Certificate Revocation Checking

The Connection Server instance or security server that has the smart card connected cannot perform certificate revocation checking on the server's TLS certificate unless you have configured smart card certificate revocation checking.

Problem

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a Connection Server instance or security server cannot reach the servers that provide revocation checking because of firewalls or other controls.

Important Make sure the CRL file is up to date.

Cause

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 (Certificate Authority) that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate. The CA must be accessible from the Connection Server or security server host. This issue can only occur if you configured revocation checking of smart card certificates. See Using Smart Card Certificate Revocation Checking.

Solution

1 Create your own (manual) procedure for downloading an up-to-date CRL from the CA website you use to a path on your Horizon 7 server.

2 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`

3 Add the `enableRevocationChecking` and `crlLocation` properties in the `locked.properties` file to the local path to where the CRL is stored.

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

Further Troubleshooting Information

You can find further troubleshooting information in VMware Knowledge Base articles.

The VMware Knowledge Base (KB) is continually updated with new troubleshooting information for VMware products.

For more information about troubleshooting Horizon 7, see the KB articles that are available on the VMware KB Web site:

http://kb.vmware.com/selfservice/microsites/microsite.do

Using the vdmadmin Command 12

You can use the vdmadmin command line interface to perform a variety of administration tasks on a Connection Server instance.

You can use vdmadmin to perform administration tasks that are not possible from within the Horizon Administrator user interface or to perform administration tasks that need to run automatically from scripts.

For a comparison of the operations that are possible in Horizon Administrator, Horizon 7 cmdlets, and vdmadmin, see the *Horizon 7 Integration* document.

- vdmadmin Command Usage

  The syntax of the vdmadmin command controls its operation.

- Configuring Logging in Horizon Agent Using the -A Option

  You can use the vdmadmin command with the –A option to configure logging by Horizon Agent.

- Overriding IP Addresses Using the -A Option

  You can use the vdmadmin command with the –A option to override the IP address reported by Horizon Agent.

- Updating Foreign Security Principals Using the -F Option

  You can use the vdmadmin command with the –F option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.

- Listing and Displaying Health Monitors Using the -H Option

  You can use the vdmadmin command –H to list the existing health monitors, to monitor instances for Horizon 7 components, and to display the details of a specific health monitor or monitor instance.

- Listing and Displaying Reports of Horizon 7 Operation Using the -I Option

  You can use the vdmadmin command with the –I option to list the available reports of Horizon 7 operation and to display the results of running one of these reports.

- Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option

  You can use the vdmadmin command with the –I option to record Horizon 7 event messages in Syslog format in event log files. Many third-party analytics products require flat-file Syslog data as input for their analytics operations.

- Assigning Dedicated Machines Using the -L Option

  You can use the `vdmadmin` command with the `–L` option to assign machines from a dedicated pool to users.

- Displaying Information About Machines Using the -M Option

  You can use the `vdmadmin` command with the `–M` option to display information about the configuration of virtual machines or physical computers.

- Reclaiming Disk Space on Virtual Machines Using the -M Option

  You can use the `vdmadmin` command with the `–M` option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.

- Configuring Domain Filters Using the -N Option

  You can use the `vdmadmin` command with the `–N` option to control the domains that Horizon 7 makes available to end users.

- Configuring Domain Filters

  You can configure domain filters to limit the domains that a Connection Server instance or security server makes available to end users.

- Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options

  You can use the `vdmadmin` command with the `–O` and `–P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.

- Configuring Clients in Kiosk Mode Using the -Q Option

  You can use the `vdmadmin` command with the `–Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

- Displaying the First User of a Machine Using the -R Option

  You can use the `vdmadmin` command with the `–R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.

- Removing the Entry for a Connection Server Instance or Security Server Using the -S Option

  You can use the `vdmadmin` command with the `–S` option to remove the entry for a Connection Server instance or security server from the Horizon 7 configuration.

- Providing Secondary Credentials for Administrators Using the -T Option

  You can use the `vdmadmin` command with the `–T` option to provide Active Directory secondary credentials to administrator users.

- Displaying Information About Users Using the -U Option

  You can use the `vdmadmin` command with the `–U` option to display detailed information about users.

- Unlocking or Locking Virtual Machines Using the -V Option

  You can use the `vdmadmin` command with the `–V` option to unlock or lock virtual machines in the data center.

- Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option

  You can use the `vdmadmin` command with the `–X` option to detect and resolve LDAP entry collisions and LDAP schema collisions on replicated Connection Server instances in a group. You can also use this option to detect and resolve LDAP schema collisions in a Cloud Pod Architecture environment.

vdmadmin Command Usage

The syntax of the `vdmadmin` command controls its operation.

Use the following form of the `vdmadmin` command from a Windows command prompt.

```
vdmadmin command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option.

By default, the path to the `vdmadmin` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid having to enter the path on the command line, add the path to your *PATH* environment variable.

- vdmadmin Command Authentication

  You must run the `vdmadmin` command as a user who is in the **Administrators** role for a specified action to succeed.

- vdmadmin Command Output Format

  Some `vdmadmin` command options allow you to specify the format of the output information.

- vdmadmin Command Options

  You use the command options of the `vdmadmin` command to specify the operation that you want it to perform.

vdmadmin Command Authentication

You must run the `vdmadmin` command as a user who is in the **Administrators** role for a specified action to succeed.

You can use Horizon Administrator to assign the **Administrators** role to a user. See Chapter 6 Configuring Role-Based Delegated Administration.

If you are logged in as a user with insufficient privileges, you can use the –b option to run the command as a user who has been assigned the **Administrators** role, if you know that user's password. You can specify the –b option to run the vdmadmin command as the specified user in the specified domain. The following usage forms of the –b option are equivalent.

```
–b username domain [password | *]
```

```
–b username@domain [password | *]
```

```
–b domain\username [password | *]
```

If you specify an asterisk (*) instead a password, you are prompted to enter the password, and the vdmadmin command does not leave sensitive passwords in the command history on the command line.

You can use the –b option with all command options except the –R and –T options.

vdmadmin Command Output Format

Some vdmadmin command options allow you to specify the format of the output information.

The following table shows the options that some vdmadmin command options provide for formatting output text.

Table 12-1. Options for Selecting Output Format

Option	Description
–csv	Formats the output as comma-separated values.
–n	Display the output using ASCII (UTF-8) characters. This is the default character set for comma-separated values and plain text output.
–w	Display the output using Unicode (UTF-16) characters. This is the default character set for XML output.
–xml	Formats the output as XML.

vdmadmin Command Options

You use the command options of the vdmadmin command to specify the operation that you want it to perform.

The following table shows the command options that you can use with the vdmadmin command to control and examine the operation of Horizon 7.

Table 12-2. Vdmadmin Command Options

Option	Description
–A	Administers the information that Horizon Agent records in its log files. See Configuring Logging in Horizon Agent Using the -A Option. Overrides the IP address reported by Horizon Agent. See Overriding IP Addresses Using the -A Option
–C	Sets the name for a Connection Server group. See GUID-3AD7B00C-43C4-417E-A06B-7251805657D6#GUID-3AD7B00C-43C4-417E-A06B-7251805657D6.
–F	Updates the Foreign Security Principals (FSPs) in Active Directory for all users or for specified users. See Updating Foreign Security Principals Using the -F Option.
–H	Displays health information about Horizon 7 services. See Listing and Displaying Health Monitors Using the -H Option.
–I	Generates reports about Horizon 7 operation. See Listing and Displaying Reports of Horizon 7 Operation Using the -I Option.
–L	Assigns a dedicated desktop to a user or removes an assignment. See Assigning Dedicated Machines Using the -L Option.
–M	Displays information about a virtual machine or physical computer. See Displaying Information About Machines Using the -M Option.
–N	Configures the domains that a Connection Server instance or group makes available to Horizon Client. See Configuring Domain Filters Using the -N Option.
–O	Displays the remote desktops that are assigned to users who are no longer entitled to those desktops. See Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options.
–P	Displays the user policies that are associated with the remote desktops of unentitled users. See Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options.
–Q	Configures the account in Active Directory account and Horizon 7 configuration of a client device in kiosk mode. See Configuring Clients in Kiosk Mode Using the -Q Option.
–R	Reports the first user who accessed a remote desktop. See Displaying the First User of a Machine Using the -R Option.
–S	Removes a configuration entry for a Connection Server instance from the configuration of Horizon 7. See Removing the Entry for a Connection Server Instance or Security Server Using the -S Option.
–T	Provides Active Directory secondary credentials to administrator users. See Providing Secondary Credentials for Administrators Using the -T Option.
–U	Displays information about a user including their remote desktop entitlements and ThinApp assignments, and Administrator roles. See Displaying Information About Users Using the -U Option.
–V	Unlocks or locks virtual machines. See Unlocking or Locking Virtual Machines Using the -V Option.
–X	Detects and resolves duplicated LDAP entries on replicated Connection Server instances. See Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option.

Configuring Logging in Horizon Agent Using the -A Option

You can use the `vdmadmin` command with the –A option to configure logging by Horizon Agent.

Syntax

```
vdmadmin –A [–b authentication_arguments] –getDCT–outfile local_file –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –getlogfile logfile –outfile local_file –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –getloglevel [–xml] –d desktop [–m machine]
```

```
vdmadmin –A [–b authentication_arguments] –getstatus [–xml] –d desktop [–m machine]
```

```
vdmadmin –A [–b authentication_arguments] –getversion [–xml] –d desktop [–m machine]
```

```
vdmadmin –A [–b authentication_arguments] –list [–xml] [–w | –n] –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –setloglevel level –d desktop [–m machine]
```

Usage Notes

To assist VMware Technical Support in troubleshooting Horizon Agent, you can create a Data Collection Tool (DCT) bundle. You can also change the logging level, display the version and status of Horizon Agent, and save individual log files to your local disk.

Options

The following table shows the options that you can specify to configure logging in Horizon Agent.

Table 12-3. Options for Configuring Logging in Horizon Agent

Option	Description
–d *desktop*	Specifies the desktop pool.
–getDCT	Creates a Data Collection Tool (DCT) bundle and saves it to a local file.
–getlogfile *logfile*	Specifies the name of the log file to save a copy of.
–getloglevel	Displays the current logging level of Horizon Agent.
–getstatus	Displays the status of Horizon Agent.
–getversion	Displays the version of Horizon Agent.
–list	List the log files for Horizon Agent.
–m *machine*	Specifies the machine within a desktop pool.

Table 12-3. Options for Configuring Logging in Horizon Agent (Continued)

Option	Description	
`–outfile` *local_file*	Specifies the name of the local file in which to save a DCT bundle or a copy of a log file.	
`–setloglevel` *level*	Sets the logging level of Horizon Agent.	
	debug	Logs error, warning, and debugging events.
	normal	Logs error and warning events.
	trace	Logs error, warning, informational, and debugging events.

Examples

Display the logging level of Horizon Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getloglevel
```

Set the logging level of Horizon Agent for the machine machine1 in the desktop pool dtpool2 to debug.

```
vdmadmin –A –d dtpool2 –m machine1 –setloglevel debug
```

Display the list of the Horizon Agent log files for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –list
```

Save a copy of the Horizon Agent log file `log–2009–01–02.txt` for the machine machine1 in the desktop pool dtpool2 as `C:\mycopiedlog.txt`.

```
vdmadmin –A –d dtpool2 –m machine1 –getlogfile log–2009–01–02.txt –outfile C:\mycopiedlog.txt
```

Display the version of Horizon Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getversion
```

Display the status of Horizon Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getstatus
```

Create the DCT bundle for the machine machine1 in the desktop pool dtpool2 and write it to the zip file `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Overriding IP Addresses Using the -A Option

You can use the vdmadmin command with the –A option to override the IP address reported by Horizon Agent.

Syntax

```
vdmadmin –A [–b authentication_arguments] –override –i ip_or_dns –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –list –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –r –d desktop [–m machine]
```

Usage Notes

Horizon Agent reports the discovered IP address of the machine on which it is running to the Connection Server instance. In secure configurations where the Connection Server instance cannot trust the value that Horizon Agent reports, you can override the value provided by Horizon Agent and specify the IP address that the managed machine should be using. If the address of a machine that Horizon Agent reports does not match the defined address, you cannot use Horizon Client to access the machine.

Options

The following table shows the options that you can specify to override IP addresses.

Table 12-4. Options for Overriding IP Addresses

Option	Description
–d *desktop*	Specifies the desktop pool.
–i *ip_or_dns*	Specifies the IP address or resolvable domain name in DNS.
–m *machine*	Specifies the name of the machine in a desktop pool.
–override	Specifies an operation for overriding IP addresses.
–r	Removes an overridden IP address.

Examples

Override the IP address for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

Display the IP addresses that are defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

Remove the IP addresses that is defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

Remove the IP addresses that are defined for the desktops in the desktop pool dtpool3.

```
vdmadmin –A –override –r –d dtpool3
```

Updating Foreign Security Principals Using the -F Option

You can use the `vdmadmin` command with the `–F` option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.

Syntax

```
vdmadmin –F [–b authentication_arguments] [–u domain\user]
```

Usage Notes

If you trust domains outside of your local domains, you allow access by security principals in the external domains to the local domains' resources. Active Directory uses FSPs to represent security principals in trusted external domains. You might want to update the FSPs of users if you modify the list of trusted external domains.

Options

The `–u` option specifies the name and domain of the user whose FSP you want to update. If you do not specify this option, the command updates the FSPs of all users in Active Directory.

Examples

Update the FSP of the user Jim in the EXTERNAL domain.

```
vdmadmin –F –u EXTERNAL\Jim
```

Update the FSPs of all users in Active Directory.

```
vdmadmin –F
```

Listing and Displaying Health Monitors Using the -H Option

You can use the `vdmadmin` command `–H` to list the existing health monitors, to monitor instances for Horizon 7 components, and to display the details of a specific health monitor or monitor instance.

Syntax

```
vdmadmin –H [–b authentication_arguments] –list –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –list –monitorid monitor_id –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –monitorid monitor_id –instanceid instance_id –xml [–w | –n]
```

Usage Notes

The following table shows the health monitors that Horizon 7 uses to monitor the health of its components.

Table 12-5. Health Monitors

Monitor	Description
CBMonitor	Monitors the health of Connection Server instances.
DBMonitor	Monitors the health of the events database.
DomainMonitor	Monitors the health of the Connection Server host's local domain and all trusted domains.
SGMonitor	Monitors the health of security gateway services and security servers.
VCMonitor	Monitors the health of vCenter servers.

If a component has several instances, Horizon 7 creates a separate monitor instance to monitor each instance of the component.

The command outputs all information about health monitors and monitor instances in XML format.

Options

The following table shows the options that you can specify to list and display health monitors.

Table 12-6. Options for Listing and Displaying Health Monitors

Option	Description
–instanceid *instance_id*	Specifies a health monitor instance
–list	Displays the existing health monitors if a health monitor ID is not specified.
–list –monitorid *monitor_id*	Displays the monitor instances for the specified health monitor ID.
–monitorid *monitor_id*	Specifies a health monitor ID.

Examples

List all existing health monitors in XML using Unicode characters.

```
vdmadmin –H –list –xml
```

List all instances of the vCenter monitor (VCMonitor) in XML using ASCII characters.

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

Display the health of a specified vCenter monitor instance.

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

Listing and Displaying Reports of Horizon 7 Operation Using the -I Option

You can use the `vdmadmin` command with the `–I` option to list the available reports of Horizon 7 operation and to display the results of running one of these reports.

Syntax

```
vdmadmin –I [–b authentication_arguments] –list [–xml] [–w | –n]
```

```
vdmadmin –I [–b authentication_arguments] –report report –view view [–startdate yyyy–MM–dd–HH:mm:ss]
[–enddate yyyy–MM–dd–HH:mm:ss] [–w | –n] –xml | –csv
```

Usage Notes

You can use the command to display the available reports and views, and to display the information that Horizon 7 has recorded for a specified report and view.

You can also use the `vdmadmin` command with the `–I` option to generate Horizon 7 log messages in `syslog` format. See Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option.

Options

The following table shows the options that you can specify to list and display reports and views.

Table 12-7. Options for Listing and Displaying Reports and Views

Option	Description
`–enddate` *yyyy-MM-dd-HH:mm:ss*	Specifies a upper limit for the date of information to be displayed.
`–list`	Lists the available reports and views.

Table 12-7. Options for Listing and Displaying Reports and Views (Continued)

Option	Description
`–report` *report*	Specifies a report.
`–startdate` *yyyy-MM-dd-HH:mm:ss*	Specifies a lower limit for the date of information to be displayed.
`–view` *view*	Specifies a view.

Examples

List the available reports and views in XML using Unicode characters.

```
vdmadmin –I –list –xml –w
```

Display a list of user events that occurred since August 1, 2010 as comma-separated values using ASCII characters.

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option

You can use the `vdmadmin` command with the `–I` option to record Horizon 7 event messages in `Syslog` format in event log files. Many third-party analytics products require flat-file `Syslog` data as input for their analytics operations.

Syntax

```
vdmadmin –I –eventSyslog –disable
```

```
vdmadmin –I –eventSyslog –enable –localOnly
```

```
vdmadmin –I –eventSyslog –enable –path path
```

```
vdmadmin –I –eventSyslog –enable –path path
 –user DomainName\username –password password
```

Usage Notes

You can use the command to generate Horizon 7 event log messages in `Syslog` format. In a `Syslog` file, Horizon 7 event log messages are formatted in key-value pairs, which makes the logging data accessible to analytics software.

You can also use the vdmadmin command with the –I option to list the available reports and views and to display the contents of a specified report. See Listing and Displaying Reports of Horizon 7 Operation Using the -I Option.

Options

You can disable or enable the eventSyslog option. You can direct the Syslog output to the local system only or to another location. Direct UDP connection to a Syslog server is supported with Horizon 7 5.2 or later. See "Configure Event Logging for Syslog Servers" in the *Horizon 7 Installation* document.

Table 12-8. Options for Generating Horizon 7 Event Log Messages in Syslog Format

Option	Description
–disable	Disables Syslog logging.
–e|–enable	Enables Syslog logging.
–eventSyslog	Specifies that Horizon 7 events are generated in Syslog format.
–localOnly	Stores the Syslog output on the local system only. When you use the –localOnly option, the default destination of the Syslog output is %PROGRAMDATA%\VMware\VDM\events\.
–password *password*	Specifies the password for the user that authorizes access to the specified destination path for the Syslog output.
–path	Determines the destination UNC path for the Syslog output.
–u|–user *DomainName\username*	Specifies the domain and username that can access the destination path for the Syslog output.

Examples

Disable generating Horizon 7 events in Syslog format.

```
vdmadmin –I –eventSyslog –disable
```

Direct Syslog output of Horizon 7 events to the local system only.

```
vdmadmin –I –eventSyslog –enable –localOnly
```

Direct Syslog output of Horizon 7 events to a specified path.

```
vdmadmin –I –eventSyslog –enable –path path
```

Direct Syslog output of Horizon 7 events to a specified path that requires access by an authorized domain user.

```
vdmadmin –I –eventSyslog –enable –path \\logserver\share\ViewEvents –user mydomain\myuser
 –password mypassword
```

Assigning Dedicated Machines Using the -L Option

You can use the vdmadmin command with the –L option to assign machines from a dedicated pool to users.

Syntax

```
vdmadmin –L [–b authentication_arguments] –d desktop –m  machine –u domain\user
```

```
vdmadmin –L [–b authentication_arguments] –d desktop [–m machine | –u domain\user] –r
```

Usage Notes

Horizon 7 assigns machines to users when they first connect to a dedicated desktop pool. Under some circumstances, you might want to preassign machines to users. For example, you might want to prepare their system environments in advance of their initial connection. After a user connects to a remote desktop that Horizon 7 assigns from a dedicated pool, the virtual machine that hosts the desktop remains assigned to the user for the life span of the virtual machine. You can assign a user to a single machine in a dedicated pool.

You can assign a machine to any entitled user. You might want to do this when recovering from the loss of View LDAP data on a Connection Server instance, or when you want to change ownership of a particular machine.

After a user connects to a remote desktop that Horizon 7 assigns from a dedicated pool, that remote desktop remains assigned to the user for the life span of the virtual machine that hosts the desktop. You might want to remove the assignment of a machine to a user who has left the organization, who no longer requires access to the desktop, or who will use a desktop in a different desktop pool. You can also remove assignments for all users who access a desktop pool.

Note The vdmadmin –L command does not assign ownership to View Composer persistent disks. To assign linked-clone desktops with persistent disks to users, use the **Assign User** menu option in Horizon Administrator.

If you do use vdmadmin –L to assign a linked-clone desktop with a persistent disk to a user, unexpected results can occur in certain situations. For example, if you detach a persistent disk and use it to recreate a desktop, the recreated desktop is not assigned to the owner of the original desktop.

Options

The following table shows the options that you can specify to assign a desktop to a user or to remove an assignment.

Table 12-9. Options for Assigning Dedicated Desktops

Option	Description
–d *desktop*	Specifies the name of the desktop pool.
–m *machine*	Specifies the name of the virtual machine that hosts the remote desktop.
–r	Removes an assignment to a specified user, or all assignments to a specified machine.
–u *domain\user*	Specifies the login name and domain of the user.

Examples

Assign the machine machine2 in the desktop pool dtpool1 to the user Jo in the CORP domain.

```
vdmadmin –L –d dtpool1 –m machine2 –u CORP\Jo
```

Remove the assignments for the user Jo in the CORP domain to desktops in the pool dtpool1.

```
vdmadmin –L –d dtpool1 –u Corp\Jo –r
```

Remove all user assignments to the machine machine1 in the desktop pool dtpool3.

```
vdmadmin –L –d dtpool3 –m machine1 –r
```

Displaying Information About Machines Using the -M Option

You can use the `vdmadmin` command with the `–M` option to display information about the configuration of virtual machines or physical computers.

Syntax

```
vdmadmin –M [–b authentication_arguments] [–m machine | [–u domain\user][–d desktop]] [–xml | –csv]
[–w | –n]
```

Usage Notes

The command displays information about a remote desktop's underlying virtual machine or physical computer.

- Display name of the machine.
- Name of the desktop pool.
- State of the machine.

The machine state can be one of the following values: `UNDEFINED, PRE_PROVISIONED, CLONING, CLONINGERROR, CUSTOMIZING, READY, DELETING, MAINTENANCE, ERROR, LOGOUT`.

The command does not display all dynamic machine states, such as `Connected` or `Disconnected`, that are displayed in Horizon Administrator.

- SID of the assigned user.
- Account name of the assigned user.
- Domain name of the assigned user.
- Inventory path of the virtual machine (if applicable).
- Date on which the machine was created.
- Template path of the machine (if applicable).
- URL of the vCenter Server (if applicable).

Options

The following table shows the options that you can use to specify the machine whose details you want to display.

Table 12-10. Options for Displaying Information About Machines

Option	Description
`–d` *desktop*	Specifies the name of the desktop pool.
`–m` *machine*	Specifies the name of the virtual machine.
`–u` *domain\user*	Specifies the login name and domain of the user.

Examples

Display information about the underlying machine for the remote desktop in the pool dtpool2 that is assigned to the user Jo in the CORP domain and format the output as XML using ASCII characters.

```
vdmadmin –M –u CORP\Jo –d dtpool2 –xml –n
```

Display information about the machine machine3 and format the output as comma-separated values.

```
vdmadmin –M –m machine3 –csv
```

Reclaiming Disk Space on Virtual Machines Using the -M Option

You can use the `vdmadmin` command with the `–M` option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.

Syntax

```
vdmadmin –M [–b authentication_arguments] –d desktop –m machine –markForSpaceReclamation
```

Usage Notes

With this option, you can initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes.

Space reclamation does not take place if you run this command when a blackout period is in effect.

The following prerequisites must be met before you can reclaim disk space by using the `vdmadmin` command with the `–M` option:

- Verify that Horizon 7 is using vCenter Server and ESXi version 5.1 or later.
- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on the virtual machine.
- Verify that the virtual machine is virtual hardware version 9 or later.
- In Horizon Administrator, verify that the **Enable space reclamation** option is selected for vCenter Server. See Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines.
- In Horizon Administrator, verify that the **Reclaim VM disk space** option was selected for the desktop pool. See "Reclaim Disk Space on View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.
- Verify that the virtual machine is powered on before you initiate the space reclamation operation.
- Verify that a blackout period is not in effect. See "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.

Options

Table 12-11. Options for Reclaiming Disk Space on Virtual Machines

Option	Description
`–d` *desktop*	Specifies the name of the desktop pool.
`–m` *machine*	Specifies the name of the virtual machine.
`–MarkForSpaceReclamation`	Marks the virtual machine for disk space reclamation.

Example

Marks the virtual machine `machine3` in the desktop pool `pool1` for disk space reclamation.

```
vdmadmin –M –d pool1 –m machine3 –markForSpaceReclamation
```

Configuring Domain Filters Using the -N Option

You can use the `vdmadmin` command with the `–N` option to control the domains that Horizon 7 makes available to end users.

Syntax

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain –add
[–s connsvr]
```

```
vdmadmin –N [–b authentication_arguments] –domains –list [–w | –n] [–xml]
```

```
vdmadmin –N [–b authentication_arguments] –domains –list –active [–w | –n] [–xml]
```

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain
–remove [–s connsvr]
```

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –removeall [–s
connsvr]
```

Usage Notes

Specify one of the `–exclude`, `–include`, or `–search` options to apply an operation to the exclusion list, inclusion list, or search exclusion list respectively.

If you add a domain to a search exclusion list, the domain is excluded from an automated domain search.

If you add a domain to an inclusion list, the domain is included in the results of the search.

If you add a domain to an exclusion list, the domain is excluded from the results of the search.

Options

The following table shows the options that you can specify to configure domain filters.

Table 12-12. Options for Configuring Domain Filters

Option	Description
`–add`	Adds a domain to a list.
`–domain` *domain*	Specifies the domain to be filtered. You must specify domains by their NetBIOS names and not by their DNS names.
`–domains`	Specifies a domain filter operation.
`–exclude`	Specifies an operation on a exclusion list.
`–include`	Specifies an operation on an inclusion list.

Table 12-12. Options for Configuring Domain Filters (Continued)

Option	Description
`–list`	Displays the domains that are configured in the search exclusion list, exclusion list, and inclusion list on each Connection Server instance and for the Connection Server group.
`–list –active`	Displays the available domains for the Connection Server instance on which you run the command.
`–remove`	Removes a domain from a list.
`–removeall`	Removes all domains from a list.
`–s` *connsvr*	Specifies that the operation applies to the domain filters on a Connection Server instance. You can specify the Connection Server instance by its name or IP address. If you do not specify this option, any change that you make to the search configuration applies to all Connection Server instances in the group.
`–search`	Specifies an operation on a search exclusion list.

Examples

Add the domain FARDOM to the search exclusion list for the Connection Server instance csvr1.

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

Add the domain NEARDOM to the exclusion list for a Connection Server group.

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

Display the domain search configuration on both Connection Server instances in the group, and for the group.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :
```

```
Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

Horizon 7 limits the domain search on each Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that Horizon 7 excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

Display the domain filters in XML using ASCII characters.

```
vdmadmin -N -domains -list -xml -n
```

Display the domains that are available to Horizon 7 on the local Connection Server instance.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Display the available domains in XML using ASCII characters.

```
vdmadmin -N -domains -list -active -xml -n
```

Remove the domain NEARDOM from the exclusion list for a Connection Server group.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

Remove all domains from the inclusion list for the Connection Server instance csvr1.

```
vdmadmin -N -domains -include -removeall -s csvr1
```

Configuring Domain Filters

You can configure domain filters to limit the domains that a Connection Server instance or security server makes available to end users.

Horizon 7 determines which domains are accessible by traversing trust relationships, starting with the domain in which a Connection Server instance or security server resides. For a small, well-connected set of domains, Horizon 7 can quickly determine a full list of domains, but the time that this operation takes increases as the number of domains increases or as the connectivity between the domains decreases. Horizon 7 might also include domains in the search results that you would prefer not to offer to users when they log in to their remote desktops.

If you have previously set the value of the Windows registry key that controls recursive domain enumeration (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) to false, recursive domain searching is disabled, and the Connection Server instance uses only the primary domain. To use the domain filtering feature, delete the registry key or set its value to true, and restart the system. You must do this for every Connection Server instance on which you have set this key.

The following table shows the types of domain lists that you can specify to configure domain filtering.

Table 12-13. Types of Domain List

Domain List Type	Description
Search exclusion list	Specifies the domains that Horizon 7 can traverse during an automated search. The search ignores domains that are included in the search exclusion list, and does not attempt to locate domains that the excluded domain trusts. You cannot exclude the primary domain from the search.
Exclusion list	Specifies the domains that Horizon 7 excludes from the results of a domain search. You cannot exclude the primary domain.
Inclusion list	Specifies the domains that Horizon 7 does not exclude from the results of a domain search. All other domains are removed apart from the primary domain.

The automated domain search retrieves a list of domains, excluding those domains that you specify in the search exclusion list and domains that are trusted by those excluded domains. Horizon 7 selects the first non-empty exclusion or inclusion list in this order.

1 Exclusion list configured for the Connection Server instance.

2 Exclusion list configured for the Connection Server group.

3 Inclusion list configured for the Connection Server instance.

4 Inclusion list configured for the Connection Server group

Horizon 7 applies only the first list that it selects to the search results.

If you specify a domain for inclusion, and its domain controller is not currently accessible, Horizon 7 does not include that domain in the list of active domains.

You cannot exclude the primary domain to which a Connection Server instance or security server belongs.

Example of Filtering to Include Domains

You can use an inclusion list to specify the domains that Horizon 7 does not exclude from the results of a domain search. All other domains, apart from the primary domain, are removed.

A Connection Server instance is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX domain.

Display the currently active domains for the Connection Server instance.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains appear in the list because they are trusted domains of the DEPTX domain.

Specify that the Connection Server instance should make only the YOURDOM and DEPTX domains available, in addition to the primary MYDOM domain.

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

Display the currently active domains after including the YOURDOM and DEPTX domains.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 applies the include list to the results of a domain search. If the domain hierarchy is very complex or network connectivity to some domains is poor, the domain search can be slow. In such cases, use search exclusion instead.

Example of Filtering to Exclude Domains

You can use an inclusion list to specify the domains that Horizon 7 excludes from the results of a domain search.

A group of two Connection Server instances, CONSVR-1 and CONSVR-2, is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX and FARDOM domains.

The FARDOM domain is in a remote geographical location, and network connectivity to that domain is over a slow, high-latency link. There is no requirement for users in the FARDOM domain to be able to access the Connection Server group in the MYDOM domain.

Display the currently active domains for a member of the Connection Server group.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains are trusted domains of the DEPTX domain.

To improve connection performance for Horizon Client, exclude the FARDOM domain from being searched by the Connection Server group.

```
vdmadmin –N –domains –search –domain FARDOM –add
```

The command displays the currently active domains after excluding the FARDOM domain from the search.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Extend the search exclusion list to exclude the DEPTX domain and all its trusted domains from the domain search for all Connection Server instances in a group. Also, exclude the YOURDOM domain from being available on CONSVR-1.

```
vdmadmin –N –domains –search –domain DEPTX –add
vdmadmin –N –domains –exclude –domain YOURDOM –add –s CONSVR–1
```

Display the new domain search configuration.

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR-1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

Horizon 7 limits the domain search on each Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that Horizon 7 excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

On CONSVR-1, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

On CONSVR-2, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options

You can use the `vdmadmin` command with the `–O` and `–P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.

Syntax

```
vdmadmin –O [–b authentication_arguments] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath path]]
```

```
vdmadmin –P [–b authentication_arguments] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath path]]
```

Usage Notes

If you revoke a user's entitlement to a persistent virtual machine or to a physical system, the associated remote desktop assignment is not automatically revoked. This condition might be acceptable if you have temporarily suspended a user’s account or if the user is on a sabbatical. When you reenable entitlement, the user can continue using the same virtual machine as previously. If a user has left the organization, other users cannot access the virtual machine, and it is considered to be orphaned. You might also want to examine any policies that are assigned to unentitled users.

Options

The following table shows the options that you can specify to display the virtual machines and policies of unentitled users.

Table 12-14. Options for Displaying the Machines and Policies of Unentitled Users

Option	Description
`–ld`	Orders output entries by machine.
`–lu`	Orders output entries by user.
`–noxslt`	Specifies that the default stylesheet should not be applied to the XML output.
`–xsltpath` *path*	Specifies the path to the stylesheet that is used to transform XML output.

Table 12-15 shows the stylesheets that you can apply to the XML output to transform it into HTML. The stylesheets are located in the directory `C:\Program Files\VMware\VMware View\server\etc`.

Table 12-15. XSL Stylesheets

Stylesheet File Name	Description
`unentitled-machines.xsl`	Transforms reports containing a list of unentitled virtual machines, grouped either by user or system, and which are currently assigned to a user. This is the default stylesheet.
`unentitled-policies.xsl`	Transforms reports containing a list of virtual machines with user-level policies that are applied to unentitled users.

Examples

Display the virtual machines that are assigned to unentitled users, grouped by virtual machine in text format.

```
vdmadmin -O -ld
```

Display virtual machines that are assigned to unentitled users, grouped by user, in XML format using ASCII characters.

```
vdmadmin -O -lu -xml -n
```

Apply your own stylesheet `C:\tmp\unentitled-users.xsl` and redirect the output to the file `uu-output.html`.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

Display the user policies that are associated with unentitled users' virtual machinse, grouped by desktop, in XML format using Unicode characters.

```
vdmadmin -P -ld -xml -w
```

Apply your own stylesheet `C:\tmp\unentitled-policies.xsl` and redirect the output to the file `up-output.html`.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

Configuring Clients in Kiosk Mode Using the -Q Option

You can use the `vdmadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

Syntax

```
vdmadmin –Q –clientauth –add [–b authentication_arguments] –domain domain_name–clientid client_id
[–password "password" | –genpassword] [–ou DN] [–expirepassword | –noexpirepassword] [–group
group_name | –nogroup] [–description "description_text"]
```

```
vdmadmin –Q –disable [–b authentication_arguments] –s connection_server
```

```
vdmadmin –Q –enable [–b authentication_arguments] –s connection_server [–requirepassword]
```

```
vdmadmin –Q –clientauth –getdefaults [–b authentication_arguments] [–xml]
```

```
vdmadmin –Q –clientauth –list [–b authentication_arguments] [–xml]
```

```
vdmadmin –Q –clientauth –remove [–b authentication_arguments] –domain domain_name–clientid client_id
```

```
vdmadmin –Q –clientauth –removeall [–b authentication_arguments] [–force]
```

```
vdmadmin –Q –clientauth –setdefaults [–b authentication_arguments] [–ou DN] [ –expirepassword |
–noexpirepassword ] [–group group_name | –nogroup]
```

```
vdmadmin –Q –clientauth –update [–b authentication_arguments] –domain domain_name–clientid client_id
[–password "password" | –genpassword] [–description "description_text"]
```

Usage Notes

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients use to connect to their remote desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all Connection Server instances in a group.

When you add a client in kiosk mode, Horizon 7 creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with the characters "custom-" or with one of the alternate strings that you can define in ADAM, and it cannot be more than 20 characters long. You should use each specified name with no more than one client device.

You can define alternate prefixes to "custom-" in the `pae-ClientAuthPrefix` multi-valued attribute under `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM on a Connection Server instance. Avoid using these prefixes with ordinary user accounts.

If you do not specify a name for a client, Horizon 7 generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with Connection Server instances that you enable to authenticate clients.

Some thin clients allow only account names that start with the characters "custom-" or "cm-" to be used with kiosk mode.

An automatically generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, you must use the `–password` option to specify the password.

If you use the `–group` option to specify a group or you have previously set a default group, Horizon 7 adds the client's account to this group. You can specify the `–nogroup` option to prevent the account being added to any group.

If you enable a Connection Server instance to authenticate clients in kiosk mode, you can optionally specify that clients must provide a password. If you disable authentication, clients cannot connect to their remote desktops.

Although you enable or disable authentication for an individual Connection Server instance, all Connection Server instances in a group share all other settings for client authentication. You need only add a client once for all Connection Server instances in a group to be capable of accepting requests from the client.

If you specify the `–requirepassword` option when enabling authentication, the Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a Connection Server instance to specify this option, such clients cannot authenticate themselves, and they fail with the error message `Unknown username or bad password`.

Options

The following table shows the options that you can specify to configure clients in kiosk mode.

Table 12-16. Options for Configuring Clients in Kiosk Mode

Option	Description
`–add`	Adds an account for a client in kiosk mode.
`–clientauth`	Specifies an operation that configures authentication for a client in kiosk mode.
`–clientid` *client_id*	Specifies the name or the MAC address of the client.
`–description` "*description_text*"	Creates a description of the account for the client device in Active Directory.
`–disable`	Disables authentication of clients in kiosk mode on a specified Connection Server instance.
`–domain` *domain_name*	Specifies the domain for the account for the client device.
`–enable`	Enables authentication of clients in kiosk mode on a specified Connection Server instance.

Table 12-16. Options for Configuring Clients in Kiosk Mode (Continued)

Option	Description
`–expirepassword`	Specifies that the expiry time for the password on client accounts is the same as for the Connection Server group. If no expiry time is defined for the group, passwords do not expire.
`–force`	Disables the confirmation prompt when removing the account for a client in kiosk mode.
`–genpassword`	Generates a password for the client's account. This is the default behavior if you do not specify either `–password` or `–genpassword`.
`–getdefaults`	Gets the default values that are used for adding client accounts.
`–group` *group_name*	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.
`–list`	Displays information about clients in kiosk mode and about the Connection Server instances on which you have enabled authentication of clients in kiosk mode.
`–noexpirepassword`	Specifies that the password on an account does not expire.
`–nogroup`	When adding an account for a client, specifies that the client's account is not added to the default group. When setting the default values for clients, clears the setting for the default group.
`–ou` *DN*	Specifies the distinguished name of the organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com **Note** You cannot use the `–setdefaults` option to change the configuration of an organizational unit.
`–password` "*password*"	Specifies an explicit password for the client's account.
`–remove`	Removes the account for a client in kiosk mode.
`–removeall`	Removes the accounts of all clients in kiosk mode.
`–requirepassword`	Specifies that clients in kiosk mode must provide passwords. Horizon 7 will not accept generated passwords for new connections.
`–s` *connection_server*	Specifies the NetBIOS name of the Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
`–setdefaults`	Sets the default values that are used for adding client accounts.
`–update`	Updates an account for a client in kiosk mode.

Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group kc–grp
```

Get the current default values for clients in plain text format.

```
vdmadmin –Q –clientauth –getdefaults
```

Get the current default values for clients in XML format.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –group kc–grp
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –
description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin –Q –clientauth –removeall –force
```

Enable authentication of clients for the Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Disable authentication of clients for the Connection Server instance csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password, and requires the end user to provide this. The Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
==============================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Displaying the First User of a Machine Using the -R Option

You can use the `vdmadmin` command with the `–R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.

Note The `vdmadmin` command with the `–R` option works only on virtual machines that are earlier than View Agent 5.1. On virtual machines that run View Agent 5.1 and later and Horizon Agent 7.0 and later versions, this option does not work. To locate the first user of a virtual machine, use the Events database to determine which users logged into the machine.

Syntax

```
vdmadmin –R –i network_address
```

Usage Notes

You cannot use the `–b` option to run this command as a privileged user. You must be logged in as a user in the **Administrator** role.

Options

The `–i` option specifies the IP address of the virtual machine.

Examples

Display the first user who accessed the virtual machine at the IP address 10.20.34.120.

```
vdmadmin –R –i 10.20.34.120
```

Removing the Entry for a Connection Server Instance or Security Server Using the -S Option

You can use the `vdmadmin` command with the `–S` option to remove the entry for a Connection Server instance or security server from the Horizon 7 configuration.

Syntax

```
vdmadmin –S [–b authentication_arguments] –r –s server
```

Usage Notes

To ensure high availability, Horizon 7 allows you to configure one or more replica Connection Server instances in a Connection Server group. If you disable a Connection Server instance in a group, the entry for the server persists within the Horizon 7 configuration.

You can also use the `vdmadmin` command with the `–S` option to remove a security server from your Horizon 7 environment. You do not have to use this option if you intend to upgrade or reinstall a security server without removing it permanently.

To make the removal permanent, perform these tasks:

1 Uninstall the Connection Server instance or security server from the Windows Server computer by running the Connection Server installer.

2 Remove the Adam Instance VMwareVDMDS program from the Windows Server computer by running the Add or Remove Programs tool.

3 On another Connection Server instance, use the `vdmadmin` command to remove the entry for the uninstalled Connection Server instance or security server from the configuration.

If you want to reinstall Horizon 7 on the removed systems without replicating the Horizon 7 configuration of the original group, restart all the Connection Server hosts in the original group before performing the reinstallation. This prevents the reinstalled Connection Server instances from receiving configuration updates from their original group.

Options

The `–s` option specifies the NetBIOS name of the Connection Server instance or security server to be removed.

Examples

Remove the entry for the Connection Server instance connsvr3.

```
vdmadmin –S –r –s connsvr3
```

Providing Secondary Credentials for Administrators Using the -T Option

You can use the `vdmadmin` command with the `–T` option to provide Active Directory secondary credentials to administrator users.

Syntax

```
vdmadmin –T [–b authentication_arguments] –domainauth
 {–add | –update | –remove | –removeall | –list} –owner domain\user –user domain\user [–password
password]
```

Usage Notes

If your users and groups are in a domain with a one-way trust relationship with the Connection Server domain, you must provide secondary credentials for the administrator users in Horizon Administrator. Administrators must have secondary credentials to give them access to the one-way trusted domains. A one-way trusted domain can be an external domain or a domain in a transitive forest trust.

Secondary credentials are required only for Horizon Administrator sessions, not for end users' desktop or application sessions. Only administrator users require secondary credentials.

With the `vdmadmin` command, you configure secondary credentials on a per-user basis. You cannot configure globally specified secondary credentials.

For a forest trust, you typically configure secondary credentials only for the forest root domain. Connection Server can then enumerate the child domains in the forest trust.

Active Directory account lock, disable, and logon hours checks can be performed only when a user in a one-way trusted domain first logs on.

PowerShell administration and smart card authentication of users is not supported in one-way trusted domains. SAML authentication of users in one-way trusted domains is not supported.

Secondary credential accounts require the following permissions. A standard user account should have these permissions by default.

- List Contents
- Read All Properties
- Read Permissions
- Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

Limitations

- PowerShell administration and smart card authentication of users in one-way trusted domains is not supported.
- SAML authentication of users in one-way trusted domains is not supported.

Options

Table 12-17. Options for Providing Secondary Credentials

Option	Description
`–add`	Adds a secondary credential for the owner account. A Windows logon is performed to verify that the specified credentials are valid. A foreign security principal (FSP) is created for the user in View LDAP.
`–update`	Updates a secondary credential for the owner account. A Windows logon is performed to verify that the updated credentials are valid.
`–list`	Displays the security credentials for the owner account. Passwords are not displayed.
`–remove`	Removes a security credential from the owner account.
`–removeall`	Removes all security credentials from the owner account.

Examples

Add a secondary credential for the specified owner account. A Windows logon is performed to verify that the specified credentials are valid.

```
vdmadmin –T –domainauth –add –owner domain\user –user domain\user –password password
```

Update a secondary credential for the specified owner account. A Windows logon is performed to verify that the updated credentials are valid.

```
vdmadmin –T –domainauth –update –owner domain\user –user domain\user –password password
```

Remove a secondary credential for the specified owner account.

```
vdmadmin –T –domainauth –remove –owner domain\user –user domain\user
```

Remove all secondary credentials for the specified owner account.

```
vdmadmin –T –domainauth –removeall –owner domain\user
```

Display all secondary credentials for the specified owner account. Passwords are not displayed.

```
vdmadmin –T –domainauth –list –owner domain\user
```

Displaying Information About Users Using the -U Option

You can use the `vdmadmin` command with the `–U` option to display detailed information about users.

Syntax

```
vdmadmin –U [–b authentication_arguments] –u domain\user [–w | –n] [–xml]
```

Usage Notes

The command displays information about a user obtained from Active Directory and Horizon 7.

- Details from Active Directory about the user's account.
- Membership of Active Directory groups.
- Machine entitlements including the machine ID, display name, description, folder, and whether a machine has been disabled.
- ThinApp assignments.
- Administrator roles including the administrative rights of a user and the folders in which they have those rights.

Options

The –u option specifies the name and domain of the user.

Examples

Display information about the user Jo in the CORP domain in XML using ASCII characters.

```
vdmadmin –U –u CORP\Jo –n –xml
```

Unlocking or Locking Virtual Machines Using the -V Option

You can use the vdmadmin command with the –V option to unlock or lock virtual machines in the data center.

Syntax

```
vdmadmin –V [–b authentication_arguments] –e –d desktop –m machine [–m machine] ...
```

```
vdmadmin –V [–b authentication_arguments] –e –vcdn vCenter_dn –vmpath inventory_path
```

```
vdmadmin –V [–b authentication_arguments] –p –d desktop –m machine [–m machine] ...
```

```
vdmadmin –V [–b authentication_arguments] –p –vcdn vCenter_dn –vmpath inventory_path
```

Usage Notes

You should only use the `vdmadmin` command to unlock or lock a virtual machine if you encounter a problem that has left a remote desktop in an incorrect state. Do not use the command to administer remote desktops that are operating normally.

If a remote desktop is locked and the entry for its virtual machine no longer exists in ADAM, use the `–vmpath` and `–vcdn` options to specify the inventory path of the virtual machine and the vCenter Server. You can use vCenter Client to find out the inventory path of a virtual machine for a remote desktop under `Home/Inventory/VMs and Templates`. You can use ADAM ADSI Edit to find out the distinguished name of the vCenter Server under the `OU=Properties` heading.

Options

The following table shows the options that you can specify to unlock or lock virtual machines.

Table 12-18. Options for Unlocking or Locking Virtual Machines

Option	Description
`–d` *desktop*	Specifies the desktop pool.
`–e`	Unlocks a virtual machine.
`–m` *machine*	Specifies the name of the virtual machine.
`–p`	Locks a virtual machine.
`–vcdn` *vCenter_dn*	Specifies the distinguished name of the vCenter Server.
`–vmpath` *inventory_path*	Specifies the inventory path of the virtual machine.

Examples

Unlock the virtual machines machine 1 and machine2 in desktop pool dtpool3.

```
vdmadmin –V –e –d dtpool3 –m machine1 –m machine2
```

Lock the virtual machine machine3 in desktop pool dtpool3.

```
vdmadmin –V –p –d dtpool3 –m machine3
```

Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option

You can use the `vdmadmin` command with the `–X` option to detect and resolve LDAP entry collisions and LDAP schema collisions on replicated Connection Server instances in a group. You can also use this option to detect and resolve LDAP schema collisions in a Cloud Pod Architecture environment.

Syntax

```
vdmadmin -X [-b authentication_arguments] -collisions [-resolve]
vdmadmin -X [-b authentication_arguments] -schemacollisions [-resolve] [-global]
```

Usage Notes

Duplicate LDAP entries on two or more Connection Server instances can cause problems with the integrity of LDAP data in Horizon 7. This condition can occur during an upgrade, while LDAP replication is inoperative. Although Horizon 7 checks for this error condition at regular intervals, you can run the `vdmadmin` command on one of the Connection Server instances in the group to detect and resolve LDAP entry collisions manually.

LDAP schema collisions can also occur during an upgrade, while LDAP replication is inoperative. Because Horizon 7 does not check for this error condition, you must run the `vdmadmin` command to detect and resolve LDAP schema collisions manually.

Options

The following table shows the options that you can specify to detect and resolve LDAP entry collisions.

Table 12-19. Options for Detecting and Resolving LDAP Entry Collisions

Option	Description
`-collisions`	Specifies an operation for detecting LDAP entry collisions in a Connection Server group.
`-resolve`	Resolves all LDAP collisions in the LDAP instance. If you do not specify this option, the command only lists the problems that it finds.

The following table shows the options that you can specify to detect and resolve LDAP schema collisions.

Table 12-20. Options for Detecting and Resolving LDAP Schema Collisions

Option	Description
`-schemacollisions`	Specifies an operation for detecting LDAP schema collisions in a Connection Server group or Cloud Pod Architecture environment.
`-resolve`	Resolves all LDAP schema collisions in the LDAP instance. If you do not specify this option, the command only lists the problems that it finds.
`-global`	Applies the checks and fixes to the global LDAP instance in a Cloud Pod Architecture environment. If you do not specify this option, the checks are run against the local LDAP instance.

Examples

Detect LDAP entry collisions in a Connection Server group.

```
vdmadmin –X –collisions
```

Detect and resolve LDAP entry collisions in the local LDAP instance.

```
vdmadmin –X –collisions –resolve
```

Detect and resolve LDAP schema collisions in the global LDAP instance.

```
vdmadmin –X –schemacollisions –resolve –global
```