Horizon Administration

VMware Horizon 2106

vmware®

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

https://docs.vmware.com/

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

Contents

VMware Horizon Administration

1

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

VMware Horizon Console is the latest version of the Web interface through which you can create and manage virtual desktops and published desktops and applications.

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

Intended Audience

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

Using VMware Horizon Console 2

VMware Horizon Console is the web interface for VMware Horizon through which you can create and manage virtual desktops and published desktops and applications.

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

This chapter includes the following topics:

Log In to Horizon Console

To perform desktop or application pool deployment tasks, or monitoring and troubleshooting tasks, you must log in to Horizon Console. You access Horizon Console 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 Console. For more information about supported Web browsers, see the *Horizon 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 contacted host will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security. VMware recommends using the FQDN instead of the IP address.

   Your access to Horizon Console 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.

Note If you use an older Web browser such as Internet Explorer 11, a pop-up window appears that displays the Web browsers you should use for the best user experience for Horizon Console. You can also click on your preferred Web browser in the pop-up window to download the Web browser.

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

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

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

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

3 Optionally, to remember the user name for every login, select **Remember user name**.

4 Click **Sign In**.

What to do next

You can also right-click any link in Horizon Console to open in another web browser tab.

Tips for Using the Horizon Console Interface

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

Horizon Console includes many common user interface features. For example, the navigation pane on the left side of each page directs you to other Horizon Console 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 Console.

Table 2-1. Horizon Console Navigation and Display Features

Horizon Console Feature	Description
Navigating backward and forward in Horizon Console pages	Click your browser's **Back** button to go to the previously displayed Horizon Console 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 Console wizard or dialog box, you return to the main Horizon Console page. The information you entered in the wizard or dialog is lost.
Bookmarking Horizon Console pages	You can bookmark Horizon Console 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 Console table to sort the Horizon objects in alphabetical order based on that heading. To sort the Horizon objects by a secondary item, Ctrl+click another heading. 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.
Customizing table columns	You can customize the display of Horizon Console table columns by hiding selected columns and locking the first column. This feature lets you control the display of large tables 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.
Selecting Horizon objects and displaying Horizon object details	In Horizon Console 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 **Inventory > Desktops** 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 Console 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 web browser operations on Horizon objects	You can right-click Horizon objects in Horizon Console tables to display context menus to perform web browser operations such as opening the object in another tab or window.

Configuring Horizon Connection Server

3

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

This chapter includes the following topics:

Configuring vCenter Server in Horizon Console

To use VMware vSphere virtual machines as remote desktops, you must configure VMware Horizon to communicate with vCenter Server.

For more information, see "Add vCenter Server Instances to VMware Horizon" in the *Horizon Installation* document.

Remove a vCenter Server Instance from VMware Horizon

You can remove the connection between VMware Horizon and a vCenter Server instance. When you do so, VMware Horizon 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* document.

Procedure

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

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

3 Click **Remove**.

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

4 Click **OK**.

Results

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

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 VMware Horizon, 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.

Disable or Enable Horizon Connection Server in Horizon Console

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

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

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

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

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

Procedure

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

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

3 Click **Disable**.

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

Understanding VMware Horizon Services

The operation of Connection Server instances 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 VMware Horizon services. If you stop VMware Horizon services on a Connection Server host, 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 VMware Horizon functionality that it controls appears to be unresponsive.

Stop and Start VMware Horizon Services

The operation of Connection Server instances 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 VMware Horizon.

When you stop VMware Horizon 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 Connection Server service on a Connection Server host. Do not stop any other component services.

Prerequisites

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

Procedure

1 Start the Windows Services tool by entering **`services.msc`** at the command prompt.

2 Select the VMware Horizon Connection Server service on a Connection Server host 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 VMware Horizon depends on several services that run on a Connection Server host.

Table 3-1. Horizon Connection Server Host Services

Service Name	Startup Type	Description
VMware Horizon 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 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 Script Host service.
VMware Horizon Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.
VMware Horizon Message Bus Component	Manual	Provides messaging services between the VMware Horizon components. This service must always be running.
VMware Horizon 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 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 Security Gateway Component	Manual	Provides common gateway services. This service must always be running.
VMware Horizon Web Component	Manual	Provides web services. This service must always be running.
VMwareVDMDS	Automatic	Provides Horizon LDAP services. This service must always be running. During upgrades of VMware Horizon, this service ensures that existing data is migrated correctly.

Configuring Untrusted Domains

You can add user domains that do not have a formal trust relationship with the Connection Server domain. Setting up a one-way or two-way trust relationship between the Connection Server domain and the user's domain is often times an intrusive activity into the user's Active Directory (AD) infrastructure. Instead, you can deploy VMware Horizon in a separate domain and set up communication with the user domain by configuring it as an untrusted domain.

Establishing an untrusted relationship can be an easier set up to manage in some scenarios such as when you have a cloud-hosted Connection Server domain communicating with an on-premises user domain.

You can create a primary domain bind account to set up the untrusted relationship between the Connection Server domain and another domain. Horizon uses the domain bind account to query and perform lookups in Active Directory. You can also add multiple auxiliary accounts in case the primary domain bind account becomes inaccessible or locked out.

When configured, Horizon uses the auxiliary domain bind account to query and perform lookups in Active Directory.

In Horizon Console, you can view the configured untrusted domains on the **Domain Bind** tab and information and trust relationships for Connection Server domains on the **Connection Server** tab by navigating to **Settings > Domains**.

When an untrusted domain is configured successfully and later on an administrator establishes a formal trust relationship (one-way or two-way) of the untrusted domain with a Connection Server domain, the untrusted domain will be treated as a Connection Server domain. The untrusted domain will no longer appear in **Domains > Domain Bind** tab and will appear in **Domains > Connection Server** tab.

Users belonging to an untrusted domain can use SAML authentication and smart card authentication. To use SAML authentication, see Using SAML Authentication. Users belonging to an untrusted domain can also use True SSO with SAML authentication. To use smart card authentication, see Chapter 4 Setting Up Smart Card Authentication.

Domain Bind Account Properties

When you create a domain bind account, you must specify certain account configuration and Active Directory (AD) registration properties. Horizon uses the domain bind account as the primary service account to connect to the Active Directory server of an untrusted user domain and query Active Directory.

Table 3-2. Domain Bind Account Properties

Properties	Description
DNS Name	Fully qualified Active Directory domain name.
Netbios	Active Directory NetBIOS domain name.
Protocol	(Not editable) LDAP is the only supported protocol.
Primary Service Account	Credentials for the primary domain bind service account: ■ **User name**. User name of the primary domain bind administrator. ■ **Password**. Password of the primary domain bind administrator.
Port	The default port is 389 (LDAP). You do not need to modify this text box unless you are using a non-standard port.

Table 3-2. Domain Bind Account Properties (continued)

Properties	Description
Context	LDAP naming context relevant for the DNS domain name. This field is automatically populated from the DNS name. For example, "dc=horizon,dc=example,dc=com".
Automatic	Select this option to automatically discover domain controllers.
Domain Controller IPs	Specify which domain controller IPs to use to communicate with this Active Directory. Multiple IPs can be provided as a comma separated list.
Sitename	Preferred site to search the domain controller or controllers.

Add a Domain Bind Account

Add a primary domain bind account to set up the untrusted relationship between the Connection Server domain and a different domain.

Prerequisites

- Verify that you have prepared Active Directory for the Connection Server's domain. See "Preparing Active Directory" in the *Horizon Installation* document.
- Gather the untrusted domain bind account properties. See, Domain Bind Account Properties.
- Verify that the Connection Server domain is not in any formal trust relationship with the target user domain. You can view the domain information for the Connection Server domain by navigating to **Settings > Domain** and clicking the **Connection Server** tab.
- Verify that your DNS infrastructure can resolve untrusted domain FQDN from each Connection Server successfully.
- Verify that the Connection Server machine and the untrusted domain's domain controller are synchronized in time.

Procedure

1. In Horizon Console, navigate to **Settings > Domain**.
2. Click the **Domain Bind** tab.
3. Click **Add** to add an untrusted domain bind account.
4. Enter the untrusted domain bind account properties.
5. (Optional) Select **Add auxiliary account after adding No Trust Domain Account** to add an auxiliary domain bind account.

   In the **Manage Auxiliary Account** window, click **Add** and enter the user name and password for auxiliary domain bind account user, then click **OK**.
6. Click **OK**.

Results

On the **Domain Bind** tab, you can view the primary domain bind account under the **Service Account** column.

What to do next

Add auxiliary domain bind accounts. See Manage Auxiliary Domain Bind Accounts.

Manage Auxiliary Domain Bind Accounts

After you add a primary domain bind account, you can add, edit, and remove auxiliary domain bind accounts. You can also add multiple auxiliary domain bind accounts. When configured, Horizon will use an auxiliary domain bind account if the primary domain bind account is inaccessible or locked out.

Prerequisites

Verify that you have added a domain bind account. See Add a Domain Bind Account .

Procedure

1. In Horizon Console, navigate to **Settings > Domain**.
2. Click the **Domain Bind** tab.
3. Select an untrusted domain.
4. Click **Manage Auxiliary Accounts**.
5. Enter a user name and password for the auxiliary account.
6. (Optional) Click **Add** to add another auxiliary account and enter the user name and password for the auxiliary account user.

   Optionally, you can also edit or remove auxiliary accounts. Click **Edit** to edit the user name and password for the auxiliary account user. Click **Remove** to remove the auxiliary account.

   Note An auxiliary domain bind account user can edit a password, but not the username of the auxiliary account.
7. Click **OK**.

Results

On the **Domain Bind** tab, you can view the number of auxiliary accounts added under the **Auxiliary Accounts** column.

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" in the *Horizon Installation* document.

Prerequisites

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

Procedure

1. In Horizon Console, select **Settings > Global Settings**.
2. Choose whether to configure general settings, security settings, or client restriction settings.

Option	Description
General global settings	In the **General Settings** tab, click **Edit**.
Global security settings	In the **Security Settings** tab, click **Edit**.
Global client restrictions settings	In the **Client Restrictions Settings** tab, 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" in the *Horizon Security* document.

Global Settings for Client Sessions

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

In Horizon Console, you can configure global settings by navigating to **Settings > Global Settings > General Settings** .

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

Table 3-3. General Global Settings for Client Sessions

Setting	Description
View API Session Timeout	Determines how long an idle View API session continues before the View API session times out. **Important** Setting the View API session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Console. Use caution when you allow an idle session to persist a long time. By default, the View API session timeout is 10 minutes. You can set a session timeout from 10 to 4320 minutes (72 hours).
Connection Server Session Timeout	Determines how long an idle Horizon Console session continues before the Connection Server session times out. **Important** Setting the Horizon Console session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Console. Use caution when you allow an idle session to persist a long time. Before a session times out, a warning message appears with a 60 second countdown. If you click in the session before the countdown ends, the session continues. After 60 seconds, an error message appears informing you that the session has timed out and you need to log in again. You can set a minimum Connection Server session timeout of 2 minutes and a maximum Connection Server session timeout of 4320 minutes (72 hours). To override the **Connection Server Session Timeout** value and configure your own user preference for how long an idle Horizon Console session times out, in the Horizon Console header, click **Settings**. In the **My Preferences** dialog box, enter a value for **Connection Server Session Timeout Override**.
Forcibly disconnect users	Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to VMware Horizon. 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**.

Table 3-3. General Global Settings for Client Sessions (continued)

Setting	Description
Single sign-on (SSO)	If SSO is enabled, VMware Horizon 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 VMware Horizon 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 VMware Horizon Agent 6.0 or later or Horizon Agent 7.0 or later, 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 Connection Server or exit Horizon Client, and reconnect to Connection Server. However, if the desktop is launched from Workspace ONE or VMware Identity Manager and the desktop is locked, SSO credentials are not discarded.
Enable automatic status updates	Determines if status updates appear in the global status pane in the upper-left corner of Horizon Console every few minutes. The dashboard page of Horizon Console is also updated every few minutes. By default, this setting is not enabled.
For clients that support applications Disconnect Applications and Discard SSO credentials for Idle Users	Protects application sessions when there is no keyboard or mouse activity on the client device. If set to **After ... minutes**, VMware Horizon 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**, VMware Horizon never disconnects applications or discards SSO credentials due to user inactivity. Do not enable **Bypass Session Timeout** for a farm or application pool. The default is **Never**.
Other clients Discard SSO credentials	Discards SSO credentials after the specified number of minutes. This setting is for clients that do not support application remoting. If set to **After ... minutes**, users must log in again to connect to a desktop after the specified number of minutes has passed since the user logged in to VMware Horizon, regardless of any user activity on the client device. If set to **Never**, VMware Horizon 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**.

Table 3-3. General Global Settings for Client Sessions (continued)

Setting	Description
Display a pre-login message	Displays a disclaimer or another message to Horizon Client users when they log in. Type your information or instructions in the text box in the Global Settings dialog box. To display no message, leave the check box unselected.
Display warning before forced logoff	Displays a warning message when users are forced to log off because a scheduled or immediate update such as a desktop-refresh operation is about to start. This setting also determines how long to wait after the warning is shown before the user is logged off. Check the box to display a warning message. Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is 5 minutes. Type your warning message. You can use the default message: `Your desktop is scheduled for an important update and will be shut down in 5 minutes. Please save any unsaved work now.`
Enable Windows Server desktops	Determines whether you can select available Windows Server 2008 R2 and Windows Server 2012 R2 machines for use as desktops. When this setting is enabled, Horizon Console displays all available Windows Server machines, including machines on which VMware Horizon server components are installed. **Note** The Horizon Agent software cannot coexist on the same virtual or physical machine with any other VMware Horizon server software component, including a Connection Server.
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, VMware Horizon 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. Enabling this setting also affects how HTML Access behaves when it is started from Workspace ONE. For more information, see the Workspace ONE documentation. When this setting is disabled, the credentials remain in cache. This feature is disabled by default.
Hide server information in client user interface	Enable this security setting to hide server URL information in Horizon Client.

Table 3-3. General Global Settings for Client Sessions (continued)

Setting	Description
Hide domain list in client user interface	Enable this security setting to hide the Domain drop-down menu in Horizon Client. When users log in to a Connection Server instance for which the **Hide domain list in client user interface** global setting is enabled, the Domain drop-down menu is hidden in Horizon Client and users provide domain information in the Horizon Client **User name** text box. For example, users must enter their user name in the format `domain\username` or `username@domain`. **Important** If you enable the **Hide domain list in client user interface** setting and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching prevents users from entering domain information in the user name text box and login always fails. This does not apply to Horizon Client version 5.0 and later if there is a single user domain. **Important** For more information about the security and usability implications of this setting, see the *Horizon Security* document.
Send domain list	Select the checkbox to allow the Connection Server to send the list of domain names to the client before the user is authenticated. **Important** For more information about the security and usability implications of this setting, see the *Horizon Security* document.
Enable 2 Factor Reauthentication	Select this setting to enable two-factor authentication to occur for an end user after a session times out.

Global Security Settings for Client Sessions and Connections

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

In Horizon Console, you can configure global security settings by navigating to **Settings > Global Settings > Security Settings** .

TLS is required for all Horizon Client connections and Horizon Console connections to VMware Horizon. If your VMware Horizon 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.

Table 3-4. 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 VMware Horizon components takes place. ■ When the mode is set to **Enhanced**, security is provided by mutually authenticated TLS. JMS connections and access control on JMS topics. For new installations, by default, message security mode is set to **Enhanced**. If you upgrade from a previous version, the setting used in the previous version is retained.
Enhanced Security Status (Read-only)	Read-only field that appears when **Message security mode** is changed from **Enabled** to **Enhanced**. Because the change is made in phases, this field shows the progress through the phases: ■ **Waiting for Message Bus restart** is the first phase. This state is displayed until you manually restart either all Connection Server instances in the pod or the VMware Horizon Message Bus Component service on all Connection Server hosts in the pod. ■ **Pending Enhanced** is the next state. After all Horizon Message Bus Component services have been restarted, the system begins changing the message security mode to **Enhanced** for all desktops. ■ **Enhanced** is the final state, indicating that all components are now using **Enhanced** message security mode.

Global Client Restriction Settings for Client Sessions

Global client restriction settings can restrict launching of virtual desktops, published desktops, and published applications to specific clients and versions, and also provide warning messages to clients.

In Horizon Console, you can configure global client restriction settings by navigating to **Settings > Global Settings > Client Restriction Settings**.

Client restrictions are available for Horizon Client versions 4.5.0 or later, except Horizon Client for Chrome, which must be version 4.8.0 or later. Either specific or earlier versions of Horizon Client for the client type are prevented from connecting to remote desktops and published applications when this feature is configured. The capability to show warning messages to specific client versions is available for Horizon Client 2006 or later.

Note Client restriction settings only prevent end users from launching remote desktops and published applications. This feature does not prevent end users from logging in to VMware Horizon.

Table 3-5. Global Client Restriction Settings for Client Sessions

Setting	Description
Horizon Client for Windows	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.
Horizon Client for Linux	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.
Horizon Client for Mac	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.

Table 3-5. Global Client Restriction Settings for Client Sessions (continued)

Setting	Description
Horizon Client for iOS	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.
Horizon Client for Android	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.
Horizon Client for UWP	Enter a Horizon Client version number to block all clients earlier than that version.
Horizon Client for Chrome	For the **Block Connections from Client Version(s)** setting, select one of these options: ■ **Earlier than**: specify the earliest client version to block all clients earlier than that version. ■ **Specific**: enter specific versions (separated by commas) that block users when they connect with those client versions. For the **Warn Users Connecting from Specific Client Version(s)** setting, enter comma separated versions to warn users connecting from those client versions. The warning for Horizon Client version 5.5.0 is enabled by default. You can remove this version to disable the warning.
Horizon Client for HTML Access	Enter a Horizon Client version number to block all clients earlier than that version.

Table 3-5. Global Client Restriction Settings for Client Sessions (continued)

Setting	Description
Block Additional Clients	When you select this option, all other clients types except the whitelisted Horizon Clients will be blocked from launching any desktops or published applications. However, if you want your end users to use other client types to launch desktops and published applications, you must add the client type to the `pae-AdditionalClientTypes` LDAP attribute to bypass the block settings for that client type. You can use the ADSI Edit utility to edit LDAP attributes on the Connection Server. In the ADSI Edit utility, the `pae-AdditionalClientTypes` LDAP attribute is available under `CN=Common`, `OU=Global`, `OU=Properties`, `DC=vdi`, `DC=vmware`, `DC=int`. If a pod federation is present, the attribute is `DC=vdiglobal`. If a pod federation is not present, the attribute is `DC=vdi`.
Message for Blocked Client Versions	Enter the message to display to users that try to connect using a blocked Horizon Client version. Character length limit for the message is 1024.
Warning Message	Enter the warning message to display to users that connect using a restricted Horizon Client version. Character length limit for the message is 1024.

Join the Customer Experience Improvement Program

You can configure VMware Horizon to join the VMware Customer Experience Improvement Program (CEIP).

For information about the type of data that VMware collects through the CEIP, and how VMware uses that data, see the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

To configure data sharing in Horizon Client, see the appropriate Horizon Client installation and setup guide. For example, for Windows clients, see the *VMware Horizon Client for Windows Installation and Setup Guide* document. To configure data sharing in HTML Access, see the *VMware Horizon HTML Access Installation and Setup Guide* document.

Procedure

1. In Horizon Console, select **Settings > Product Licensing and Usage**.
2. Select the **Customer Experience Program** tab and click **Edit Settings**.
3. To join the CEIP, select **Join VMware Customer Experience Improvement Program**.

   If you do not select this option, you cannot join the CEIP.
4. (Optional) Select your geographic location, business vertical, or the number of employees in your organization.

5 Click **OK**.

Note In addition to information collected for CEIP, VMware may collect Operational Data. This means that VMware may monitor and collect configuration, performance, usage, and consumption data relating to Customer's and its Users' use of the Software to facilitate the delivery and operation of the products and services (collectively, "Operational Data") as described in the VMware Privacy Notice.

The collection of Operational Data is entirely separate from CEIP, and may occur whether or not you have joined CEIP. You can deactivate the collection of Operational Data by contacting VMware support.

Setting Up Smart Card Authentication

4

For added security, you can configure a Connection Server instance 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 Installation* document for information about Active Directory, 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.

Note Internet Explorer is not a recommended Web browser for smart card authentication. For a list of recommended and supported Web browsers, see "Horizon Console Requirements" in the *Horizon Installation* document.

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 that is configured for smart card authentication, the Connection Server instance 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, which verifies the certificate by checking the certificate trust and validity period. Typically, users and administrators can successfully authenticate if their user certificate is signed and valid. If certificate revocation checking is configured, users or administrators who have revoked user certificates are prevented from authenticating.

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

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

4 Modify Horizon Connection Server Configuration Properties

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

5 Configure Smart Card Settings in Horizon Console

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

Obtain the Certificate Authority Certificates

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

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

Procedure

- Obtain the CA certificates from one of the following sources.
  - A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.

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

Obtain the CA Certificate from Windows

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

Procedure

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

   If the user certificate does not appear in your personal store, use the reader software to export the user certificate to a file. This file is used in Step 4 of this procedure.
2. In Internet Explorer, select **Tools > Internet Options**.
3. On the **Content** tab, click **Certificates**.
4. On the **Personal** tab, select the certificate you want to use and click **View**.

   If the user certificate does not appear on the list, click **Import** to manually import it from a file. After the certificate is imported, you can select it from the list.
5. On the **Certification Path** tab, select the certificate at the top of the tree and click **View Certificate**.

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

   The **Certificate Export Wizard** appears.
7. Click **Next > Next** and type a name and location for the file that you want to export.

   Use the default file type CER for the file that you want to export.
8. Click **Next** to save the file as a root certificate in the specified location.

Add the CA Certificate to a Server Truststore File

You must add root certificates, intermediate certificates, or both to a server truststore file for all users and administrators that you trust. Connection Server instances 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 host. See the *Horizon Installation* document for more information.

Procedure

1. On your Connection 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`* `-storetype JKS`

   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 host.

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

What to do next

Modify Connection Server configuration properties to enable smart card authentication.

Modify Horizon Connection Server Configuration Properties

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

Prerequisites

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

Procedure

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

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

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

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

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

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

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

Example: locked.properties File

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

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

What to do next

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

Configure Smart Card Settings in Horizon Console

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

Prerequisites

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

Procedure

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

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

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

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

b Configure the smart card removal policy.

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

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

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

c Configure the smart card user name hints feature.

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

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

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

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

5 Click **OK**.

6 Restart the Connection Server service.

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

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

What to do next

Prepare Active Directory for smart card authentication, if required. See "Prepare Active Directory for Smart Card Authentication" in the *Horizon Installation* document.

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

Configure Smart Card Authentication on Third Party Solutions

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

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

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

Procedure

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

   See Configure a SAML Authenticator in Horizon Console.

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

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

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

   See the product documentation for the third-party device.

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

   See the product documentation for the third-party device.

Verify Your Smart Card Authentication Configuration in Horizon Console

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

Procedure

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

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

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

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

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

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

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

  a Select **Settings > Servers**.

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

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

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

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

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

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

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

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

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

- If smart card users select the PCoIP display protocol or the VMware Blast display protocol to connect to single-session desktops, verify that the Horizon Agent component called Smartcard Redirection is installed on the single-user machines. The smart card feature lets users log in to single-session desktops with smart cards. RDS hosts, which have the Remote Desktop Services role installed, support the smart card feature automatically. As a result, there is no need to install the feature.

- Check the log files in *Drive Letter*:\ProgramData\VMware\log\ConnectionServer on the Connection Server host for messages stating that smart card authentication is enabled.

  Note This file path is a symbolic link that redirects to the actual location of the log files, which is *Drive Letter*:\ProgramData\VMware\VDM\logs

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.

VMware Horizon 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. The CA must be accessible from the Connection Server host.

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

- Logging in with CRL Checking

  When you configure CRL checking, VMware Horizon 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, VMware Horizon sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. VMware Horizon 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, VMware Horizon 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, VMware Horizon 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, VMware Horizon 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 VMware Horizon cannot read the CRL.

Logging in with OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, VMware Horizon sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. VMware Horizon 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.

VMware Horizon 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, VMware Horizon 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 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 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, VMware Horizon 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 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 to make your changes take effect

Example: locked.properties File

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

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

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

Smart Card Certificate Revocation Checking Properties

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

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

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

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

Using Smart Card Caching Emulation

You can use smart card caching emulation for non-Microsoft Windows client connections.

Some middleware applications used by non-Microsoft Windows clients require caching API support to function properly. In the case of remote sessions from non-Microsoft Windows clients, you can use smart card caching emulation to deliver this functionality.

Smart card caching emulation is controlled by the registry key `HKLM\SOFTWARE\VMware, Inc.\VMWare VDM\Agent\EmulateSCCaching`. To activate smart card caching emulation, set this key to "true" (the default value is "false").

Important Some third party middleware forces the Microsoft Smart Card Resource Manager service to run on the agent machine. Because of the way the APIs are implemented by Microsoft, smart card caching emulation is not activated if this service is running.

Setting Up Other Types of User Authentication

5

VMware Horizon uses your existing Active Directory infrastructure for user and administrator authentication and management. You can also integrate VMware Horizon 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.
- VMware Horizon also provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into VMware Horizon.

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.

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

- Logging in Using Two-Factor Authentication

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

- Enable Two-Factor Authentication in Horizon Console

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

- Troubleshooting RSA SecureID Access Denied

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

- Troubleshooting RADIUS Access Denial

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

Logging in Using Two-Factor Authentication

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

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

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

  After a user enters credentials in Horizon Client, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism, to the user's cell phone with a code. The user can enter this text and code into Horizon Client to complete the authentication.

- Because some RADIUS vendors provide the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.

Enable Two-Factor Authentication in Horizon Console

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

Prerequisites

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

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

Procedure

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

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

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

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

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

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

   - To enable custom user name and passcode labels to appear in the RADIUS authentication dialog for end users, enter custom labels in the **Username Label** and **Passcode Label** fields.
   - Set **Accounting port** to **0** unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a nonzero number, the messages are sent and ignored and retried a number of times, resulting in a delay in authentication.

     Accounting data can be used in order to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring.
   - If you specify a realm prefix string, the string is placed at the beginning of the username when it is sent to the RADIUS server. For example, if the username entered in Horizon Client is **jdoe** and the realm prefix **DOMAIN-A** is specified, the username **DOMAIN-A\jdoe** is sent to the RADIUS server. Similarly if you use the realm suffix, or postfix, string **@mycorp.com**, the username **jdoe@mycorp.com** is sent to the RADIUS server.

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

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

Results

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

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

What to do next

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

Troubleshooting RSA SecureID Access Denied

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

Problem

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

Cause

The RSA Agent host node secret needs to be reset.

Solution

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

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

Troubleshooting RADIUS Access Denial

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

Problem

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

Cause

RADIUS does not receive a reply from the RADIUS server, causing VMware Horizon 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 Connection Server instance as a RADIUS client. Each Connection Server instance using RADIUS must be set up as a client on the RADIUS server. See the documentation for your RADIUS two-factor authentication product.
- The shared secret values on the Connection Server instance and the RADIUS server do not match.

Using SAML Authentication

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

You can use SAML authentication to integrate VMware Horizon with VMware Workspace ONE, VMware Workspace ONE Access, or a qualified third-party load balancer or gateway. When configuring SAML for a third-party device, refer to the vendor documentation for information on configuring VMware Horizon to work with it. When SSO is enabled, users who log in to VMware Workspace ONE Access 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 Workspace ONE Access, or a third-party device, you must create a SAML authenticator in VMware Horizon. A SAML authenticator contains the trust and metadata exchange between VMware Horizon and Workspace ONE, VMware Workspace ONE Access, or the third-party device. You associate a SAML authenticator with a Connection Server instance.

Using SAML Authentication for VMware Workspace ONE Access Integration

Integration between VMware Horizon and VMware Workspace ONE Access (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 Workspace ONE Access or Workspace ONE with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure.

When VMware Workspace ONE Access and VMware Horizon are integrated, VMware Workspace ONE Access generates a unique SAML artifact whenever a user logs in to VMware Workspace ONE Access and clicks a desktop or application icon. VMware Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access.

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 Workspace ONE Access and VMware Horizon integration involves configuring VMware Workspace ONE Access with VMware Horizon information and configuring VMware Horizon to delegate responsibility for authentication to VMware Workspace ONE Access.

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

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

Configure a SAML Authenticator in Horizon Console

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

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

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

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

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

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

Prerequisites

- Verify that Workspace ONE, VMware Workspace ONE Access, 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 Installation* document.
- Make a note of the FQDN or IP address of the Workspace ONE server, VMware Workspace ONE Access server, or external-facing load balancer.
- (Optional) If you are using Workspace ONE or VMware Workspace ONE Access, make a note of the URL of the connector Web interface.
- If you are creating an authenticator for a Unified Access Gateway appliance or a third-party appliance that requires you to generate SAML metadata and create a static authenticator, perform the procedure on the device to generate the SAML metadata, and then copy the metadata.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **Connection Servers** tab, select a server instance to associate with the SAML authenticator and click **Edit**.
3. On the **Authentication** tab, select a setting from the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down menu to enable or disable the SAML authenticator.

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

   You can configure each Connection Server instance in your deployment to have different SAML authentication settings, depending on your requirements.
4. Click **Manage SAML Authenticators** and click **Add**.

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

Option	Description
Type	For a Unified Access Gateway appliance or a third-party device, select **Static**. For VMware Workspace ONE Access select **Dynamic**. For dynamic authenticators, you can specify a metadata URL and an administration URL. For static authenticators, you must first generate the metadata on the Unified Access Gateway appliance or a third-party device, copy the metadata, and then paste it into the **SAML metadata** text box.
Label	Unique name that identifies the SAML authenticator.
Description	Brief description of the SAML authenticator. This value is optional.
Metadata URL	(For dynamic authenticators) URL for retrieving all of the information required to exchange SAML information between the SAML identity provider and the Connection Server instance. In the URL `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml`, click **<YOUR HORIZON SERVER NAME>** and replace it with the FQDN or IP address of the VMware Workspace ONE Access 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 Workspace ONE Access, this URL should point to the VMware Workspace ONE Access Connector Web interface. This value is optional.
SAML metadata	(For static authenticators) Metadata text that you generated and copied from the Unified Access Gateway appliance or a third-party device.
Enabled for Connection Server	Select this check box to enable the authenticator. You can enable multiple authenticators. Only enabled authenticators are displayed in the list.

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

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

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

What to do next

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

Configure Proxy Support for VMware Workspace ONE Access

VMware Horizon provides proxy support for the VMware Workspace ONE Access (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 VMware Horizon 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`.
3. Select **Action > Properties**, and add the values for the entries **`pae-SAMLProxyName`** and **`pae-SAMLProxyPort`**.

Change the Expiration Period for Service Provider Metadata on Connection Server

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

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

Prerequisites

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

Procedure

1. Start the ADSI Edit utility on your Connection Server host.
2. In the console tree, select **Connect to**.
3. In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **`DC=vdi, DC=vmware, DC=int`**.
4. In the Computer pane, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the Connection Server host followed by port 389.

   For example: **`localhost:389`** or **`mycomputer.example.com:389`**
5. Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.
6. In the Properties dialog box, edit the **pae-NameValuePair** attribute to add the following values

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

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

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

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

Prerequisites

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

Procedure

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

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

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

   This page displays the SAML metadata from Connection Server.

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

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

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

What to do next

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

Response Time Considerations for Multiple Dynamic SAML Authenticators

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

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

Configure Workspace ONE Access Policies in Horizon Console

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

Prerequisites

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

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **Connection Servers** tab, select a server instance that is associated with a SAML authenticator and click **Edit**.
3. On the **Authentication** tab, set the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** option to **Required**.

   The Required option enables SAML authentication. The end user can only connect to the Horizon server with a SAML token provided by vIDM or a third-party identity provider. You cannot start desktops or applications from Horizon Client manually.
4. Select **Enable Workspace ONE mode**.
5. In the **Workspace ONE server hostname** text box, enter the Workspace ONE Hostname FQDN value.
6. (Optional) Select **Block connections from clients that don't support Workspace ONE mode** to restrict Horizon Clients that support Workspace ONE mode from accessing applications.

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.

Results

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

Authenticating Users and Groups 6

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

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

This chapter includes the following topics:

Restricting Remote Desktop Access Outside the Network

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

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

Configure Remote Access

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

Prerequisites

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

Procedure

1. In Horizon Console, select **Users and Groups**.
2. Click the **Remote Access** tab.
3. Click **Add** and select one or more search criteria, and click **Find** to find users or groups based on your search criteria.

   Note Unauthenticated access users will not appear in the search results.
4. To provide remote access for a user or group or a user with unauthenticated access, select a user or group and click **OK**.
5. To remove a user or group from remote access, select the user or group, click **Delete**, and click **OK**.

Configuring Unauthenticated Access

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

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

Note Unauthenticated access is not supported for applications published in a desktop pool.

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 Workspace ONE Access 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 for applications published from a desktop pool.
- Unauthenticated access is not supported with an Unified Access Gateway appliance.
- User preferences are not preserved for unauthenticated users.
- Virtual desktops are not supported for unauthenticated users.
- Horizon Console 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.
- Application sessions that run forever with the Bypass Session Timeout enabled are not supported for unauthenticated users.

Create Users for Unauthenticated Access

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

Prerequisites

- Administrators can create only one user for each Active Directory account.
- Administrators cannot create unauthenticated user groups. If you create an unauthenticated access user and there is an existing client session for that AD user, you must restart the client session to make the changes take effect.
- If you select a user with desktop entitlements and make the user an unauthenticated access user, the user will not have access to the entitled desktops.

Procedure

1. In Horizon Console, select **Users and Groups**.
2. On the **Unauthenticated Access** tab, click **Add**.
3. In the **Add Unauthenticated User** wizard, select one or more search criteria and click **Find** to find users based on your search criteria.
4. Select a user and click **Next**.
5. Enter the user alias.

   The default user alias is the user name that was configured for the AD account. End users can use the user alias to log in to the Connection Server instance from Horizon Client.
6. (Optional) Review the user details and add comments.
7. Click **Submit**.

Results

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

What to do next

After you create users for unauthenticated access, you must enable unauthenticated access in Connection Server to enable users to connect and access published applications. See, Enable Unauthenticated Access for Users.

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 Console, select **Settings > 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. For more information on creating farms, see the *Setting Up Published Desktops and Applications in Horizon Console* document.
- Create an application pool for published applications that run on a farm of RDS hosts. For more information on creating published applications, see the *Setting Up Published Desktops and Applications in Horizon Console*.

Procedure

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

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

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

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

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

What to do next

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

Search Unauthenticated Access Sessions

Use Horizon Console 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 Console, select **Monitor > Sessions**.
2. In the **Sessions** drop down menu, select **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), pool or farm, bypass session timeout, DNS name, client ID, client version, and security gateway. The session start time, duration, state, last session, and display protocol also appear in the search results.

   Note Last Session is the duration of the last connection period of the session in milliseconds. If the session is currently connected, this is the duration of the session in the connected state. If the session is currently disconnected, this is the duration of its previous connection period.

Delete an Unauthenticated Access User

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

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

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

Procedure

1. In Horizon Console, select **Users and Groups**.
2. On the **Unauthenticated Access** tab, select the user and click **Delete**.
3. Click **OK**.

What to do next

Remove application entitlements for the user.

Unauthenticated Access From Horizon Client

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

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

Prerequisites

- Verify that the unauthenticated access users are created. 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.

Configure Login Deceleration for Unauthenticated Access to Published Applications

Because users do not enter credentials when using unauthenticated access, it is possible for RDS hosts to become overwhelmed by requests for published applications. Login deceleration alleviates this. You can adjust the level of deceleration. You can also block clients that do not support deceleration.

Prerequisites

- Verify that you have enabled unauthenticated access for users.
- Verify that you have Horizon Client version 4.9 or later.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. Click the **Connection Servers** tab.
3. Select a Connection Server and click **Edit**.
4. Click the **Authentication** tab.

5 From the **Login Deceleration Level** drop-down menu, select a deceleration level for unauthenticated access logins.

Option	Description
Low	Sets a low deceleration level for unauthenticated access logins. For Web browsers such as Microsoft Internet Explorer and Microsoft Edge, the recommendation is to set the low deceleration level.
Medium	Sets a medium deceleration level for unauthenticated access logins. Set by default. Do not change this setting if you use Horizon Client version 4.8.
High	Sets a high deceleration level for unauthenticated access logins. Setting a high deceleration level might increase the log in time and affect the end-user experience.

6 (Optional) To prevent any client that does not support login deceleration from connecting to VMware Horizon with unauthenticated access, select **Block Non-Compliant Clients**.

Horizon Clients earlier than version 4.8 are not compliant.

7 Click **OK**.

What to do next

Log in to Horizon Client with unauthenticated access and start the published application. See, Unauthenticated Access From Horizon Client.

Configure Users for Hybrid Logon in Horizon Console

After you create an unauthenticated access user, you can enable hybrid logon for the user. Enabling hybrid logon provides unauthenticated access users domain access to network resources such as fileshare or network printers without the need to enter credentials. Hybrid logon is supported on Windows Server 2019 and earlier with Terminal Services (RDSH) installed.

Note The hybrid logon feature uses the same domain user for all logged on users for a given unauthenticated access user configured for hybrid logon.

Note If you use the user profile tab to set the home directory as a network path from the RDS host machine, by default the administrative user interface on Windows removes all existing permissions on the home directory folder and adds permissions for the administrator and local user with full control. Use the administrator account to remove the local user from the permissions list and then add the domain user with the permissions that you need to set for the user.

Prerequisites

- Verify that you selected the Hybrid Logon custom option when you installed Horizon Agent on the RDS host. For more information on Horizon Agent custom setup options for an RDS host, see the *Setting Up Published Desktops and Applications in Horizon Console* document.

- Verify that you created an unauthenticated access user. See, Create Users for Unauthenticated Access.
- Verify that Kerberos DES encryption is not enabled for the user account in the domain. Kerberos DES encryption is not supported for the hybrid logon feature.

Procedure

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

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

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

The user must have a valid UPN.

4 Select an unauthenticated access 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 Select **Enable Hybrid Logon**.

The **Enable True SSO** option is selected by default. You must have True SSO enabled for the VMware Horizon environment. Then, unauthenticated access users enabled for hybrid logon use True SSO to log in to the Connection Server instance from Horizon Client.

Note If the Connection Server pod is not configured for True SSO, then the user can start an entitled application with unauthenticated access. However, the user does not have network access because True SSO is not enabled on the pod.

8 (Optional) To enable the user to log in to the Connection Server instance from Horizon Client, select **Enable Password Logon** and enter the user's password.

Use this setting if you do not have True SSO configured for the VMware Horizon environment.

In a CPA environment, the hybrid logon user feature only works on the Connection Server pod on which the hybrid logon user was configured with the **Enable Password Logon** setting and entitled to published applications.

For example, in a CPA environment with Pod A and Pod B, with the hybrid logon user configured with the **Enable Password Logon** setting is entitled to an application on Pod A. The user can view and start the application from a client that connects to either Pod A or Pod B. However, if another application is entitled to the same user on Pod B, then the user cannot view and start the application from a client that connects to Pod B. For the hybrid logon

feature to work on Pod B, you must create another hybrid logon user configured with the **Enable Password Logon** setting and entitle applications to that user. For more information on how to set up a CPA environment, see the *Administering Cloud Pod Architecture in Horizon* document.

Note In a remote pod, an unauthenticated access user with a hybrid logon password cannot be used as a default unauthenticated access user. If you have existing unauthenticated access users with hybrid logon passwords that are cross pod users, such as in upgrades, these users might see inconsistent global application entitlements in Horizon Client when connecting to different pods. For example, cross pod users might not see global application entitlements, even if the pod where the user was created has local pools, and these might be visible when connecting to some other pod. If this inconsistency occurs, remove these cross pod users.

9 Click **Finish**.

What to do next

Entitle the user to published applications. See, Entitle Unauthenticated Access Users to Published Applications.

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

With Horizon Client for Windows, when users select **Log in as current user** in the **Options** menu, 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 using Kerberos. 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 Connection Server instance, enable the **Accept logon as current user** setting to allow the Connection Server instance to accept the user identity and credential information that is passed when users select **Log in as current user** in the **Options** menu in Horizon Client.

  Important You must understand the security risks before enabling this setting. See, "Security-Related Server Settings for User Authentication" in the *Horizon Security* document.

- 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.

  When you select **Accept logon as current user**, you can enable the following user settings:

  - Allow Legacy Clients: Support for older clients. Horizon Client versions 2006 and 5.4 and earlier versions are considered older clients.
  - Allow NTLM Fallback: Uses NTLM authentication instead of Kerberos when there is no access to the domain controller. The NTLM group policy settings must be enabled in Horizon Client configuration.
  - Disable Channel Bindings: An additional security layer to secure NTLM authentication. By default, channel bindings are enabled on the client.
  - True SSO Integration: Enable this setting on Connection Server to allow SSO to the desktop using True SSO. For example, in a nested mode, True SSO is used to log on to a nested client and then a secondatry desktop logon was performed. For information on nested mode, see the *VMware Horizon Client for Windows Installation and Setup Guide*.
    - Disabled: The user has to enter login information if the client did not receive logon credentials.
    - Optional: Client credentials will be used, if available, else True SSO will be used. This is the recommended setting if both True SSO and Log in as current user are enabled.
    - Enabled: True SSO will be used to log on to the desktop.

Administrators can use Horizon Client group policy settings to control the availability of the **Log in as current user** setting in the **Options** menu 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 **Log in as current user** 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.

Note The Recursive Unlock feature may be slow when you use Log in as current user with NTLM authentication if Horizon Client is unable to access the domain controllers. To mitigate this issue, enable the group policy setting **Always use NTLM for servers** in the **VMware Horizon Client Configuration > Security Settings > NTLM Settings** folder in the Group Policy Management Editor.

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 **Log in as current user** 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.

Setting Up True SSO

With the True SSO (single sign-on) feature, after users log in to VMware Workspace ONE Access using a smart card or RSA SecurID or RADIUS authentication, or a third-party identity provider using an Unified Access Gateway appliance, 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.

Users belonging to an untrusted domain can use True SSO. See Configuring Untrusted Domains.

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.

You must perform the following tasks to set up your environment for True SSO:

1 Set Up an Enterprise Certificate Authority

2 Create Certificate Templates Used with True SSO

3 Install and Set Up an Enrollment Server

4 Export the Enrollment Service Client Certificate

5 Configure SAML Authentication to Work with True SSO

6 Configure Horizon Connection Server for True SSO

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.

Prerequisites

If you have an existing instance of Microsoft Certificate Services, consider whether to set up a sub-CA for True SSO. To understand the changes needed for an existing instance to support True SSO, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/2149312.

If you don't have an existing instance of Microsoft Certificate Services, consult the Microsoft documentation to decide on type of deployment to use. To see the Microsoft documentation, search for the string "Server Certificate Deployment Overview" in the Microsoft documentation available at https://docs.microsoft.com.

To deploy a new Root Certificate Authority, search for the string "Install the Certification Authority" in the Microsoft documentation available at https://docs.microsoft.com.

Procedure

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

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

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

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

   Note This setting is usually required to prevent failure of revocation checking, because the root certificate authority that True SSO uses will typically be offline. However, you can skip this setting if you plan to keep the root certificate authority online.

3. 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 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 the Windows operating system. ■ For **Certificate Recipient**, select the Windows operating system.
General tab	■ Change the template display name to a name of your choice. Example: 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.

Install and Set Up an Enrollment Server

You run the Connection Server installer and select the Horizon 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 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 2012 R2, Windows server 2016, or Windows Server 2019 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 Horizon component, including Connection Server, Horizon Client, or Horizon Agent is installed on the virtual machine.
- Verify that the virtual machine is part of the Active Directory domain for the Horizon 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 Horizon 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 download, which includes Connection Server.

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 Enrollment Server**, then click **Next**.

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

Prerequisites

Verify that you have a Connection Server. For installation instructions, see the *Horizon Installation* document. For upgrade instructions, see the *Horizon Upgrades* document.

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 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 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 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 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 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 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 Workspace ONE Access. See Configure SAML Authentication to Work with True SSO.

Configure SAML Authentication to Work with True SSO

With the True SSO feature, users can log in to VMware Workspace ONE Access 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 Workspace ONE Access has not changed, one additional step has been added for True SSO. You must configure VMware Workspace ONE Access so that True SSO is enabled.

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 Console, select **Settings > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.
- Verify that VMware Workspace ONE Access is installed and configured. See the VMware Workspace ONE Access documentation, available at https://docs.vmware.com/en/VMware-Workspace-ONE-Access/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 Servers," in the *Scenarios for Setting Up TLS Certificates for Horizon* document.
- Make a note of the FQDN of the VMware Workspace ONE Access server instance.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select a server instance to associate with the SAML authenticator and click **Edit**.
3. On the **Authentication** tab, 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 Workspace ONE Access server instance.
Description	(Optional) You can use the FQDN of the VMware Workspace ONE Access 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 Workspace ONE Access server instance.
Administration URL	URL for accessing the administration console of the SAML identity provider (VMware Workspace ONE Access 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 and VMware Workspace ONE Access.

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 Console dashboard, click **View** and 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 Workspace ONE Access 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 Workspace ONE Access administration console, navigate to the desktop pool from the **Catalog > Virtual Apps** page, and select the **True SSO Enabled** 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 Console to assign the Administrators role to a user. See Chapter 8 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 Workspace ONE Access. 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 Workspace ONE Access and a connection server, using Horizon Console.

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 Workspace ONE Access. 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 Workspace ONE Access.

What to do next

In Horizon Console, verify the health status of the True SSO configuration. For more information, see Using the 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 6-1. vdmutil Command Authentication Options

Option	Description
`--authAs`	Name of a Horizon 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 administrator user specified in the `--authAs` option.
`--authPassword`	Password for the Horizon 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 6-2. 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 6-2. 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 6-3. 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 Workspace ONE Access and 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 6-4. 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-`*`YYMM-x.x.x-yyyyyyyy`*`.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 download, which includes the GPO Bundle containing the ZIP file.

Table 6-5. 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 6-6. 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 6-6. 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 Console 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 Console 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 6-7. 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"

LDAP URL filters are not supported for users from untrusted domains.

Unlock a Desktop With True SSO and Workspace ONE

After users use True SSO to login to the desktop, they can unlock the desktop after reauthentication from the Workspace ONE portal using the same logon credentials.

Prerequisites

- Verify that you have VMware Horizon version 7.8 or later.
- Verify that you have Horizon Client for Windows version 5.0 or later.
- Verify that you have Workspace ONE version 19.03 or later.

Procedure

1. Enable Workspace ONE and configure it for use with Connection Server.

   See the Workspace ONE documentation at the Workspace ONE documentation Web page.
2. Configure Horizon Connection Server for True SSO.

   See Configure Horizon Connection Server for True SSO.
3. To start virtual or published desktops, connect to a Connection Server in Workspace ONE mode that has True SSO configured. See, the Horizon Client documentation at the VMware Horizon Clients documentation Web page.
4. Start virtual or published desktops from the Workspace ONE portal so that the user can use single sign on with True SSO.
5. Lock the desktop.
6. To unlock the desktop, select **VMware True SSO User** and click **Submit**.

   You are redirected to the browser to re-authenticate with Workspace ONE.
7. Enter the credentials and passcode of the locked desktop.

What to do next

You can disable this feature by setting a registry key on the machine where Horizon Agent is installed, in the following location:

`HKLM\Software\VMware, Inc.\VMware VDM\Agent\CertSSO[DisableCertSSOUnlock=true]`

You can also disable this feature by setting the registry key `DisabledFeatures=TrueSSOUnlock` on Horizon Client for Windows in the following locations:

- On a Windows 32-bit operating system: `[HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client] or [HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM \Client]`.
- On a Windows, 64-bit operating system: `[HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client] or [HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM \Client]`.

If the registry key is set, the **VMware True SSO User** option does not appear when the user unlocks the desktop.

Using the Dashboard to Troubleshoot Issues Related to True SSO

You can use the system health dashboard in Horizon Console 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.

In Horizon Console, navigate to **Monitor > Dashboard** and click **View** in the **System Health** pane and click the **True SSO** tab to see the 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.

- On the **True SSO** tab, you can 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 Workspace ONE Access 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 Console, select **Settings > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.

Table 6-8. 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 6-9. 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.

Table 6-9. Enrollment Server Connectivity (continued)

Status Text	Description
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 6-10. 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 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 6-11. 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 6-12. 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 6-13. 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.

Entitling Users and Groups 7

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

For information about configuring global entitlements in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon* document.

Note When you entitle users and groups in Active Directory, you can search users and groups across the entire directory or in a particular domain. In Horizon Console, when you navigate to **Users and Groups** and select the **Entire Directory** option, Connection Server searches and counts the users and groups across all domains in Connection Server domain's forest. Any domains that are not part of Connection Server domain's forest are excluded in the **Entire Directory** option. To search users or groups in domains that are not part of Connection Server domain's forest, you must select those domains explicitly, and this is applicable to both Connection Server domains and untrusted domains.

This chapter includes the following topics:

Add Entitlements to a Desktop or Application Pool in Horizon Console

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

Prerequisites

Create a desktop or application pool.

Procedure

1 Select the desktop or application pool.

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

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

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

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

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

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

Remove Entitlements from a Desktop or Application Pool in Horizon Console

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

Procedure

1 Select the desktop or application pool.

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

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

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

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

Review Desktop or Application Pool Entitlements

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

Procedure

1. In Horizon Console, select **Users and Groups** and click the name of the user or group.
2. Click the **Entitlements** tab and review the desktop or application pools to which the user or group is entitled.

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

Configuring Shortcuts for Entitled Pools

You can configure shortcuts for entitled pools. When an entitled user connects to a Connection Server instance from a Windows client, Horizon Client for Windows places these shortcuts in the Start menu, on the desktop, or both, on the user's client device. You can configure a shortcut when you create or modify a pool.

You must select a category folder, or the root (/) folder, during shortcut configuration. You can add and name your own category folders. You can configure up to four folder levels. For example, you might add a category folder named Office and select that folder for all work-related apps, such as Microsoft Office and Microsoft PowerPoint.

On Windows 10 client devices, Horizon Client places category folders and shortcuts in the Apps list. If you select the root (/) folder for a shortcut, Horizon Client places the shortcut directly in the Apps list.

After you create a shortcut, a check mark appears in the **App Shortcut** column for the pool in Horizon Console.

By default, Horizon Client for Windows prompts entitled users to install shortcuts the first time they connect to a server. You can configure Horizon Client for Windows to install shortcuts automatically, or to never install shortcuts, by modifying the **Automatically install shortcuts when configured on the Horizon server** group policy setting. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

By default, changes that you make to shortcuts are synchronized on a user's Windows client device each time the user connects to the server. Windows users can disable the shortcut synchronization feature in Horizon Client. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

You can also configure a shortcut when you create or modify a global entitlement. For information about configuring global entitlements, see the *Administering Cloud Pod Architecture in Horizon* document.

Create Shortcuts for a Desktop Pool in Horizon Console

You can create shortcuts for an entitled desktop pool in Horizon Console so that the desktop pool appears in the Windows Start menu, on the Windows desktop, or both, on the user's Windows client device. You can specify up to four category folder levels for shortcuts. You can create shortcuts when you create a desktop pool. You can also create and modify shortcuts when you edit the desktop pool.

Prerequisites

Decide how to configure the pool settings based on the type of desktop pool that you want to create.

Procedure

1. In Horizon Console, click **Inventory > Desktops** and click **Add**.
2. In the **Add Pool** wizard, select the type of desktop pool you want to create, and click **Next**.
3. Follow the wizard prompts to the **Desktop Pool Settings** page.
4. Create shortcuts for the desktop pool.
   a. Click the Category Folder **Browse** button.
   b. Select the **Select a category folder from the folder list** option.
   c. Type a folder name in the **Select a category folder or create a new folder to place a shortcut to this pool in the client device** text box.

      A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords.
   d. Select the shortcut creation method.

      You can select one or both methods.

Option	Description
Start Menu/Launcher	Creates a Windows Start menu shortcut on the Windows client device.
Desktop	Creates a shortcut on the desktop on the Windows client device.

   e. To save your changes, click **Submit**.
5. Follow the wizard prompts to the **Ready to Complete** page and select **Entitle users after this wizard finishes** and click **Submit**.

6 In the **Add Entitlements** wizard, click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria, select the users or groups you want to entitle to the desktops in the pool and click **OK**.

A check mark appears in the **App Shortcut** column for the desktop pool on the **Desktop Pools** page.

Create Shortcuts for an Application Pool in Horizon Console

You can create shortcuts for entitled applications in Horizon Console so that the shortcuts appear in the Windows Start menu, on the Windows desktop, or both, on the user's Windows client device. You can specify up to four category folder levels for shortcuts. You can create shortcuts when you create an application pool. You can also create shortcuts when you edit the application pool.

On Mac clients, if Horizon Client for Mac is configured to run published applications from the `Applications` folder on the local system and allow folder settings from servers, category folders appear in the `Applications` folder on the Mac client device. For more information, see the *VMware Horizon Client for Mac Installation and Setup Guide* document.

Prerequisites

See the *Setting Up Published Desktops and Applications in Horizon* and the *Setting Up Virtual Desktops in Horizon* documents:

- Set up the RDS hosts.
- Create a farm that contains the RDS hosts.
- If you plan to add the application pool manually, gather information about the application.
- Install Horizon Client for Windows on the client device.

Procedure

1 In Horizon Console, click **Inventory > Applications** and click **Add**.

2 Select the type of application pool you want to create.

Option	Description
Add application pool manually	Enter the information about the application.
Select installed applications	Filter to find applications by name, installed path, or application type, or select from a list of installed applications.

3 In the **Add Application Pool** wizard, select an RDS farm, enter a pool ID, and the full pathname of the application.

4 Create a shortcut for the application pool.

a Click the Category Folder **Browse** button.

b Select the **Select a category folder from the folder list** option.

c Select a category folder from the list, or type a folder name in the **Select a category folder or create a new folder to place a shortcut to this pool in the client device** text box.

A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords.

Note If needed, non-Windows clients can translate the backslash to a forward slash.

d Select the shortcut creation method.

You can select one or both methods.

Option	Description
Start Menu/Launcher	Creates a Windows Start menu shortcut on the Windows client device.
Desktop	Creates a shortcut on the desktop on the Windows client device.

e To save your changes, click **Submit**.

5 Select **Entitle users after this wizard finishes**.

6 In the **Add Entitlements** wizard, click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria, select the users or groups you want to entitle to the application in the pool and click **OK**.

A check mark appears in the **App Shortcut** column for the application pool on the **Application Pools** page.

Implementing Client Restrictions for Desktop Pools, Published Desktops, and Application Pools

You can restrict access to entitled desktop pools, published desktops, and application pools to specific client computers. To restrict access, you must add the names of the client computers that are allowed to access the desktop pools, published desktops, or applications in an Active Directory security group and then entitle this group to a pool. The Active Directory security group can contain client computers that belong to any AD Organizational Units (OUs) or default Computer container.

The client restrictions features has certain requirements and limitations.

- You must enable the client restrictions policy when you create or modify the desktop pool, published desktop or application pool. By default, the client restrictions policy is disabled. For published desktop pool and application pool settings, see the *Setting Up Published Desktops and Applications in Horizon* document. For instant-clone, full-clone, and manual desktop pool settings, see the *Setting Up Virtual Desktops in Horizon* document.

- When you create or modify entitlements for the desktop pool, published desktop, or application pool, you must add the Active Directory security group that contains the names of the client computers that are allowed to access the desktop pool, published desktop, or application pool.
- The client restrictions feature allows only specific client computers to access desktop pools, published desktops, and application pools. It does not give users access to non-entitled desktop and application pools. For example, if a user is not included in an application pool entitlement (either as a user or as a member of a user group), the user cannot access the application pool, even if the user's client computer is part of the AD security group that is entitled to the application pool.
- The client restrictions feature is supported only with Windows client computers.
- When the client restrictions policy is enabled for desktop pools, published desktops, or application pools, non-Windows clients and HTML Access clients cannot launch the desktops or applications from the restricted pools.
- The client restrictions feature only restricts new sessions from Windows clients. This feature does not restrict existing application session connections from previous user sessions.
- Horizon Client for Windows requires that the client computers belonging to an Active Directory security group be located in the default AD location "CN=Computers."

Configuring Role-Based Delegated Administration

8

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

This chapter includes the following topics:

Understanding Roles and Privileges

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

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

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

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

To create administrators, you select users and groups from your Active Directory users and groups and assign administrator roles. If the role contains object-specific privileges, you might need to apply the role to an access group, a federation access group (Cloud Pod Architecture environments only), or to both. 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.

For information about configuring federation access groups to delegate the administration of global entitlements, see the *Administering Cloud Pod Architecture in Horizon* document.

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

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

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

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

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

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

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

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

In a Cloud Pod Architecture environment, you can configure federation access groups to delegate the administration of global entitlements. For information, see the *Administering Cloud Pod Architecture in Horizon* document.

- Different Administrators for Different Access Groups

  You can create a different administrator to manage each access group in your configuration.
- Different Administrators for the Same Access Group

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

Different Administrators for Different Access Groups

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

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

Table 8-1. Different Administrators for Different Access Groups shows an example of this type of configuration.

Table 8-1. 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 8-2. Different Administrators for the Same Access Group shows an example of this type of configuration.

Table 8-2. 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 and Access Groups

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

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

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

Table 8-3. Permissions on the Administrators and Groups Tab for Admin 1

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

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

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

Table 8-4. Permissions on the Access Groups Tab for MarketingDesktops

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

The first permission is the same as the first permission shown in Table 8-3. Permissions on the Administrators and Groups Tab for Admin 1. The second permission is inherited from the second permission shown in Table 8-3. Permissions on the Administrators and Groups Tab for Admin 1. Because access groups inherit permissions from the root access group, Admin1 has the Administrators (Read only) role on the `MarketingDesktops` access group. When a permission is inherited, a check mark appears in the Inherited column.

The following table shows how the first permission in Table 8-3. Permissions on the Administrators and Groups Tab for Admin 1 appears in Horizon Console when you select the Inventory Administrators role.

Table 8-5. Permissions on the Role Permissions Tab for Inventory Administrators

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

For information about permissions and federation access groups, see the *Administering Cloud Pod Architecture in Horizon* document.

Manage Administrators

Users who have the Manage Roles and Permissions privilege can use Horizon Console to add and remove administrator users and groups.

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

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

- Create an Administrator in Horizon Console

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

- Remove an Administrator in Horizon Console

  You can remove an administrator user or group.

Create an Administrator in Horizon Console

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

Prerequisites

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

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Administrators and Groups** tab, click **Add User or Group**.
3. Click **Add**, select one or more search criteria, and click **Find** to filter Active Directory users or groups based on your search criteria.
4. Select the Active Directory user or group that you want to be an administrator user or group and click **OK**.

   You can press the Ctrl and Shift keys to select multiple users and groups.
5. Click **Next** and select a role.

   The **Access Groups** 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.

   Note Even though the Help Desk Administrators and Help Desktop Administrators (Read only) roles are shown as applicable to access groups, administrators can be added only to the root access group.

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

For information about federation access groups, see the *Administering Cloud Pod Architecture in Horizon* document.

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

Results

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

Remove an Administrator in Horizon Console

You can remove an administrator user or group.

You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root access group. If the local pod is part of a Cloud Pod Architecture environment, a super administrator has the Administrators role on the root federation access group as well.

Procedure

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

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

Results

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

Manage and Review Permissions

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

In a Cloud Pod Architecture environment, you can add, delete, and review permissions for federation access groups. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

- Add a Permission in Horizon Console

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

- Delete a Permission in Horizon Console

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

- Review Permissions in Horizon Console

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

Add a Permission in Horizon Console

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

In a Cloud Pod Architecture environment, you can add permissions for federation access groups. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Procedure

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

2 Create the permission.

Option	Action
Create a permission that includes a specific administrator user or group.	a On the **Administrators and Groups** tab, select the administrator or group and click **Add Permission**. b Select a role. c If the role does not apply to access groups, click **Finish**. d If the role applies to access groups, click **Next**, select one or more access groups, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group.
Create a permission that includes a specific role.	a On the **Role Permissions** tab, select the role, click **Permissions**, and click **Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d If the role does not apply to access groups, click **Finish**. e If the role applies to access groups, click **Next**, select one or more access groups, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group.
Create a permission that includes a specific access group.	a On the **Access Groups** tab, select the access group and click **Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d Click **Next**, select a role, and click **Finish**. A role must contain at least one object-specific privilege to apply to an access group. Only roles applicable to access groups are available for selection. **Note** Even though the Help Desk Administrators and Help Desk Administrators (Read only) roles are shown as applicable to access groups, permissions can be created only on the root access group.

Delete a Permission in Horizon Console

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

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

In a Cloud Pod Architecture environment, you can delete permissions for federation access groups. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Procedure

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

2 Select the permission to delete.

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

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

Review Permissions in Horizon Console

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

In a Cloud Pod Architecture environment, you can review permissions for federation access groups. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Procedure

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

2 Review the permissions.

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

Manage and Review Access Groups

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

For information about managing and reviewing federation access groups in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon* document.

- Add an Access Group in Horizon Console

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

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

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

- Remove an Access Group in Horizon Console

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

- Review the Objects in an Access Group

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

- Review the vCenter Virtual Machines in an Access Group

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

Add an Access Group in Horizon Console

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

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

Procedure

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

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

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

The description is optional.

What to do next

Move one or more objects to the access group.

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

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

Procedure

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

2 Select a pool or a farm.

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

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

Results

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

Remove an Access Group in Horizon Console

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

Prerequisites

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

Procedure

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

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

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

Review the Objects in an Access Group

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

Procedure

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

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

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

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

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

Review the vCenter Virtual Machines in an Access Group

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

Procedure

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

2 Select the **vCenter** tab.

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

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

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

Manage Custom Roles

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

- Add a Custom Role in Horizon Console

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

- Modify the Privileges in a Custom Role in Horizon Console

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

- Remove a Custom Role in Horizon Console

  You can remove a custom role if it does not have any permissions. You cannot remove the predefined administrator roles.

Add a Custom Role in Horizon Console

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

Prerequisites

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

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Role Privileges** tab, click **Add Role**.
3. Enter a name and description for the new role, select one or more privileges, and click **OK**.

   The new role appears in the left pane.

Modify the Privileges in a Custom Role in Horizon Console

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

In a Cloud Pod Architecture environment, when a pod is part of a pod federation, permissions might be added or deleted automatically when a role is updated. For more information, see the *Administering Cloud Pod Architecture in Horizon* document. Permissions are not created or deleted automatically when the Connection Server instance is not part of a pod federation.

Prerequisites

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

Procedure

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

Remove a Custom Role in Horizon Console

You can remove a custom role if it does not have any permissions. You cannot remove the predefined administrator roles.

Prerequisites

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

Procedure

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

   The **Remove Role** button is not available for predefined roles or for custom roles that have permissions.
3. Click **OK** to remove the role.

Predefined Roles and Privileges

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

- Predefined Administrator Roles

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

  Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to access groups. In a Cloud Pod Architecture environment, roles that contain only global privileges also cannot be applied to federation 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. In a Cloud Pod Architecture environment, roles that contain certain object-specific privileges are applicable to federation access groups.
- Privilege Scopes

  Administrator privileges can be limited in scope.
- Internal Privileges

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

Predefined Administrator Roles

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

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

The following table describes the predefined roles and indicates whether a role can be applied to access groups or federation access groups. Federation access groups are available only in Cloud Pod Architecture environments.

Table 8-6. Predefined Roles in Horizon Console

Role	User Capabilities	Applies to Access Group	Applies to Federation 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. When administrators have this role on an access group or federation access group, they can manage only the inventory objects in that access group or federation access group. **Important** An administrator must have the Administrators role on the root access group to perform the following tasks: ■ Use the `vdmadmin` , `vdmimport`, and `lmvutil` commands.	Yes	Yes
Administrators (Read only)	■ View, but not modify, global settings and inventory objects. ■ Run all PowerShell commands and command line utilities, including `vdmexport` but excluding `vdmadmin`, `vdmimport`, and `lmvutil`. In a Cloud Pod Architectureenvironment, 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 or federation access group, they can view only the inventory objects in that access group or federation access group.	Yes	Yes

Table 8-6. Predefined Roles in Horizon Console (continued)

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

Table 8-6. Predefined Roles in Horizon Console (continued)

Role	User Capabilities	Applies to Access Group	Applies to Federation 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.	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.	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. In a Cloud Pod Architecture environment, roles that contain only global privileges also cannot be applied to federation access groups.

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

Table 8-7. Global Privileges

Privilege	Privilege Set	User Capabilities	Predefined Roles
Collect Operation Logs	LOG_COLLECTION GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Collect operation logs for pools, farms, or Connection Server.	
Console Interaction	GLOBAL_ADMIN_UI_INTERACTIVE	Log in to and use Horizon Console. **Note** VMware Horizon adds the **Console Interaction** privilege to new roles automatically. This privilege does not appear in the list of global privileges in Horizon Console.	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Global Configuration and Policy Administrators Global Configuration and Policy Administrators (Read only) Helpdesk Administrators Helpdesk Administrators (Read Only) Local Administrators Local Administrators (Read Only)
Direct Interaction	GLOBAL_ADMIN_SDK_INTERACTIVE	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. **Note** VMware Horizon adds the **Direct Interaction** privilege to new roles automatically. This privilege does not appear in the list of global privileges in Horizon Console.	Administrators Administrators (Read only)
Manage Access Groups	GLOBAL_PERMISSION_VIEW GLOBAL_ROLE_VIEW FOLDER_VIEW FOLDER_MANAGEMENT GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Add and remove access groups and, in a Cloud Pod Architecture environment, federation access groups.	Administrators Local Administrators

Table 8-7. Global Privileges (continued)

Privilege	Privilege Set	User Capabilities	Predefined Roles
Manage Global Configuration and Policies	GLOBAL_CONFIG_MANAGEMENT GLOBAL_CONFIG_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	View and modify global policies and configuration settings except for administrator roles and permissions.	Administrators Global Configuration and Policy Administrators
Manage Roles and Permissions	GLOBAL_PERMISSION_MANAGEMENT GLOBAL_PERMISSION_VIEW GLOBAL_ROLE_MANAGEMENT GLOBAL_ROLE_PERMISSION_MANAGEMENT GLOBAL_ROLE_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Create, modify, and delete administrator roles and permissions.	Administrators
Register Agent	GLOBAL_MACHINE_REGISTER GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	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
Manage vCenter Configuration (Read only)	VC_CONFIG_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Read only access to the vCenter Server configuration.	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Local Administrators Local Administrators (Read Only)

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. In a Cloud Pod Architecture environment, roles that contain certain object-specific privileges are applicable to federation access groups.

The following table describes the object-specific privileges. The predefined roles Administrators, Local Administrators, Help Desk Administrators, and Inventory Administrators contain these privileges.

Table 8-8. Object-Specific Privileges

Privilege	Privilege Set	User Capabilities	Object
Enable Farms and Desktop Pools	MACHINE_VIEW POOL_ENABLE POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Enable and disable desktop pools.	Desktop pool, application pool, farm
Entitle Desktop and Application Pools	MACHINE_VIEW POOL_ENTITLE POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Add and remove user entitlements.	Desktop pool, application pool
Manage Cloud Pod Architecture	FEDERATED_LDAP_VIEW FEDERATED_LDAP_MANAGE MACHINE_VIEW POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Configure and manage a Cloud Pod Architecture environment, including global entitlements, sites, home sites, and pods. To manage a Cloud Pod Architecture configuration, an administrator must have this privilege on the root federation access group.	Desktop pool, application pool, farm, machine, global entitlements
Manage Global Sessions	FEDERATED_SESSIONS_MANAGE FEDERATED_SESSIONS_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Manage global sessions in a Cloud Pod Architecture environment.	Global sessions
Manage Maintenance Operations on Automated Desktops and Farms	MACHINE_VIEW POOL_SVI_IMAGE_MANAGEMENT POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Schedule push image, schedule maintenance, and change the default image for a desktop pool and farm.	Desktop pool, farm
Manage Machine	MACHINE_MANAGE_OFFLINE_SESSION MACHINE_MANAGE_VDI_SESSION MACHINE_MANAGEMENT MACHINE_REBOOT MACHINE_VIEW MANAGE_REMOTE_PROCESS POOL_VIEW REMOTE_ASSISTANCE GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Perform all machine and session-related operations.	Machine

Table 8-8. Object-Specific Privileges (continued)

Privilege	Privilege Set	User Capabilities	Object
Manage Machine Alias and User Assignment	GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE MACHINE_USER_MANAGEMENT MACHINE_VIEW POOL_VIEW	Assign and unassign users for machines and update machine aliases.	Machine
Manage Machine Maintenance	GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE MACHINE_MAINTENANCE MACHINE_VIEW POOL_VIEW	Put machines into maintenance mode and take machines out of maintenance mode.	Machine
Manage Farms and Desktop and Application Pools	MACHINE_VIEW POOL_ENABLE POOL_ENTITLE POOL_MANAGEMENT POOL_SVI_IMAGE_MANAGEMENT POOL_VIEW VC_CONFIG_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	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	MACHINE_MANAGE_VDI_SESSION MACHINE_VIEW POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Disconnect and log off sessions and send messages to users.	Session
Manage Reboot Operation	MACHINE_REBOOT MACHINE_VIEW POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Reset virtual machines or restart virtual desktops.	Machine
Manage Help Desk (Read only)	FEDERATED_LDAP_VIEW FEDERATED_SESSIONS_VIEW FOLDER_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE GLOBAL_CONFIG_VIEW HELPDESK_ADMINISTRATOR_VIEW MACHINE_VIEW POOL_VIEW	Read-only access to the Horizon Help Desk Tool, global settings, and global policies, except for administrators and roles and Cloud Pod Architecture configurations.	Desktop pool, application pool, farm, machine, session, global entitlements, global sessions

Table 8-8. Object-Specific Privileges (continued)

Privilege	Privilege Set	User Capabilities	Object
Manage Remote Processes and Applications	MACHINE_VIEW MANAGE_REMOTE_PROCESS POOL_VIEW GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Manage remote processes and applications on remote desktop.	Machine
Remote Assistance	MACHINE_VIEW POOL_VIEW REMOTE_ASSISTANCE GLOBAL_ADMIN_SDK_INTERACTIVE GLOBAL_ADMIN_UI_INTERACTIVE	Remote assistance to remote desktop.	Machine

Privilege Scopes

Administrator privileges can be limited in scope.

Scope	Description
Global	Privileges that have this scope have the following characteristics: ■ Not applicable to access groups. ■ Not applicable to federation access groups in a Cloud Pod Architecture environment. ■ Part of the local pod cluster only. ■ Pertain to global settings that are applicable to the local pod cluster.
Federation group	Privileges that have this scope are applicable to federation access groups in a Cloud Pod Architecture environment.
Access group, Federation group	Privileges that have this scope are applicable to access groups and, in a Cloud Pod Architecture environment, federation access groups.
Local pod	Privileges that have this scope are applicable to access groups and will contain global privileges.
All	Privileges that have this scope are applicable to access groups and, in a Cloud Pod Architecture environment, federation access groups, and will contain global privileges.

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 8-9. Internal Privileges

Privilege	Description	Predefined Roles
Local (Read only)	Grants read-only access to inventory objects, global settings, and global policies.	Administrators, Administrators (Read only), Local Administrators, Local Administrators (Read only)
Full (Read only)	Grants read-only access to all settings.	Administrators, Administrators (Read only)
Manage Inventory (Read only)	Grants read-only access to inventory objects.	Administrators, Administrators (Read only), Inventory Administrators, Inventory Administrators (Read only), Local Administrators, Local 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.	Administrators, Administrators (Read only), Help Desk Administrators, Help Desk Administrators (Read only), Local Administrators, Local Administrators (Read only)

Minimum vCenter Server Privileges for Managing Full Clones and Instant Clones

An administrator must have certain vCenter Server privileges to manage full clones and instant clones.

Horizon administrators need to create a custom role in vCenter Server and select the following privileges to manage full clones. The following table lists the minimum vCenter Server privileges to perform basic operations in vCenter Server.

Table 8-10. Full Clone Privileges

Task	Privilege Group on vCenter Server for Full Clones
■ Create a folder ■ Delete a folder	**Folder**
Allocation space	**Datastore**

Table 8-10. Full Clone Privileges (continued)

Task	Privilege Group on vCenter Server for Full Clones

■ Configuration
  ■ Add or remove a device
  ■ Advanced
  ■ Modify device settings
■ Interaction
  ■ Power Off
  ■ Power On
  ■ Reset
  ■ Suspend
  ■ Perform wipe or shrink operations
■ Inventory
  ■ Create new
  ■ Create from existing
  ■ Remove
■ Provisioning
  ■ Customize
  ■ Deploy template
  ■ Read customization specifications
  ■ Clone template
  ■ Clone virtual machine
	Virtual Machine

Assign virtual machine to a resource pool	**Resource**
Act as vCenter Server (required even if you do not use View Storage Accelerator)	**Global**
(All – if you are using Virtual SAN datastores of Virtual Volumes)	**Profile Driven Storage**
Implement View Storage Accelerator to enable ESXi host caching: Configure advanced settings.	**Host**

Table 8-11. Instant Clone Privileges

Task	Privilege Group on vCenter Server for Instant Clones
■ Create a folder ■ Delete a folder	**Folder**
■ Allocation space ■ Browse datastore	**Datastore**

Table 8-11. Instant Clone Privileges (continued)

Task	Privilege Group on vCenter Server for Instant Clones
■ Configuration ■ Add or remove a device ■ Advanced ■ Modify device settings ■ Change CPU count ■ Change memory ■ Change settings ■ Change resource ■ Configure Host USB device ■ Configure raw device ■ Configure mangedby ■ Display connection settings ■ Extend virtual disk ■ Query fault tolerance compatibility ■ Query unknown files ■ Reload from path ■ Remove disk ■ Rename ■ Reset guest information ■ Set annotation ■ Toggle disk change tracking ■ Toggle fork parent ■ Upgrade virtual machine compatibility ■ Interaction ■ Power Off ■ Power On ■ Reset ■ Suspend ■ Perform wipe or shrink operations ■ Connect Devices ■ Inventory ■ Create new ■ Create from existing ■ Remove ■ Move ■ Register ■ Unregister ■ Snapshot management ■ Create snapshot ■ Remove snapshot ■ Rename snapshot ■ Revert snapshot ■ Provisioning ■ Customize	**Virtual Machine**

Table 8-11. Instant Clone Privileges (continued)

Task	Privilege Group on vCenter Server for Instant Clones
■ Deploy template ■ Read customization specifications ■ Clone template ■ Clone virtual machine ■ Allow disk access	
Assign virtual machine to a resource pool	**Resource**
■ Act as vCenter Server ■ Enable methods ■ Disable methods ■ Manage custom attributes ■ Set custom attributes	**Global**
■ Inventory: modify cluster ■ Implement View Storage Accelerator: Configure advanced settings	**Host**
Assign	**Network**
(All – if you are using Virtual SAN datastores of Virtual Volumes)	**Profile Driven Storage**
Use vTPM with instant clones: ■ Clone ■ Decrypt ■ Direct access ■ Encrypt ■ Manage KMS ■ Migrate ■ Register Host	**Cryptographic operations**

Required Privileges for Common Tasks

Many common administration tasks require a coordinated set of privileges. Some operations require permission at the root access group, or at the federation root access group in a Cloud Pod Architecture environment, in addition to access to the object that is being manipulated.

Privileges for Managing Pools

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

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

Table 8-12. Pool Management Tasks and Privileges

Task	Required Privileges
Enable or disable a farm, desktop, or application pool.	**Enable Farms, Desktops and Applications Pools**
Entitle or unentitle users to a pool.	**Entitle Desktop and Application Pools**
Add a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Modify or delete a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for deleting an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Add or remove desktops from a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding or removing unmanaged virtual desktops in the desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Schedule push image, schedule maintenance, and change the default image for a desktop pool and farm.	**Manage Maintenance Operations on Automated Desktops & Farms** and **Manage vCenter Configuration (Read only)**.
Change access groups.	**Manage Farms and Desktop and Application Pools** on both the source and target access groups.

Privileges for Managing Machines

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

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

Table 8-13. Machine Management Tasks and Privileges

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

Table 8-13. Machine Management Tasks and Privileges (continued)

Task	Required Privileges
Update machine alias; Assign or remove user ownership.	**Manage Machine Alias and User Assignment**
Enter or exit maintenance mode.	**Manage Machine Maintenance**
Disconnect or log off sessions.	**Manage Sessions**

Privileges for Managing Users and Administrators

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

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

Table 8-14. User and Administrator Management Tasks and Privileges

Task	Required Privileges
Update general user information.	**Manage Global Configuration and Policies**
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 and Roles for Managing Remote Access and Unauthenticated Access

To access the **Remote Access** and **Unauthenticated Access** tabs on the **Users and Groups** page, an administrator must have the Global Configuration and Policy Administrators (Read only) role. To perform operations on these tabs, an administrator must have the Global Configuration and Policy Administrators role, or, at a minimum, the **Manage Global Configuration and Policies** privilege.

If the Cloud Pod Architecture feature is enabled, to perform operations on the **Unauthenticated Access** tab, an administrator must additionally have the **Manage Cloud Pod Architecture** privilege on the root federation access group.

Privileges for Managing a Cloud Pod Architecture Environment

An administrator must have the **Manage Cloud Pod Architecture** privilege on the root federation access group to manage a Cloud Pod Architecture environment in Horizon Console or by using `lmvutil` commands.

To add global entitlements, an administrator must have the Manage Cloud Pod Architecture privilege on any federation access group. To modify global entitlement data or delete global entitlements, an administrator must have Manage Cloud Pod Architecture privilege on the global entitlement's federation access group. If an administrator has the Manage Cloud Pod Architecture privilege on a custom access group, the local pools that are listed, and the local pools that can be added, are determined according to the visibility granted by the inventory privileges on the custom access group.

For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Privileges for Managing Access Groups and Federation Access Groups

An administrator must have the **Manage Access Groups** privilege on the root access group to add and remove access groups in Horizon Console. In a Cloud Pod Architecture environment, an administrator must have the **Manage Access Groups** privilege to add and remove federation access groups in Horizon Console. If the permission for a privilege is granted on a custom access group, the permission grants only read-only access to the **Administrators** page.

Privileges for Managing Sessions and Global Sessions

Certain privileges are required to view sessions and global sessions in Horizon Console.

The following table describes the privileges required for each type of session.

Session Type	Session Description	Required Privileges
SA	Sessions that are hosted on a resource not used in a pod federation in a Cloud Pod Architecture environment.	Any privilege that has the Access group, Local pod, or All scope on the desktop pool or farm's access group.
SB	Sessions that are hosted on a local pod cluster resource but are served from a pod federation in a Cloud Pod Architecture environment.	Any privilege that has the Access group, Local pod, or All scope on the desktop pool or farm's access group, or **Manage Global Sessions** or **Manage Help Desk (Read only)** on the global entitlement's access group.
SC	Sessions that are hosted on a remote pod cluster resource but are served from a pod federation in a Cloud Pod Architecture environment.	**Manage Global Sessions** or **Manage Help Desk (Read only)** on the global entitlement's access group.

SA and SB type sessions are listed on session pages other than **Search Sessions** in Horizon Console. The following table describes the privileges required to manage sessions on those pages.

Operation	Required Privileges
Send message	**Manage Sessions** on the destkop pool or farm's access group.
Disconnect	**Manage Sessions** on the desktop pool or farm's access group.
Logoff	**Manage Sessions** on the desktop pool or farm's access group.
Restart desktop	**Manage Reboot Operation** on the desktop pool or farm's access group.
Reset virtual machine	**Manage Reboot Operation** on the desktop pool or farm's access group.

All types of sessions are listed on the **Search Sessions** page in Horizon Console. The following table describes the privileges required to manage these sessions.

Session Type	Operations	Required Privileges
SA	Send message, disconnect,log off	**Manage Sessions** on the desktop pool or farm's access group.
SA	Restart desktop, reset virtual machine	**Manage Reboot Operation** on the desktop pool or farm's access group.
SB	Send messsage, disconnect, log off	**Manage Global Sessions** on the federation access group of any of the global entitlements for the session, or **Manage Sessions** on the desktop pool or farm's access group.
SB	Restart desktop, reset virtual machine	**Manage Global Sessions** on the federation access group of any of the global entitlements for the session, or **Manage Reboot Operation** on the desktop pool or farm's access group.
SC	Any operation	**Manage Global Sessions** on the federation access group of any of the global entitlements for the session.

Privileges for Horizon Help Desk Tool Tasks

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

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

Note The Horizon Help Desk Tool supports federation access groups based on the delegation of administration, but not access group-based delegation of administration. To access the Horizon Help Desk Tool, you must have the Manage Help Desk (Read Only) privilege on the root access group and any federation access group.

Table 8-15. Horizon Help Desk Tool Tasks and Privileges

Tasks	Required Privileges
Read-only access to Horizon Help Desk Tool.	**Manage Help Desk (Read Only)** on the root access group.
Manage global sessions.	**Manage Global Sessions** must be present on any of the federation access groups of the global entitlements on which the global session exists.
Can log in to Horizon Console.	**Console Interaction** **Note** **Console Interaction** is added to new roles automatically and does not appear in the list of global privileges in Horizon Console.
Perform all machine and session-related commands on sessions served from desktop or application pools of the local pod cluster.	**Manage Machine** on the root access group.
Send message, disconnect, and log off sessions that are served from desktop or application pools of the local pod cluster.	**Manage Sessions** on the root access group.
Send message, disconnect, and log off operations for global sessions.	**Manage Global Sessions** must be present on any of the federation access groups of the global entitlements on which the global session exists. If the session is hosted on a desktop pool or farm from a local pod cluster, even if it is being served by a global entitlement, the operation is permitted if the administrator has **Manage Sessions** on root access group.
Restart and reset operations for global sessions.	**Manage Global Sessions** must be present on any of the federation access group of the global entitlements on which the global session exists. If the session is hosted on a desktop pool or farm from a local pod cluster, even if it is being served by a global entitlement, the operation is permitted if the administrator has **Manage Reboot Operation** on the root access group.
Reset and restart operations for local sessions.	**Manage Reboot Operation** on the root access group.
Remote assistance operations.	**Remote Assistance** on the root access group.
End remote processes and applications.	**Manage Remote Processes and Applications** on the root access group.
Perform all tasks in Horizon Help Desk Tool.	**Manage Global Sessions** on the root federation access group. If the local pod is not part of a pod federation, the administrator must have **Manage Global Sessions** on the root access group. In addition, the administrator must have **Manage Reboot Operation**, **Manage Sessions**, **Remote Assistance**, and **Manage Remote Processes and Applications** on the root access group.
Remote assistance operations and end remote processes and applications.	**Manage Help Desk (Read Only)**, **Remote Assistance**, and **Manage Remote Processes and Applications**

Privileges and Roles for General Administration Tasks and Commands

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

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

Table 8-16. Privileges and Roles for General Administration Tasks and Commands

Task	Required Privileges or Roles
Add or delete an access group or federation access group	**Manage Access Groups**
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 Agent	**Manage Global Configuration and Policies**
Run all PowerShell commands and command line utilities except for `vdmadmin` and `vdmimport`.	**Direct Interaction** **Note** Horizon adds the **Direct Interaction** privilege to new roles automatically. This privilege is not visible in the list of privileges in Horizon Console.
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.
Read only access to a vCenter Server configuration.	**Manage vCenter Configuration (Read only)**

Best Practices for Administrator Users and Groups

To increase the security and manageability of your VMware Horizon 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 VMware Horizon privileges.
- Keep the number of users with VMware Horizon 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 VMware Horizon configuration settings.
- Create federation access groups to segregate sensitive global entitlements. Delegate the administration of those federation access groups to a limited set of users.

Setting Group Policies for Horizon Components

9

You can use group policy settings to configure the behavior of certain Horizon components.

For general information about installing the Horizon ADMX template files and editing group policy settings, see the *Configuring Remote Desktop Features in Horizon* document.

This chapter includes the following topics:

VMware View Server Configuration ADMX Template Settings

The VMware View Server Configuration ADMX (`vdm_server.admx`) template file contains policy settings related to Connection Server.

The following table describes each policy setting in the VMware View Server 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 9-1. VMware View 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 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`.

VMware View Common Configuration ADMX Template Settings

The VMware View Common Configuration ADMX (`vdm_common.admx`) template file contains 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 VMware View 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 9-2. VMware View Common Configuration Template: Log Configuration Settings

Setting	Properties
`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.
`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.
`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.
`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.
`Send logs to a Syslog server`	Allows Horizon server logs to be sent to a Syslog server such as VMware vCenter Log Insight. Logs are sent from all Horizon 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 Horizon 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 9-3. VMware View Common Configuration Template: Performance Alarm Settings describe the performance alarm settings in the VMware View 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 9-3. VMware 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.
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 wild cards 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 only to Connection Server and Horizon Agent systems. These settings do not apply to Horizon Client systems.

Security Settings

Table 9-4. VMware View Common Configuration Template: Security Settings describe the security settings in the VMware View 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 9-4. VMware 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 The default is WholeChainButRoot.

General Settings

Table 9-5. VMware View Common Configuration Template: General Settings describes the general settings in the VMware View 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 9-5. VMware View Common Configuration Template: General Settings

Setting	Properties
Configure dump count on program error	Limits the number of dump files that can be created. Set **Maximum dump files to be created** to any numerical value. The value takes effect per process and per process for each user. If you set the value to 0, no dump files are created. If you do not configure this setting, the number of dump files that can be created is 128 or unlimited, depending on the process that generates the dump files.
Configure dump type on program error	Specifies the size of the dump files that can be created. Valid values are as follows: ■ **Full** - Produces a full dump. The dump contains the full memory of a process. The size of a full dump is relatively large. ■ **Mini** - The dump contains enough information to produce a stack trace and enable you to perform basic troubleshooting steps. The dump does not contain full memory, so you cannot extract information about some objects or object names. The size of the dump is relatively small. If this setting is not configured, a full dump is created by default.
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.

Table 9-5. VMware View Common Configuration Template: General Settings (continued)

Setting	Properties
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 Components 10

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

This chapter includes the following topics:

Backing Up and Restoring VMware Horizon Configuration Data

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

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

Backing Up Horizon Connection Server Data

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

VMware Horizon stores LDAP Connection Server configuration data in the Horizon LDAP repository.

When you use Horizon Console to perform backups, VMware Horizon backs up the Horizon LDAP configuration data. The Horizon LDAP data is exported in encrypted LDAP data interchange format (LDIF). For a description of Horizon LDAP, see "Horizon LDAP" in the *Horizon Architecture Planning* document.

You can perform backups in several ways.

- Schedule automatic backups by using the VMware Horizon configuration backup feature.
- Initiate a backup immediately by using the **Backup Now** feature in Horizon Console.

- Manually export Horizon LDAP data by using the `vdmexport` utility. This utility is provided with each instance of Connection Server.

  The `vdmexport` utility can export Horizon 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 Horizon LDAP data only. This tool does not back up Horizon Console database information.

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

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

- VMware Horizon 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 VMware Horizon synchronizes data in replicated instances of Connection Server, any data lost in one instance might be lost in all members of the group.

Schedule VMware Horizon Configuration Backups

You can schedule your VMware Horizon configuration data to be backed up at regular intervals. VMware Horizon backs up the contents of the Horizon 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 Configuration Backup Settings.

Procedure

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

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

Table 10-1. Horizon Configuration Backup Settings

Setting	Description
Automatic backup frequency	Every Hour. Backups take place every hour on the hour. Every 6 Hours. Backups take place at midnight, 6 am, noon, and 6 pm. Every 12 Hours. Backups take place at midnight and noon. Every Day. Backups take place every day at midnight. Every 2 Days. Backups occur at midnight on Saturday, Monday, Wednesday, and Friday. Every Week. Backups take place weekly at midnight on Saturday. Every 2 Weeks. Backups take place every other week at midnight on Saturday. Never. Backups do not take place automatically.
Backup time	Time to schedule a backup.
Backup time offset	Time offset for a scheduled backup.
Max number of backups	Number of backup files that can be stored on the Connection Server instance. The number must be an integer greater than 0. When the maximum number is reached, VMware Horizon 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**, VMware Horizon 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 Horizon LDAP repository.

You use the `vdmexport` command to export the Horizon 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.

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 Horizon LDAP configuration. The cleansed configuration data is missing passwords and other critical information.

Results

For more information about the `vdmexport` command, see Export LDAP Configuration Data.

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 Configuration Data.

Restoring Horizon Connection Server Configuration Data

You can manually restore the Connection Server LDAP configuration files that were backed up by VMware Horizon.

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

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

Note In certain situations, you might have to install the current version of a Connection Server instance and restore the existing VMware Horizon 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 VMware Horizon configuration, or for other reasons. For more information, see the *Horizon 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 Horizon LDAP repository in the Connection Server instance.

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

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

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

For information about backing up the Horizon LDAP repository, see Backing Up Horizon Connection Server 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. Uninstall all instances of Horizon Connection Server.

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

2. Install one instance of Connection Server.
3. Stop the Connection Server instance by stopping the Windows service VMware Horizon Connection Server.
4. Click **Start > Command Prompt**.
5. Decrypt the encrypted LDIF file.

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

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

6. Import the decrypted LDIF file to restore the Horizon LDAP configuration.

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

7. Uninstall Connection Server.

   Uninstall only the package VMware Horizon Connection Server.

8. Reinstall Connection Server.
9. Log in to Horizon Console and validate that the configuration is correct.
10. Reinstall the replica server instances.

Results

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

Note Make sure that the configuration that is being restored matches the virtual machines that are known to vCenter Server.

Setting Up Clients in Kiosk Mode

11

You can set up unattended clients that can obtain access to their desktops from VMware Horizon.

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.

VMware Horizon uses the Flexible Authentication feature 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 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.

In a Cloud Pod Architecture environment, the Connection Server instances in the pod federation do not share information about clients in kiosk mode. To implement a workaround, see VMware Knowledge Base (KB) article 2148888.

This chapter includes the following topics:

Configure Clients in Kiosk Mode

To configure Active Directory and VMware Horizon 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 Console to entitle users or groups to remote desktops.
- **Administrators** or an equivalent role to run the `vdmadmin` command.

Procedure

1. Prepare Active Directory and VMware Horizon 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 VMware Horizon 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 an instant-clone desktop 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.

VMware Horizon 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 Console, 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, instant-clone desktop pool as being most suitable for the requirements of your client application.

   Important Do not entitle a client or a group to more than one desktop pool. If you do, VMware Horizon 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, VMware Horizon 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, VMware Horizon 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 VMware Horizon 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!"
```

Monitoring and Troubleshooting in Horizon Console

12

You can use a variety of procedures for monitoring, diagnosing, and fixing problems that you might encounter when using VMware Horizon. You can use Horizon Help Desk Tool for monitoring and 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 Console* document.

This chapter includes the following topics:

Using Horizon Help Desk Tool in Horizon Console

Horizon Help Desk Tool is a Web application that you can use to get the status of VMware Horizon 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 VMware Horizon. To verify that you have the correct license, see "Change the Product License Key or License Modes in Horizon Console" in *Horizon Administration*.
- An event database to store information about VMware Horizon components. For more information about configuring an event database, see the *Horizon 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 "Privileges for Help Desk Tool Tasks" in *Horizon Administration*.
- Enable the timing profiler on each Connection Server instance to view login 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}
  ```

Start Horizon Help Desk Tool in Horizon Console

Horizon Help Desk Tool is integrated into Horizon Console. You can search for a user that you want to troubleshoot problems for in Horizon Help Desk Tool.

Procedure

1. You can search for a user name in the User Search text box or navigate directly to the Horizon Help Desk Tool tool.
   - In Horizon Console, enter a user name in the User Search text box.
   - Select **Monitor > Help Desk** and enter a user name in the User Search text box.

   Horizon Console displays a list of users in the search results. The search can return up to 100 matching results.
2. Select a user name.

   The user information appears in a user card.

What to do next

To troubleshoot problems, click the related tabs in the user card.

Troubleshooting Users in Horizon Help Desk Tool

In Horizon Help Desk Tool, you can view basic user information in a user card. You can click tabs in the user card to get more details about specific components.

The user details can sometimes appear in tables. You can sort these user details by table columns.

- To sort a column by ascending order, click the column once.
- To sort a column by descending order, click the column twice.
- To not sort the column, click the column thrice.

Basic User Information

Displays basic user information such as user name, phone number, and email address of the user and the connected or disconnected status of the user. If the user has a desktop or application session, the status of the user is connected. If the user does not have any desktop or application sessions, the status of the user is disconnected.

You can click the email address to send a message to the user.

You can also click the phone number to open a Skype for Business session to call the user to collaborate with the user on a troubleshooting task.

Note The Skype for Business information is not displayed for Linux desktop users.

Sessions

The **Sessions** tab displays information about desktop or application sessions that the user is connected to.

You can use the **Filter** text box to filter desktop or application sessions.

Note The **Sessions** tab does not display session information for sessions that use the Microsoft RDP display protocol or sessions that access VMs from vSphere Client or ESXi.

The **Sessions** tab includes the following information:

Table 12-1. Sessions tab

Option	Description
State	Displays information about the state of the desktop or application session. ■ Appears green, if the session is connected. ■ L, if the session is a local session or a session running in the local pod.
Computer Name	Name of the desktop or application session. Click the name to open the session information in a card. You can click the tabs in the session card to view additional information: ■ The **Details** tab displays the user information such as the VM information, CPU, or memory usage. ■ The **Processes** tab displays information about CPU and memory related processes. ■ The **Applications** tab displays the details about the applications that are running. **Note** You cannot access the **Applications** tab for Linux desktop sessions.
Protocol	Display protocol for the desktop or application session.
Type	Displays whether the desktop is a published desktop, virtual machine desktop, or an application.
Connection Time	The time the session connected to Connection Server.
Session Duration	The duration of time the session remained connected to Connection Server.

Desktops

The **Desktops** tab displays information about the published desktops or virtual desktops that the user is entitled to use.

Table 12-2. Desktops

Option	Description
State	Displays information about the state of the desktop session. ■ Appears green, if the session is connected.
Desktop Pool Name	Name of the desktop pool for the session. Displays Linux as the desktop pool for a Linux desktop session.
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 12-2. Desktops (continued)

Option	Description
Type	Displays information about the type of desktop entitlement. ■ Local, for a local entitlement.
vCenter	Displays the name of the virtual machine in vCenter Server. **Note** Does not display any information if the session is running in a different pod in the pod federation.
Default Protocol	Default display protocol for the desktop or application session.

Applications

The **Applications** tab displays information about the published applications that the user is entitled to use.

Note You cannot access the **Applications** tab for Linux desktop sessions.

Table 12-3. Applications

Option	Description
State	Displays information about the state of the application session. ■ Appears green, if the session is connected.
Applications	Displays the names of published applications in the application pool.
Farm	Name of the farm that contains the RDS host that the session connects to. **Note** If there is a global application entitlement, this column shows the number of farms in the global application entitlement.
Type	Displays information about the type of application entitlement. ■ Local, for a local entitlement.
Publisher	Software manufacturer name of the published application.

Activities

The **Activities** tab displays the event log information about the user's activities. You can filter activities by a time range such as the Last 12 hours or Last 30 Days or by administrator name. Click **Help Desk Event Only** to filter only by Horizon Help Desk Tool activities. Click the refresh icon to refresh the event log. Click the export icon to export the event log as a file.

Note The event log information is not displayed for users in a Cloud Pod Architecture environment.

Table 12-4. Activities

Option	Description
Time	Select a time range. Default is the last 12 hours. ■ **Last 12 Hours** ■ **Last 24 Hours** ■ **Last 7 Days** ■ **Last 30 Days** ■ **All**
Admins	Name of the administrator user.
Message	Displays messages for a user or administrator that are specific to the activities that the user or administrator performed.
Resource Name	Displays information about the desktop pool or virtual machine name on which the activity was performed.

Session Details for Horizon Help Desk Tool

The session details appear on the **Details** tab when you click a user name in the **Computer Name** option on the **Sessions** tab. You can view details for Horizon Client, the virtual or published desktop, and CPU and memory details.

Horizon Client

Displays information that depends on the type of Horizon Client and includes details such as user name, version of Horizon Client, IP address of the client machine, and the operating system of the client machine.

Note If you upgraded Horizon Agent, you must also upgrade Horizon Client to the latest version. Else, no version is displayed for Horizon Client. For more information about upgrading Horizon Client, see the *Horizon Upgrades* document.

VM

Displays information about virtual desktops or published desktops.

Table 12-5. VM Details

Option	Description
Computer Name	Name of the desktop or application session.
Agent Version	Horizon Agent version.
OS Version	Operating System version.
Connection Server	The Connection Server that the session connects to.
Pool	Name of the desktop or application pool. Displays Linux for a Linux desktop pool.
vCenter	IP address of vCenter Server.
Session State	State of the desktop or application session. The session states can be idle, active, or disconnected. If the user is not active for one minute, the session status turns idle. The status icon appears as green outline for idle, solid green for active, and gray for disconnected. **Note** Linux desktop sessions do not display the idle status.
Session Duration	The time the session remained connected to Connection Server.
State Duration	The time the session remained in the same state.
Logon Time	The logon time of the user who logged in to the session.
Logon Duration	The time the user remained logged in to the session.
Gateway/Proxy Name	Name of the security server, Unified Access Gateway appliance, or load balancer. This information might take from 30 seconds through 60 seconds to display after connecting to the session.
Gateway/Proxy IP	IP address of the security server, Unified Access Gateway appliance, or load balancer. This information might take from 30 seconds through 60 seconds to display after connecting to the session.
Farm	The farm of RDS hosts for the published desktop or application session.

User Experience Metrics

Displays performance details for a virtual or published desktop session that uses the PCoIP or VMware Blast display protocol. To view these performance details, click **More**. To refresh these details, click the refresh icon.

Table 12-6. PCoIP Display Protocol Details

Option	Description
Tx Bandwidth	The transmission bandwidth, in kilobits per second, in a PCoIP session.
Frame Rate	The frame rate, in frames per second, in a PCoIP session.
Packet Loss	Percentage of packet loss in a PCoIP session.
Skype Status	The Skype for Business status in a PCoIP session. ■ Optimized ■ Fallback ■ Optimized (version-mismatch) ■ Fallback (version-mismatch) ■ Connecting ■ Disconnected ■ Undefined This option appears as N/A for Linux desktop sessions.

Table 12-7. Blast Display Protocol Details

Option	Description
Frame Rate	The frame rate, in frames per second, in a Blast session.
Skype Status	The Skype for Business status in a Blast session. ■ Optimized ■ Fallback ■ Optimized (version-mismatch) ■ Fallback (version-mismatch) ■ Connecting ■ Disconnected ■ Undefined This option appears as N/A for Linux desktop sessions.
Blast Session Counters	■ **Estimated Bandwidth (Uplink)**. Estimated bandwidth for an uplink signal. ■ **Packet Loss (Uplink)**. Percentage of packet loss for an uplink signal.
Blast Imaging Counters	■ **Transmitted Bytes**. Total number of bytes for imaging data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for imaging data that have been received for a Blast session.

Table 12-7. Blast Display Protocol Details (continued)

Option	Description
Blast Audio Counters	■ **Transmitted Bytes**. Total number of bytes for audio data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for audio data that have been received for a Blast session.
Blast CDR Counters	■ **Transmitted Bytes**. Total number of bytes for Client Drive Redirection data that have been transmitted for a Blast session. ■ **Received Bytes**. Total number of bytes for Client Drive Redirection data that have been received for a Blast session.

CPU and Memory Usage and Network and Disk Performance

Displays charts for CPU and memory usage of the virtual or published desktop or application and the network or disk performance for the PCoIP or Blast display protocol.

Note Following a start or a restart of Horizon Agent on the desktop, the performance charts might not display the timeline immediately. The timeline appears after a few minutes.

Table 12-8. CPU Usage

Option	Description
Session CPU	CPU usage of the current session.
Host CPU	CPU usage of the virtual machine to which the session is assigned.

Table 12-9. Memory Usage

Option	Description
Session Memory	Memory usage of the current session.
Host Memory	Memory usage of the virtual machine to which the session is assigned.

Table 12-10. Network Performance

Option	Description
Latency	Displays a chart for the latency for the PCoIP or Blast session. For the Blast display protocol, the latency time is the Round-Trip Time in milliseconds. The performance counter that tracks this latency time is **VMware Blast Session Counters > RTT**. For the PCoIP display protocol, the latency time is the Round-Trip Latency time in milliseconds. The performance counter that tracks this latency time is **PCoIP Session Network Statistics > Round Trip Latency**.

Table 12-11. Disk Performance

Option	Description
Read	The number of read Input/Output (I/O) operations per second.
Write	The number of write I/O operations per second.
Disk Latency	Displays a chart for the disk latency. The disk latency is the time in milliseconds from the Input/Output Operations Per Second (IOPS) data retrieved from the Windows performance counters.
Average Read	Average number of random read I/O operations per second.
Average Write	Average number of random write I/O operations per second.
Average Latency	Average latency time in milliseconds from the IOPS data retrieved from the Windows performance counters.

Session Logon Segments

Displays the logon duration and usage segments that are created during logon.

Table 12-12. Session Logon Segments

Option	Description
Logon duration	The length of time calculated from the time the user clicks the desktop or application pool to the time when Windows Explorer starts.
Session Logon Time	The length of time that the user was logged in to the session.
Logon Segments	Displays the segments that are created during logon. ■ **Brokering**. Total time for Connection Server to process a session connect or reconnect. Calculated from the time the user clicks the desktop pool to the time when the tunnel connection is set up. Includes the times for Connection Server tasks such as user authentication, machine selection, and machine preparation for setting up the tunnel connection. ■ **GPO load**. Total time for Windows group policy processing. Displays 0 if there is no global policy configured. ■ **Profile load**. Total time for Windows user profile processing. ■ **Interactive**. Total time for Horizon Agent to process a session connect or reconnect. Calculated from the time when PCoIP or Blast Extreme uses the tunnel connection to the time when Windows Explorer starts. ■ **Protocol Connection**. Total time taken for the PCoIP or Blast protocol connection to complete during the logon process. ■ **Logon Script**. Total time taken for a logon script to execute from start to completion. ■ **Authentication**. Total time for Connection Server to authenticate the session. ■ **VM Start**. Total time taken to start a VM. This time includes the time for booting the operating system, resuming a suspended machine, and the time it takes Horizon Agent to signal that it is ready for a connection.

Use the following guidelines when you use the information in logon segments for troubleshooting:

- If the session is a new virtual desktop session, all the logon segments appear. If no global policy is configured, the **GPO Load** logon segment time is 0.
- If the virtual desktop session is a reconnected session from a disconnected session, the **Logon Duration**, **Interactive**, and **Brokering** logon segments appear.
- If the session is a published desktop session, the **Logon Duration**, **GPO Load**, or the **Profile load** logon segments appear. The **GPO Load** and **Profile load** logon segment appear for new sessions. If these logon segments do not appear for new sessions, you must restart the RDS host.

- If the session is a Linux desktop session, the **GPO Load** and **Profile load** segments do not appear.
- Logon data might not be immediately available when the desktop session connects. The logon data appears after a few minutes.

Session Processes for Horizon Help Desk Tool

The session processes appear on the **Processes** tab when you click a user name in the **Computer Name** option on the **Sessions** tab.

Processes

To avoid scrolling through the list of session processes, you can search for a session process by name by entering the process name in the search filter text box.

For each session, you can view additional details about CPU and memory related processes. For example, if you notice that the CPU and memory usage for a session is abnormally high, you can view the details for the process on the **Processes** tab.

For RDS host sessions, the **Processes** tab displays the current RDS host session processes started by the current user or current system process.

Table 12-13. Session Process Details

Option	Description
Process Name	Name of the session process. For example, chrome.exe.
CPU	CPU usage of the process in percent.
Memory	Memory usage of the process in KB.
Disk	Memory disk IOPs. Calculated using the following formula: (Total I/O bytes of current time) - (Total I/O bytes one second before the current time). This calculation can display a value of 0 KB per second if the Task Manager displays a positive value.
Username	User name of the user who owns the process.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Processes	Count of processes in the virtual machine

Table 12-13. Session Process Details (continued)

Option	Description
Refresh	The refresh icon refreshes the list of processes.
End Process	Ends a process that is running. **Note** You must have the Help Desk Administrator role to end a process. To end a process, select a process and click the **End Process** button. You cannot end critical processes such as Windows core processes that might be listed in the **Processes** tab. If you end a critical process, Horizon Help Desk Tool displays a message that states it cannot end the system process.

Application Status for Horizon Help Desk Tool

You can view the status and details of an application on the **Applications** tab when you click a user name in the **Computer Name** option on the **Sessions** tab. You cannot access the **Applications** tab for Linux desktop sessions.

Applications

To avoid scrolling through the list of applications, you can search for an application by name by entering the application name in the search filter text box.

For each application, you can view the current status and other details.

You can end an application process for the end user. To end an application process, click **End Application** and click **OK** to confirm the change.

Note The end application process can fail if the application is pending a user interaction such as unsaved data or because of other exceptions. However, Horizon Help Desk Tool does not display any success or failure message when you end an application.

Table 12-14. Application Details

Option	Description
Application	Name of the application.
Description	Description of the application.
Status	Status of the application. Displays whether the application is running or not.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.

Table 12-14. Application Details (continued)

Option	Description
Applications	List of applications that are running.
Refresh	The refresh icon refreshes the list of applications.

Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool

In Horizon Help Desk Tool, you can troubleshoot desktop or application sessions based on a user's connection status.

Prerequisites

- Start Horizon Help Desk Tool.

Procedure

1. On the user card, click the **Sessions** tab.

   A performance card appears that displays CPU and memory usage and includes information about Horizon Client, and the virtual or published desktop.

2 Choose a troubleshooting option.

Option	Action
Send Message	Sends a message to the user on the published desktop or virtual desktop. You can choose the severity of the message to include Warning, Info, or Error. Click **Send Message** and enter the type of severity and the message details, and then click **Submit**.
Remote Assistance	You can generate remote assistance tickets for connected desktop or application sessions. Administrators can use the remote assistance ticket to take control of a user's desktop and troubleshoot problems. **Note** This feature is not available for Linux desktop users. Click **Remote Assistance** and download the Help Desk ticket file. Open the ticket and wait for the ticket to be accepted by the user on the remote desktop. You can open the ticket only on a Windows desktop. After the user accepts the ticket, you can chat with the user and request control of the user's desktop. **Note** The Help Desk remote assistance feature is based on Microsoft Remote Assistance. You must install Microsoft Remote Assistance and enable the Remote Assistance feature on the published desktop. Help Desk remote assistance might not start if Microsoft Remote Assistance has connection or upgrade issues. For more information, see the Microsoft Remote Assistance documentation on the Microsoft Web site.
Restart	Initiates the Windows Restart process on the virtual desktop. This feature is not available for a published desktop or application session. Click **Restart VDI**.
Disconnect	Disconnect the desktop or application session. Click **More > Disconnect**.
Log Off	Initiates the log off process for a published desktop or virtual desktop, or the log off process for an application session. Click **More > Log Off**.
Reset	Initiates a reset of the virtual machine. This feature is not available for a published desktop or application session. Click **More > Reset VM**. **Note** The user can lose unsaved work.

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. To start the service, see KB 57051.
- Integrates with Horizon Help Desk Tool timing profiler. Logon-related metrics are aggregated and sent to the Horizon Agent events database. For information on how to enable the timing profiler, see Using Horizon Help Desk Tool in Horizon Console.
- Enables customers to upload logs to a file server for easier access.
- Integrates with other VMware products, such as 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.
- Retrives legacy data. The Retrieve Legacy Data feature not work for a session that is connected after an upgrade to Horizon 2103 or later and is only available for a session that was connected in an earlier version before the upgrade.

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 12-15. 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.

Table 12-15. Logon Monitor Metrics (continued)

Metric	Parameters	Description
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.
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.

Table 12-15. Logon Monitor Metrics (continued)

Metric	Parameters	Description
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.
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, 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 12-16. 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 VMware Horizon 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. ■ The value to set to create folders per user in remote path is 0x10. 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 12-17. 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 12-18. Horizon Performance Tracker System Requirements

System	Requirements
Virtual desktop operating systems	All operating systems that support Horizon Agent, except Linux agents.
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
.NET Framework	Horizon Performance Tracker requires .NET Framework version 4.0 or later.

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* 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 Configure the Horizon Performance Tracker Group Policy Settings.

Configure the Horizon Performance Tracker Group Policy Settings

To configure Horizon Performance Tracker, install the Horizon Performance Tracker ADMX template file (`perf_tracker.admx`) on the agent machine and use the Local Group Policy Editor to configure the policy settings.

All ADMX files that provide group policy settings for Horizon are available in `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip`, where *YYMM* is the marketing version, *x.x.x* is the internal version and *yyyyyyyy* 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 download, which includes the GPO Bundle containing the ZIP file.

Procedure

1. Extract the `perf_tracker.admx` file from the `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` file and copy it to the `%systemroot%\PolicyDefinitions` folder on the agent machine.

2 Extract the `perf_tracker.adml` file from the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy it to the appropriate language subfolder in the `%systemroot%\PolicyDefinitions\` folder on the agent machine.

   For example, copy the `en_us` version of the `perf_tracker.adml` file to the `%systemroot%\PolicyDefinitions\en_us` subfolder.

3 Start the Local Group Policy Editor (`gpedit.msc`) and navigate to **Computer Configuration > Administrative Templates > VMware Horizon Performance Tracker**.

4 Edit the group 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 starts automatically when a user logs in 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 starts automatically when a user logs in to a remote application connection. To clear this preference GPO setting, select **Disable**.

5 To make your changes take effect, restart Horizon Performance Tracker on the agent machine.

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 Configure the Horizon Performance Tracker Group 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.

Configuring Load Balancers for Horizon Connection Server Health Monitoring

To monitor load balancing health on Horizon Connection Server, follow these best practices.

To avoid flooding Connection Server with a large number of health check requests, set the polling interval to 30 seconds, with a timeout of two or three times that period. Try to have no more than two load balancers sending probes to one Connection Server instance.

The only supported health check is a fetch of `favicon.ico`. To minimize the cost of the probe, use the `HEAD` method where possible. Whether or not the check is successful, you must drop the connection after the fetch by either adding a Connection: close header to the request or else using an HTTP/1.0 request. An example of using the `HEAD` method in the send string of the load balancer:

```
HEAD /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n
```

The HTTP status is usually 200. If the Connection Server has been administratively disabled (see Disable or Enable Horizon Connection Server in Horizon Console), the status will be 503.

For timeout settings and load balancer persistence values, see the KB article on Timeout Settings and Load Balancer Persistence.

Monitor VMware Horizon Components

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

Horizon Console displays monitoring information about Connection Server instances, the event database, gateways, datastores, vCenter Server instances, domains, and sessions in a Cloud Pod Architecture environment.

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

For information about monitoring sessions in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon* document.

Procedure

1 The top panel of the Horizon Console navigator displays the summary details for dashboard statistics including the latest refresh date and the total number of issues against **Sessions**, **Problem vCenter VMs**, **Problem RDS Hosts**, **Events**, and **System Health**.

   You can click the refresh icon to get the latest dashboard statistics.

   You can click on the issue number to view more details about component issues.

   - A green check mark indicates that a component has no problems.
   - A red exclamation mark indicates that a component is unavailable or not functioning.
   - A yellow exclamation mark indicates that a component is in a warning state.
   - A gray question mark indicates that the status of a component is unknown.

2 Navigate to **Monitor > Dashboard**.

The **System Health** pane displays information about system components that have issues. You can click each system component to get a high-level view of the affected components, status, and description of the issue.

3 To view more information about an issue, click **View** and then make a selection.

Option	Description
Components	Displays information about service components. To view information about service components and perform troubleshooting tasks, click the **Connection Servers**, **Gateway Servers**, **Event Database**, or **True SSO** tabs. To perform the following tasks, select a component. ■ View status, name, version, and other details. ■ If you select a Connection Server instance, click the **View Services Status** tab to view information about gateway services. ■ If you select a Connection Server instance, click the **View Sessions Detail** tab to view information about Connection Server sessions.
RDS Farms	Displays information about farms. To view more information about the farm, including the RDS hosts that belongs to the farm, click a farm ID.
vSphere	Displays information about components related to vSphere. To view information about each component, click the **Datastores**, **ESX Hosts**, and **vCenter Servers** tabs.
Other Components	To view more information about each component, click the **Domains**, **SAML 2.0**, and **License Service** tabs. **Note** If a SAML 2.0 authenticator has a warning because of an untrusted certificate, you can click the certificate link to accept and validate the certificate.
Remote Pods	Displays information about remote Horizon pods. **Note** This section only appears when the Cloud Pod Architecture feature is enabled.

4 To see bar charts that display the number of active, disconnected, or idle sessions of virtual desktops, published desktops, and published applications, view the **Sessions** pane.

5 To view sessions, click **View** in the **Sessions** pane.

The **Sessions** page displays information about the sessions.

6 To view datastores, click **View** in the **Workload** pane.

You can select a datastore to view additional details such as current use for the datastore. Horizon Console displays a warning if the free space for a datastore slips below a threshold value. If there are desktop pools related to a selected datastore, you can view the information for the desktop pools when you select the datastore. The **Other Datastores** column displays information for desktop pools or farms that span multiple datastores.

Monitor Horizon Connection Server Load Status

You can monitor the load for a Connection Server in the Horizon Console dashboard. For each Connection Server, you can view the percentage of CPU and memory consumed, the number of display protocol sessions, Connection Server connection sessions, or the threshold for the maximum number of sessions that can connect to a Connection Server. You can also view the number of connected sessions for an RDS host.

Note When all gateway settings are enabled, Horizon Console displays a session limit, which is the Connection Server sessions allowed maximum, and expresses Connection Server session counts as a percentage of this limit. When gateway settings are not enabled, no session limit is given, and the absolute number of Connection Server sessions is shown.

Procedure

1. In Horizon Console, navigate to **Monitor > Dashboard**.
2. In the **System Health** pane, click **View**.

   In the **Components** pane, on the **Connection Servers** tab, the **Sessions** column displays the percentage of Connection Server sessions for each Connection Server. The **CPU Consumption** column displays the percentage of CPU consumed for each Connection Server. The **Memory Consumption** column displays the percentage of memory consumed for each Connection Server.
3. Select a Connection Server and click **View Sessions Detail** to view the number of gateway and non-gateway protocol sessions, and if shown the session limit, for this Connection Server.

   A gateway protocol session passes through a Blast Secure Gateway, PCoIP Secure Gateway, or HTTPS Secure Tunnel on the Connection Server that manages the connection. For example, Connection Server is configured to use PCoIP Secure Gateway connection and Horizon Client uses the PCoIP protocol to connect to the Connection Server.

   A non-gateway protocol session does not pass through a Blast Secure Gateway, PCoIP Secure Gateway, or HTTPS Secure Tunnel on the Connection Server that manages the connection. For example, Connection Server is configured to use HTTP(s) Secure Tunnel connection and Horizon Client uses the PCoIP protocol to connect to the Connection Server.
4. To view the number of sessions on an RDS host, in the **Components** pane, click **RDS Farms**, and click a farm ID.

   The Sessions column displays the number of sessions on an RDS host.

Monitor Services on Horizon Connection Server

You can monitor the gateway service components running on a Connection Server in the Horizon Console dashboard. Gateway service components include secure gateway connection configured with HTTP(s) secure tunnel, PCoIP gateway and Blast Secure Gateway connections.

Procedure

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

2 In the **System Health** pane, click **View**.

3 Select a Connection Server and select **View Services Status**.

The **Gateway Services Status** dialog displays the status of gateway service components and the gateway service components in use.

Note The service components that are not enabled appear grayed out.

Monitoring Perpetual License Usage

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

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

For named users, VMware Horizon counts the number of unique users that have accessed the VMware 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 **Usage Settings** panel displays the number of users since your VMware 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, VMware 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 **Usage Settings** panel displays the highest number of concurrent desktop sessions and published desktop and application users since your VMware 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.

Change the Product License Key or License Modes in Horizon Console

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

You can add a license to VMware Horizon while VMware Horizon 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 VMware Horizon and add-on features, obtain a valid product license key.
- To use a subscription license, verify that you enable VMware Horizon for a subscription license. See, "Enabling VMware Horizon for Subscription Licenses and Horizon Control Plane Services" in the *Horizon Installation* document. The **Licensing** panel displays information about the subscription license for the Horizon pod.

Procedure

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

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

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

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

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

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

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

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

5 Verify the license expiration date.

6 Verify that the component licenses are enabled or disabled, based on the edition of VMware Horizon that your product license entitles you to use.

   Not all features and capabilities of VMware Horizon are available in all license editions. For a comparison of feature sets in each edition, see https://www.vmware.com/products/horizon.html.

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

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

Reset Perpetual License Usage Data

In Horizon Console, you can reset the perpetual license 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 Perpetual License Usage.

Procedure

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

2 (Optional) In the **Usage** pane, select **Reset Highest Count**.

   The highest historical number of concurrent connections is reset to the current number.

3 (Optional) In the **Usage** pane, select **Reset Named Users Count**.

Monitor Events in VMware Horizon

The event database stores information about events that occur in the Connection Server host or group, Horizon Agent, and Horizon Console, and notifies you of the number of events on the dashboard. You can examine the events in detail on the **Events** page.

Note Events are listed in the Horizon Console interface for a limited time period. After this time, the events are only available in the historical database tables. You can use Microsoft SQL Server, Oracle, or PostgreSQL database reporting tools to examine events in the database tables. For more information, see Event Database Tables and Schemas.

Note If the event database becomes unavailable, VMware Horizon maintains the audit trail of the events that occur during this period of unavailability and saves them to event database once it becomes available. You must restart the event database and Connection Server to view these events in the Horizon Console interface.

In addition to monitoring events in Horizon Console, you can generate VMware Horizon events in `Syslog` format so that the event data can be accessible to analytics software. See "Configure Event Logging to File or Syslog Server" and "Generating Horizon Event Log Messages in Syslog Format Using the -l Option," in the *Horizon Installation* document.

If you configure an event database for multiple Connection Servers, Horizon Console displays the events for all Connection Servers on the **Events** page. Horizon Console filters events based on the tasks that you perform and displays these events on relevant pages such as the **Desktop Pools** or **Application Pools** pages.

Prerequisites

Create and configure the event database as described in the *Horizon Installation* document.

Procedure

1. In Horizon Console, select **Monitor > Events**.
2. (Optional) On the **Events** page, you can select the time range of the events, filter the events, and sort the listed events by one or more of the columns.

What to do next

In Horizon Console, navigate to a desktop or application pool, virtual machine, or a user or group and click the **Events** tab to view specific events.

VMware Horizon Event Messages

VMware Horizon 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 VMware Horizon reports.

Table 12-19. Types of Event Reported by VMware Horizon

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 VMware Horizon.
Error	Reports a failed operation by VMware Horizon.
Information	Reports normal operations within VMware Horizon.
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 VMware Horizon

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with VMware Horizon.

You can collect diagnostic information for various components of VMware Horizon. How you collect this information varies depending on the VMware Horizon 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`.

- Using DCT to Collect Logs for Remote Desktop Features and Components

  You can set log levels and generate log files in a Data Collection Tool (DCT) bundle for a specific remote desktop feature, or all remote desktop features, on a Horizon Agent for Windows, Horizon Client for Windows, Horizon Client for Mac, or Horizon Client for Linux system.

- Horizon Client for Windows Log Files

  Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can use group policy settings to configure the location, verbosity, and the retention period of some log files.

- Horizon Client for Mac Log Files

  Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

- Horizon Client for Linux Log Files

  Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

- Horizon Client Log Files on Mobile Devices

  On mobile devices, you might need to install a third-party program to navigate to the directory that contains log files. Mobile clients have configuration settings for sending log bundles to VMware. Because logging can affect performance, enable logging only when you need to troubleshoot an issue.

- Horizon Agent Log Files on Windows Machines

  Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can use group policy settings to configure the location, verbosity, and retention period of some log files.

- Linux Desktop Log Files

  Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

- Save Diagnostic Information for Horizon Client for Windows

  If you encounter problems using Horizon Client for Windows, 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 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 Horizon 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 Horizon 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`

Results

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.

Using DCT to Collect Logs for Remote Desktop Features and Components

You can set log levels and generate log files in a Data Collection Tool (DCT) bundle for a specific remote desktop feature, or all remote desktop features, on a Horizon Agent for Windows, Horizon Client for Windows, Horizon Client for Mac, or Horizon Client for Linux system.

Default Installation Paths

The DCT scripts are installed in the following directories and run from the agent and client installation paths.

- Horizon Agent for Windows: `C:\Program Files\VMware\VMware View\Agent\DCT \support.bat`
- Horizon Client for Windows: `C:\Program Files (x86)\VMware\VMware Horizon View Client \DCT\support.bat`
- Horizon Client for Mac: `/Applications/VMware Horizon Client.app/Contents/Library/dct/ HorizonCollector.sh`
- Horizon Client for Linux: `/usr/bin/vmware-view-log-collector`

Command Syntax

Use the following commands to run the DCT script for each platform.

- Horizon Agent for Windows: `support.bat`
- Horizon Client for Windows: `support.bat`
- Horizon Client for Mac: `HorizonCollector.sh`
- Horizon Client for Linux: `vmware-view-log-collector`

Supported Features

The remote desktop features listed in the following table have JSON configuration files that contain log level settings, log collection settings, and dump collection settings.

These services are available on Horizon Agent for Windows, Horizon Client for Windows, Horizon Client for Mac, and Horizon Client for Linux systems, with certain exceptions as noted.

For command-line options that accept feature names, specify the name shown in the Feature Name column.

Feature Name	Full Feature Name
AgentCore	Agent Core **Note** This service is only for Horizon Agent for Windows.
Blast	Blast **Note** This service is only for Horizon Agent for Windows.
Client	Client **Note** This service is not available for Horizon Agent for Windows.
CDR	Client Drive Redirection
Clipboard	Clipboard Redirection

Feature Name	Full Feature Name
DPISync	DPI Synchronization
DnD	Drag and Drop **Note** This service is not available for Horizon Client for Linux.
FA	File Type Association **Note** This service is not available for Horizon Client for Linux.
TSMMR	Multimedia Redirection **Note** This service is not available for Horizon Client for Mac.
PCoIP	PCoIP
PerfTracker	Performance Tracker **Note** This service is available only for Horizon Agent for Windows.
PrintRedir	Printer Redirection
PublishedApp	Published Applications
RTAV	RTAV
ScannerRedirection	Scanner Redirection **Note** This service is not available for Horizon Client for Mac.
SerialPortRedirection	Serial Port Redirection **Note** This service is not available for Horizon Client for Mac.
SmartCard	Smart Card Redirection
URLRedirection	URL Content Redirection
USB	USB Redirection
VDPService	VDPService
Watermark	Digital Watermark

Command-Line Options

The following table describes the command-line options and usage.

Option	Usage	Description

-l	-l	Lists log levels for all the features and components that DCT supports.
		For example, the output of the Horizon Client for Windows command `support.bat -l` lists all the components that DCT controls and the log level status:
		`- Agent Core [INFO]`
		`- PCoIP [INFO]`
		`- Virtual Channel [INFO]`
		`- VDP Service [TRACE]`
		`- Remote Features`
		`- Client Drive Redirection [TRACE]`
		`- Clipboard Redirection`
		`[DEBUG]`
		`- Drag and Drop [TRACE]`
		`- DPI Synchronization [INFO]`
		`- File Type Association [INFO]`

	-l *feature1,feature2 ...*	Lists log levels for the specified features.
		For example, the output of the Horizon Client for Windows command `support.bat -l CDR,DnD` lists the log level status for the Client Drive Redirection and Drag and Drop features:
		`- Client Drive Redirection [TRACE]`
		`- Drag and Drop [TRACE]`

	-l -dumps	Queries the dump settings for the configured processes.
		For example, the output of the Horizon Client for Windows command `support.bat -l -dumps` lists the name, dump type, and maximum dump count for each process:
		`Process Name Dump Type`
		`Max Dump Count`
		`==========`
		`vmware-view.exe Full`
		`128`
		`vmware-remotemks.exe Full`
		`128`
		`vmware-appstub.exe Full`
		`128`
		`horizon_client_service.exe Full`
		`NO LIMIT`
		Note This command is available only for Horizon Client for Windows.

Option	Usage	Description
	-l -dumps count	Queries the dump count for the configured processes. **Note** This command is available only for Horizon Client for Windows.
	-l -dumps type	Queries the dump type for the configured processes. **Note** This command is available only for Horizon Client for Windows.
-ld	-ld *feature1*,*feature2* ...	Lists log level details for the specified features.
-x	-x All:*level*	Sets the log level for all the features that DCT supports. Valid log levels are as follows: ■ Info ■ Debug ■ Trace ■ Verbose
	-x *feature1*:*level1*,*feature2*:*level2* ...	Sets the log level for the specified features or components. For example, the output of the Horizon Client for Linux command `vmware-view-log-collector -x All:TRACE` sets the log level to Trace for all components. The output of the Horizon Client for Linux command `vmware-view-log-collect -x DnD:INFO,CDR:TRACE` sets the log level for the Drag and Drop feature to Info and the log level for the Client Drive Redirection feature to Trace.
-r	-r	Resets the log levels of all features to the installation defaults.
-c	-c All	Collects all logs.
	-c *feature1*,*feature2* ...	Collects logs for the specified features or components.
-d	-d *directory1*	Redirects DCT output to the specified directory.
-f	-f *bundleName*	Specifies the full name of the log bundle file to *bundleName*.
-h	-h	Displays help information for command-line options and lists supported features and components for DCT.

Option	Usage	Description
-del	-del -dumps All	Deletes the dumps for all the features and components that DCT supports. **Note** This command is available only for Horizon Client for Windows.
	-del -dumps *feature1*,*feature2* ...	Deletes the dumps for the specified features. For example, the output of the Horizon Client for Windows command `support.bat –del –dumps Client,FA` deletes the dump files for the Client and File Type Association features. **Note** This command is available only for Horizon Client for Windows.

Real-Time Dump

For Horizon Client for Windows and Horizon Agent for Windows, real-time dump is also supported for some features. This function dumps the target process based on the configuration file setting and collects the dump in the log bundle. Whether a real-time dump needs to be generated depends on the feature's configuration.

For example, if you run the command `support.bat –c` for Horizon Client for Windows, the message `You can choose to generate diagnostic dumps of the VMware Horizon Client processes running on this machine, please note these files can be very large` appears. If you choose Y, dump files are generated for existing processes related to Horizon Client for Windows.

Horizon Client for Windows Log Files

Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can use group policy settings to configure the location, verbosity, and the retention period of some log files.

Log File Locations

For the file names in the following table, *YYYY* represents the year, *MM* is the month, *DD* is the day, and *XXXXXX* is a number.

Table 12-20. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	C:\Users\%*username*%\AppData\Local\Temp	vminst.log_*XXXXXX_XXXXXX*.txt vmmsi.log_*XXXXXX_XXXXXX*.txt
PCoIP client From the vmware-remotemks.exe process	C:\Users\%*username*%\AppData\Local\Temp	pcoip_client_*YYYY_MM_DD_XXXXXX*.txt **Note** You can use a GPO to configure the log level, from 0 to 3 (most verbose). Use the View PCoIP Client Session Variables ADMX template file, pcoip.admx. The setting is **Configure PCoIP event log verbosity**.
Horizon Client UI From the vmware-view.exe process	C:\Users\%*username*%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-*YYYY-MM-DD-XXXXXX*.txt **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file, vdm_common.admx.
Horizon Client logs From the vmware-view.exe process	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username-XXXXXX*	vmware-crtbora-*XXXXXX*.log
Message framework	C:\Users\%*username*%\AppData\Local\VMware\VDM\Logs	log-*YYYY-MM-DD-XXXXXX*.txt debug-*YYYY-MM-DD-XXXXXX*.txt
Remote MKS (mouse-keyboard-screen) logs From the vmware-remotemks.exe process	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	ViewMP-Client-*XXXXXX*.log vmware-mks-*XXXXXX*.log vmware-rdeSvc-*XXXXXX*.log vmware-vvaClient-*XXXXXX*.log
Tsdr client From the vmware-remotemks.exe process	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsdr-Client-*XXXXXX*.log
Tsmmr client From the vmware-remotemks.exe process	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsmmr-Client-*XXXXXX*.log
VdpService client From the vmware-remotemks.exe process	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-vdpServiceClient-*XXXXXX*.log
WSNM service From the wsnm.exe process	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-*XXXXXX*.txt **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file, vdm_common.admx.

Table 12-20. Horizon Client for Windows Log Files (continued)

Type of Logs	Directory Path	File Name
USB redirection From the `vmware-remotemks.exe` process	`C:\ProgramData\VMware\VDM\logs`	`debug-yyyy-mm-dd-XXXXXX.txt` **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file, `vdm_common.admx`.
Serial port redirection From the `vmwsprrdpwks.exe` process	`C:\ProgramData\VMware\VDM\Logs`	`Serial*.txt` `Netlink*.txt`
Scanner redirection From the `ftscanmgr.exe` process	`C:\ProgramData\VMware\VDM\Logs`	`Scanner*.txt` `Netlink*.txt`

Log File Configuration

You can use group policy settings to make the following configuration changes:

- For PCoIP client logs, you can configure the log level, from 0 to 3 (most verbose). Use the View PCoIP Client Session Variables ADMX template file, `pcoip.admx`. The setting is **Configure PCoIP event log verbosity**.
- For client user interface logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file, `vdm_common.admx`.
- For USB redirection logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file, `vdm_common.admx`.
- For WSNM service logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file, `vdm_common.admx`.

You can also use a command-line command to set a verbosity level. Navigate to the `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` directory and enter the following command:

```
support.bat loglevels
```

A new command prompt window appears, and you are prompted to select a verbosity level.

Collecting a Log Bundle

You can use the client user interface, or a command-line command, to collect logs into a ZIP file that you can send to VMware Technical Support.

- In Horizon Client, from the **Options** menu, select **Support Information**. In the dialog box that appears, click **Collect Support Data**.
- From the command line, navigate to the `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` directory and enter the `support.bat` command.

Horizon Client for Mac Log Files

Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

Log File Locations

Table 12-21. Horizon Client for Mac Log Files

Type of Logs	Directory Path	File Name
Horizon Client UI	`~/Library/Logs/VMware Horizon Client`	
PCoIP client	`~/Library/Logs/VMware Horizon Client`	
Real-Time Audio-Video	`~/Library/Logs/VMware`	`vmware-RTAV-pid.log`
USB redirection	`~/Library/Logs/VMware`	
VChan	`~/Library/Logs/VMware Horizon Client`	
Remote MKS (mouse-keyboard-screen) logs	`~/Library/Logs/VMware`	
Crtbora	`~/Library/Logs/VMware`	

Log File Configuration

Horizon Client generates log files in the `~/Library/Logs/VMware Horizon Client` directory on the Mac client. Administrators can configure the maximum number of log files and the maximum number of days to keep log files by setting keys in the `/Library/Preferences/com.vmware.horizon.plist` file on the Mac client.

Table 12-22. plist Keys for Log File Collection

Key	Description
`MaxDebugLogs`	Maximum number of log files. The maximum value is 100.
`MaxDaysToKeepLogs`	Maximum number of days to keep log files. This value has no limit.

Files that do not match these criteria are deleted when you start Horizon Client.

If the `MaxDebugLogs` or `MaxDaysToKeepLogs` keys are not set in the `com.vmware.horizon.plist` file, the default number of log files is 5 and the default number of days to keep log files is 7.

Horizon Client for Linux Log Files

Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

Log File Locations

Table 12-23. Horizon Client for Linux Log Files

Type of Logs	Directory Path	File Name
Installation	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client UI	/tmp/vmware-*username*/	vmware-horizon-client-pid.log
PCoIP client	/tmp/teradici-*username*/	pcoip_client_*YYYY_MM_DD_XXXXXX*.log
Real-Time Audio-Video	/tmp/vmware-*username*/	vmware-RTAV-pid.log
USB redirection	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log
VChan	/tmp/vmware-*username*/	VChan-Client.log **Note** This log is created when you enable RDPVCBridge logs by setting "export VMW_RDPVC_BRIDGE_LOG_ENABLED=1".
Remote MKS (mouse-keyboard-screen) logs	/tmp/vmware-*username*/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService client	/tmp/vmware-*username*/	vmware-vdpServiceClient-pid.log
Tsdr client	/tmp/vmware-*username*/	vmware-ViewTsdr-Client-pid.log

Log File Configuration

You can use a configuration property, `view.defaultLogLevel`, to set the verbosity level for client log files, from 0 (collect all events) to 6 (collect only fatal events).

For USB-specific logs, you can use the following command-line commands:

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

Collecting a Log Bundle

The log collector is located at `/usr/bin/vmware-view-log-collector`. To use the log collector, you must have execute permissions. You can set permissions from the Linux command line by entering the following command:

```
chmod +x /usr/bin/vmware-view-log-collector
```

You can run the log collector from the Linux command line by entering the following command:

`/usr/bin/vmware-view-log-collector`

Horizon Client Log Files on Mobile Devices

On mobile devices, you might need to install a third-party program to navigate to the directory that contains log files. Mobile clients have configuration settings for sending log bundles to VMware. Because logging can affect performance, enable logging only when you need to troubleshoot an issue.

iOS Client Log Files

For iOS clients, log files are in the `tmp` and `Documents` directories under *`User Programs`*`/Horizon/`. To navigate to these directories, you must first install a third-party app, such as iFunbox.

You can enable logging by turning on the **Logging** setting in the Horizon Client settings. When this setting is enabled, if the client exits unexpectedly, or if you exit the client and then start it again, the log files are merged and compressed into a single GZ file. You can then send the bundle to VMware through email. If your device is connected to a PC or Mac, you can use iTunes to retrieve the log files.

Android Client Log Files

For Android clients, log files are in the `Android/data/com.vmware.view.client.android/files/` directory. To navigate to this directory, you must first install a third-party app, such as File Explorer or My Files.

By default, logs are created only after the application exits unexpectedly. You can change this default by turning on the **Enable Log** setting in the Horizon Client settings. To send a log bundle to VMware through email, you can use the **Send the Log** setting in the Horizon Client settings.

Chrome Client Log Files

For Chrome clients, logs are available only through the JavaScript console.

Horizon Agent Log Files on Windows Machines

Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can use group policy settings to configure the location, verbosity, and retention period of some log files.

Log File Locations

For the file names in the following table, *YYYY* represents the year, *MM* is the month, *DD* is the day, and *XXXXXX* is a number.

Table 12-24. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	C:\Users\%*username*%\AppData\Local\Temp	vminst.log_*XXXXXX_XXXXXX*.txt vmmsi.log_*XXXXXX_XXXXXX*.txt
Horizon Agent	*<Drive Letter>*:\ProgramData\VMware\VDM\logs	pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt vmware-vdpServiceServer-*XXXXXX*.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-*XXXXXX*.txt **Note** You can use a GPO to configure the log file location. Use the View Common Configuration ADMX template file, vdm_common.admx.

Log File Configuration

You can use the following methods to configure logging options.

- Use group policy settings to configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file, vdm_common.admx.
- Use a command-line command to set a verbosity level. Navigate to the C:\Program Files\VMware\VMware View\Agent\DCT directory and enter support.bat loglevels. A new command prompt window appears, and you are prompted to select a verbosity level.
- Use the vdmadmin command with the -A option to configure logging by Horizon Agent. For instructions, see the *Horizon Administration* document.

Collecting a Log Bundle

You can use a command-line command to collect logs into a ZIP file that you can send to VMware Technical Support. From the command line, navigate to the C:\Program Files\VMware\VMware View\Agent\DCT directory, and enter the support.bat command.

Linux Desktop Log Files

Log files can help you troubleshoot issues related to installation, display protocols, and feature components. You can create a configuration file to configure the verbosity level.

Log File Locations

Table 12-25. Linux Desktop Log Files

Type of Logs	Directory Path
Installation	/tmp/vmware-root
Horizon Agent	/var/log/vmware
Horizon Agent	/usr/lib/vmware/viewagent/viewagent-debug.log

Log File Configuration

To configure logging, edit the /etc/vmware/config file.

Collecting a Log Bundle

You can create a Data Collection Tool (DCT) bundle that gathers the machine's configuration information and logs into a compressed tarball. Open a command prompt in the Linux desktop and run the dct-debug.sh script.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

The tarball is generated in the directory from which the script was executed (the current working directory). The file name includes the operating system, timestamp, and other information, for example, ubuntu-12-vdm-sdct-20150201-0606-agent.tgz.

This command collects log files from the /tmp/vmware-root directory and the /var/log/vmware directory, and also collects the following system log and configuration files:

- /var/log/messages*
- /var/log/syslog*
- /var/log/boot*.log
- /proc/cpuinfo, /proc/meminfo, /proc/vmstat, /proc/loadavg
- /var/log/audit/auth.log*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg*
- /etc/X11/xorg.conf
- Core files in /usr/lib/vmware/viewagent
- Any crash files in /var/crash/_usr_lib_vmware_viewagent*

Save Diagnostic Information for Horizon Client for Windows

If you encounter problems using Horizon Client for Windows, 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 for Windows 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* document.

For information about collecting support data for other Horizon Client platforms, see the Installation and Setup Guide for that platform. For example, for Horizon Client for Mac, see the *VMware Horizon Client for Mac Installation and Setup Guide*.

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 VMware Horizon 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 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 VMware Horizon 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.
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 File a support request on the Support page of the VMware Web site and attach the output file.

Collect Logs in Horizon Console

You can generate and manage log collection tasks, and download log bundles for Connection Server, desktop pools, and farms in Horizon Console.

With full administrative privileges, you can see and manage all log collection task operations, which include canceling log creation requests and deleting other users' completed log collection tasks.

Administrators without full privileges can see, manage, and cancel only the tasks they initiated.

Prerequisites

You must have log collection privileges to collect logs. In Horizon Console, navigate to **Settings > Administrators > Role Privileges > Add Role**. Create a custom role with the Collection Operation Logs privilege, and add this role to the administrator's permissions.

Procedure

1. In Horizon Console, navigate to **Troubleshooting > Log Collection**.
2. In the **Collect** tab, select the component type, and click **Find**.

   Component types include:

   - **Connection Server**: select a connection server.
   - **Agent**: select a desktop pool from the current pod.
   - **Agent RDS**: select a farm from the current pod.
3. Select a component from the list, and click **Collect**.

   The Log Collection Status window lists the selected components and the log collection task status for each component. Status includes successfully queued logs and failures due to an error. You can refresh the list to see status updates.

   - Connection Server: The log collection task for a Connection Server might fail with `Server busy, try again later` error if that Connection Server is the owner for an Agent log collection task.
   - Agent: After the log collection task completes in the Agent, the Agent log bundles are copied to the Connection Server's local file system.

   Note If a log has already been requested for a specific component, that component will be disabled to prevent duplicate log creation requests.
4. In the **Manage** tab, **Download** column, click the link to download the log bundle for the component.

   The log bundle is downloaded into the user's local file system.

5 To delete a log bundle of a completed log collection task, select the component, and click **Delete**.

The log bundle generated in the log storage directory on the local file system will be deleted. The Delete operation deletes the log collection task and the associated log bundle stored in the log storage directory (default directory: `%PROGRAMDATA%/VMware/VDM/DCT`) on the Connection Server's local file system.

Note You must have full administrative privileges to perform this operation.

6 To cancel a log creation task that you initiated, select the component, and click **Cancel**. You must cancel tasks in an error state before initiating the next task.

The Cancel process varies per component for ongoing and completed tasks:

Component	Ongoing Task Process	Completed Task Process
Connection Server	1 The process running in the background is aborted. 2 The intermediate files generated in the log storage location are deleted. 3 The task is deleted. **Note** If the process running in the background stops due to an error, the abort operation might fail, requiring a manual intervention to recover.	1 The log bundle generated in the log storage location is deleted. 2 The task is deleted.
Agent	1 Connection Server waits for the log collection to complete in the Agent. 2 The Agent log bundle is copied to the Connection Server. 3 The log bundle is deleted. 4 The task is deleted.	1 The log bundle stored in the log storage location is deleted. 2 The task is deleted.

Horizon Connection Server Integration with Skyline Collector Appliance

You can configure Horizon Connection Server to integrate with Skyline Collector Appliance, which VMware Technical Support uses to diagnose and resolve issues with VMware Horizon. Skyline Collector Appliance pulls Connection Server logs for the VMware Horizon administrator user configured for log collection.

Procedure

1 In Horizon Console, create a custom role named Log Collector Administrators with the Collect Operations Logs privilege. See, Add a Custom Role in Horizon Console.

2 Add a description for the custom role.

3 Add a new administrator user and choose the Inventory Administrator (Read Only) role and the Log Collector Administrators custom role for the user.

Results

Skyline Collector Appliance can pull the Connection Server logs for this administrator user to diagnose and resolve VMware Horizon issues.

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.

Send Feedback

Horizon Console periodically displays a pop-up requesting feedback on features. You can choose to provide feedback or provide no feedback in the pop-up or configure Horizon Console to opt out of providing feedback. The Horizon team uses the feedback you provide to improve the product.

Procedure

1 In the Horizon Console header, click the **Send Feedback** icon.

If you are in a DMZ environment and are offline, when you click the **Send Feedback** icon, a pre-populated email window appears. You can use the template email to submit your feedback.

2 Click Next in the dialog box that appears.

   You can choose to opt out of sending feedback or review the VMware Privacy Notice available in the dialog box. If you choose to opt out of sending feedback, Horizon Console will not display any pop-ups requesting feedback.

3 Fill out the fields in the **Send Feedback** window and click **Submit**.

Troubleshooting VMware Horizon Server Certificate Revocation Checking

A Connection Server instance that is used for secure Horizon Client connections might show as red in Horizon Console if certificate revocation checking cannot be performed on the server's TLS certificate.

Problem

A Connection Server icon is red on the Horizon Console dashboard. The Connection 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. By default, the VMware Horizon 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 Connection Server service.

8 On the Horizon Console dashboard, verify that the Connection Server icon is green.

Troubleshooting Smart Card Certificate Revocation Checking

The Connection Server instance 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 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

VMware Horizon 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 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 VMware Horizon server.

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

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

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 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 , 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

13

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 user interface or to perform administration tasks that need to run automatically from scripts.

- 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 VMware Horizon components, and to display the details of a specific health monitor or monitor instance.

- Listing and Displaying Reports of VMware Horizon Operation Using the -I Option

  You can use the `vdmadmin` command with the `–I` option to list the available reports of VMware Horizon operation and to display the results of running one of these reports.

- Generating VMware Horizon Event Log Messages in Syslog Format Using the -I Option

  You can use the `vdmadmin` command with the `–I` option to record VMware Horizon 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 an instant-clone virtual machine for disk space reclamation. VMware Horizon directs the ESXi host to reclaim disk space on the instant-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Console.

- Configuring Domain Filters Using the -N Option

  You can use the `vdmadmin` command with the `–N` option to control the domains that VMware Horizon 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 Using the -S Option

  You can use the `vdmadmin` command with the `–S` option to remove the entry for a Connection Server instance from the VMware Horizon 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 Console to assign the **Administrators** role to a user. See Chapter 8 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 13-1. 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 VMware Horizon.

Table 13-2. 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
–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 VMware Horizon services. See Listing and Displaying Health Monitors Using the -H Option.
–I	Generates reports about VMware Horizon operation. See Listing and Displaying Reports of VMware Horizon 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 VMware Horizon 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 VMware Horizon. See Removing the Entry for a Connection Server Instance 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 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 13-3. 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 13-3. 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 13-4. 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 VMware Horizon 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 VMware Horizon uses to monitor the health of its components.

Table 13-5. 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, VMware Horizon 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 13-6. 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 VMware Horizon Operation Using the -I Option

You can use the `vdmadmin` command with the `–I` option to list the available reports of VMware Horizon 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 VMware Horizon has recorded for a specified report and view.

You can also use the `vdmadmin` command with the `-I` option to generate VMware Horizon log messages in `syslog` format. See Generating VMware Horizon 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 13-7. 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.
`-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 VMware Horizon Event Log Messages in Syslog Format Using the -I Option

You can use the `vdmadmin` command with the `-I` option to record VMware Horizon 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 VMware Horizon event log messages in `Syslog` format. In a `Syslog` file, VMware Horizon 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 VMware Horizon 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. See "Configure Event Logging for Syslog Servers" in the *Horizon Installation* document.

Table 13-8. Options for Generating VMware Horizon Event Log Messages in Syslog Format

Option	Description
`-disable`	Disables `Syslog` logging.
`-e|-enable`	Enables `Syslog` logging.
`-eventSyslog`	Specifies that VMware Horizon 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.

Table 13-8. Options for Generating VMware Horizon Event Log Messages in Syslog Format (continued)

Option	Description
`-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 VMware Horizon events in `Syslog` format.

```
vdmadmin -I -eventSyslog -disable
```

Direct `Syslog` output of VMware Horizon events to the local system only.

```
vdmadmin -I -eventSyslog -enable -localOnly
```

Direct `Syslog` output of VMware Horizon events to a specified path.

```
vdmadmin -I -eventSyslog -enable -path path
```

Direct `Syslog` output of VMware Horizon 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

VMware Horizon 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 VMware Horizon 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 VMware Horizon 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.

Options

The following table shows the options that you can specify to assign a desktop to a user or to remove an assignment.

Table 13-9. 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 Console.
- 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 13-10. 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 an instant-clone virtual machine for disk space reclamation. VMware Horizon directs the ESXi host to reclaim disk space on the instant-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Console.

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.

Before using this option, see "Reclaim Disk Space on Instant Clones" in the *Setting Up Virtual Desktops in Horizon* document. This option is only applicable to non-vSAN datastores prior to vSphere 6.7 where space reclamation operation is performed by Horizon.

Options

Table 13-11. 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 VMware Horizon 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

VMware Horizon The following table shows the options that you can specify to configure domain filters.

Table 13-12. 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.
`–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 :
```

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 VMware Horizon 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 VMware Horizon 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.

VMware Horizon 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, VMware Horizon 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. VMware Horizon 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 13-13. Types of Domain List

Domain List Type	Description
Search exclusion list	Specifies the domains that VMware Horizon 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 VMware Horizon excludes from the results of a domain search. You cannot exclude the primary domain.
Inclusion list	Specifies the domains that VMware Horizon 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. VMware Horizon 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

VMware Horizon 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, VMware Horizon 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 VMware Horizon 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
```

VMware Horizon 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 exclusion list to specify the domains that VMware Horizon 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 :
```

VMware Horizon 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 VMware Horizon 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 13-14. Options for Displaying the Machines and Policies of Unentitled Users

Option	Description
`-ld`	Orders output entries by machine.
`-lu`	Orders output entries by user.

Table 13-14. Options for Displaying the Machines and Policies of Unentitled Users (continued)

Option	Description
`-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 13-15. XSL Stylesheets 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 13-15. 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, VMware Horizon 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, VMware Horizon 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, VMware Horizon 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 13-16. 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.
`-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.

Table 13-16. Options for Configuring Clients in Kiosk Mode (continued)

Option	Description
–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. VMware Horizon 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 Using the -S Option

You can use the `vdmadmin` command with the `–S` option to remove the entry for a Connection Server instance from the VMware Horizon configuration.

Syntax

```
vdmadmin –S [–b authentication_arguments] –r –s server
```

Usage Notes

To ensure high availability, VMware Horizon 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 VMware Horizon configuration.

To make the removal permanent, perform these tasks:

1 Uninstall the Connection Server instance 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 If the Connection Server is part of a CPA federation then, remove the Adam Instance VMwareVDMDSG program from the Windows Server computer by running the Add or Remove Programs tool.

4 On another Connection Server instance, use the `vdmadmin` command to remove the entry for the uninstalled Connection Server instance from the configuration.

If you want to reinstall VMware Horizon on the removed systems without replicating the VMware Horizon 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.

Note If you remove the Connection Server instance with the `vdmadmin –S` command without a clean uninstallation of LDAP instances on the server as described above, then you might accidentally remove the schema master node, which blocks future upgrades and installations of Connection Servers.

Options

The `–s` option specifies the NetBIOS name of the Connection Server instance 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 Console. 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 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 13-17. 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 VMware Horizon.

- 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.
- 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 13-18. 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]
vdmadmin -X [-b authentication_arguments] -seizeSchemaMaster
vdmadmin -X [-b authentication_arguments] -seizeSchemaMaster [-global]
```

Usage Notes

Duplicate LDAP entries on two or more Connection Server instances can cause problems with the integrity of LDAP data in VMware Horizon. This condition can occur during an upgrade, while LDAP replication is inoperative. Although VMware Horizon 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 VMware Horizon 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 13-19. 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 13-20. 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.

Table 13-20. Options for Detecting and Resolving LDAP Schema Collisions (continued)

Option	Description
–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.

The following table shows the options that you can specify to resolve LDAP schema master issues.

Table 13-21. Options for Resolving LDAP Schema Master Issues

Option	Description
–seizeSchemaMaster	Makes the current node the schema master node on the cluster.
–global	The schema role is seized on the global Horizon LDAP instance in a Cloud Pod Architecture environment. If you do not specify this option, the schema role is seized on the local Horizon 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
```

Make the current node the schema master node on the cluster for a local LDAP instance.

```
vdmadmin –X –seizeSchemaMaster
```

Make the current node the schema master node on the cluster for a global LDAP instance in a Cloud Pod Architecture environment.

```
vdmadmin –X –seizeSchemaMaster –global
```

Integrating VMware Horizon with the Event Database

14

You can configure VMware Horizon to record events to a Microsoft SQL Server, Oracle, or PostgreSQL database. VMware Horizon records events such as end-user actions, administrator actions, alerts that report system failures and errors, and statistical sampling.

End-user actions include logging and starting desktop and application sessions. Administrator actions include adding entitlements and creating desktop and application pools. An example of statistical sampling is recording the maximum number of users over a 24-hour period.

You can use business intelligence reporting engines such as Crystal Reports, IBM Cognos, MicroStrategy 9, and Oracle Enterprise Performance Management System to access and analyze the event database.

This chapter includes the following topics:

Event Database Tables and Schemas

VMware Horizon uses database tables to implement the event database. The event database prepends the names of these tables with a prefix that you define when you set up the database.

Event Database Tables

The following table shows the database tables that implement the event database in VMware Horizon.

Table 14-1. Event Database Tables

Table Name	Description
event	Metadata and search optimization data for recent events.
event_data	Data values for recent events.
event_data_historical	Data values for all events.
event_historical	Metadata and search optimization data for all events.

VMware Horizon records details about events to all the database tables. After a certain period of time has elapsed since writing an event record, VMware Horizon deletes the record from the event and event_data tables. You can use Horizon Console to configure the time period for which the database keeps a record in the event and event_data tables.

Important VMware Horizon does not restrict the growth of the event_historical and event_data_historical tables. You must implement a space management policy for these tables.

A unique primary key, EventID, identifies each event that VMware Horizon records in the event and event_historical tables. VMware Horizon records data values for each event in the event_data and event_data_historical tables. You can obtain the complete set of information for an event by joining the event and event_data tables or the event_ historical and event_data_historical tables on the EventID column.

The EventType, Severity, and Time columns in the event and event_historical tables identify the type and severity of an event and the time at which it occurred.

For information about setting up the event database, see the *Horizon Installation* document.

Note To purge data from the historical tables, see http://kb.vmware.com/kb/2150309.

Event Database Schemas

The following table shows the schema for the event and event_historical database tables.

Table 14-2. Schema for the event and event_historical Tables

Column Name	Oracle Data Type	SQL Server Data Type	PostgreSQL Data Type	Description
Acknowledged	SMALLINT	tinyint	integer	Whether VMware Horizon acknowledged the event. ■ 0 = false ■ 1 = true
Applicationid	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the associated application.
DesktopId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Desktop ID of the associated pool.
EndpointId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the associated endpoint.

Table 14-2. Schema for the event and event_historical Tables (continued)

Column Name	Oracle Data Type	SQL Server Data Type	PostgreSQL Data Type	Description
EventID	INTEGER	int	integer	Unique primary key for the event.
EventType	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Event name that corresponds to an item in the message catalog. For example, BROKER_USERLOGGEDIN.
FolderPath	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Full path of the folder that contains the associated object.
GroupId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	SID of the associated group in Active Directory.
LUNId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the LUN that stores the associated object.
MachineId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the associated physical or virtual machine.
Module	NVARCHAR2(512)	nvarchar(512)	character varying(512)	VMware Horizon component that raised the event. For example, Admin, Broker, Tunnel, Framework, Client, or Agent.
ModuleAndEventText	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Event message with values substituted for attribute parameters.
Node	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Name of the virtual device node.
SessionId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the associated session.
Severity	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Severity level. For example, INFO, WARNING, ERROR, AUDIT_SUCCESS, AUDIT_FAIL.
Source	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Identifier for the source of the event.
ThinappId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the associated ThinApp object.
Time	TIMESTAMP	datetime	timestamp without time zone	Time at which the event occurred, measured from the epoch (January 1, 1970).
UserDiskPathId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	ID of the user disk.
UserSID	NVARCHAR2(512)	nvarchar(512)	character varying(512)	SID of the associated user in Active Directory.

The following table shows the schema for the event_data and event_data_historical database tables.

Table 14-3. Schema for the event_data and event_data_historical Tables

Column Name	Oracle Data Type	SQL Server Data Type	PostgreSQL Data Type	Description
BooleanValue	SMALLINT	tinyint	integer	Value of a Boolean attribute. ■ 0 = false ■ 1 = true
EventID	INTEGER	int	integer	Unique primary key for the event.
IntValue	INTEGER	int	integer	Value of an integer attribute.
Name	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Attribute name (for example, UserDisplayName).
StrBlobValue	NCLOB	nvarchar(max)	text	Value of a string attribute over 500 characters.
StrValue	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Value of a string attribute. For other types of attributes, this column contains an interpretation of the data type as a string.
TimeValue	TIMESTAMP	datetime	timestamp without time zone	Value of a date and time attribute.
Type	SMALLINT	tinyint	integer	The data type of the attribute. ■ 0 = StrValue ■ 1 = IntValue ■ 2 = TimeValue ■ 3 = BooleanValue ■ 4 = StrBlobValue

The following table shows the schema for the timing_profiler database table.

Table 14-4. Schema for the timing_profiler Table

Column Name	Oracle Data Type	SQL Server Data Type	PostgreSQL Data Type	Description
EventId	NUMBER	int	integer	Unique primary key for the event.
EventType	NVARCHAR2(512)	nvarchar(512)	character varying	Type of the Timing Profiler event. For example: TIMING_PROFILER_DESKTOP_RECONNECT.
Properties	NCLOB	nvarchar(max)	text	JSON containing various attributes associated with this timing profiler event.
SessionId	NVARCHAR2(512)	nvarchar(512)	character varying	Session associated with this event.

Table 14-4. Schema for the timing_profiler Table (continued)

Column Name	Oracle Data Type	SQL Server Data Type	PostgreSQL Data Type	Description
Time	TIMESTAMP	datetime	timestamp without time zone	Time at which the event occurred, measured from the epoch (January 1, 1970).
TimingProfilerTree	NCLOB	nvarchar(max)	text	Logon timing profiler tree.
UserSid	NVARCHAR2(512)	nvarchar(512)	character varying	User involved in this event.

Horizon Connection Server Events

Horizon Connection Server events report Connection Server-related information, such as desktop and application sessions, user authentication failures, and provisioning errors.

The BROKER_DAILY_MAX_DESKTOP_SESSIONS event reports the maximum number of concurrent desktop sessions over a 24-hour period. If a user runs multiple desktop sessions concurrently, each desktop session is counted separately.

The BROKER_DAILY_MAX_APP_USERS event reports the maximum number of concurrent application users over a 24-hour period. If a user runs multiple applications concurrently, the user is counted only once. Short-lived sessions might not be included in the count because the sampling is performed every five minutes.

The BROKER_VC_DISABLED and BROKER_VC_ENABLED events report the state of the vCenter driver that VMware Horizon uses to track a vCenter Server instance.

The BROKER_VC_STATUS_* events report the state of a vCenter Server instance.

The following table lists all the event types for Connection Server.

Table 14-5. Connection Server Events

Event Type	Severity	ModuleAndEventText
BROKER_AGENT_OFFLINE	WARNING	The agent running on machine ${MachineName} has not responded to queries, marking it as offline
BROKER_AGENT_ONLINE	WARNING	The agent running on machine ${MachineName} is responding again, but did not send a startup message
BROKER_APPLICATION_LAUNCH_FAILURE	ERROR	Unable to launch from Pool ${PoolId} for user ${UserDisplayName}: The broker encountered an error while processing the request, please contact support for assistance
BROKER_APPLICATION_MISSING	WARNING	At least ${ApplicationMissingCount} applications, including ${ApplicationExecutable}, are not installed on ${MachineName} in Pool ${PoolId}

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_APPLICATION_NOT_ENTITLED	AUDIT_FAIL	Unable to launch from Pool ${PoolId} for user ${UserDisplayName}: User is not entitled to this Pool
BROKER_APPLICATION_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Unable to launch from Pool ${PoolId} for user ${UserDisplayName}: Requested protocol ${ProtocolId} is not supported
BROKER_APPLICATION_REQUEST	INFO	User ${UserDisplayName} requested Application ${Application Id}
BROKER_APPLICATION_SESSION_REQUEST	INFO	User ${UserDisplayName} requested an application session from Pool ${PoolId}
BROKER_DAILY_MAX_DESKTOP_SESSIONS	INFO	${Time}: Over the past 24 hours, the maximum number of concurrent desktop sessions was ${UserCount}
BROKER_DAILY_MAX_APP_USERS	INFO	${Time}: Over the past 24 hours, the maximum number of users with concurrent application sessions was ${UserCount}
BROKER_DESKTOP_LAUNCH_FAILURE	ERROR	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: The broker encountered an error while processing the request, please contact support for assistance
BROKER_DESKTOP_NOT_ENTITLED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: User is not entitled to this Pool
BROKER_DESKTOP_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Requested protocol ${ProtocolId} is not supported
BROKER_DESKTOP_REQUEST	INFO	User ${UserDisplayName} requested Pool ${DesktopId}
BROKER_EVENT_HANDLING_STARTED	INFO	Broker ${BrokerName} has started handling events
BROKER_EVENT_HANDLING_STOPPED	INFO	${BrokerName} has stopped handling events
BROKER_MACHINE_ALLOCATED	INFO	User ${UserDisplayName} requested Pool ${DesktopId}, allocated machine ${MachineName}
BROKER_MACHINE_ASSIGNED_UNAVAILABLE	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Assigned machine ${MachineName} is unavailable
BROKER_MACHINE_CANNOT_CONNECT	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Failed to connect to Machine ${MachineName} using ${ProtocolId}
BROKER_MACHINE_CONFIGURED_VIDEO_SETTINGS	INFO	Successfully configured video settings for Machine VM ${MachineName} in Pool ${DesktopId}

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_MACHINE_NOT_READY	WARNING	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Machine ${MachineName} is not ready to accept connections
BROKER_MACHINE_OPERATION_DELETED	INFO	machine ${MachineName} has been deleted
BROKER_MACHINE_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Machine ${MachineName} does not support protocol ${ProtocolId}
BROKER_MACHINE_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Machine ${MachineName} did not report protocol ${ProtocolId} as ready
BROKER_MACHINE_REJECTED_SESSION	WARNING	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Machine ${MachineName} rejected the start session request
BROKER_MACHINE_SESSION_TIMEDOUT	WARNING	Session for user ${UserDisplayName} timed out
BROKER_MULTIPLE_DESKTOPS_FOR_KIOSK_USER	WARNING	User ${UserDisplayName} is entitled to multiple desktop pools
BROKER_POOL_CANNOT_ASSIGN	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: There are no machines available to assign the user to
BROKER_POOL_COMANAGER_REQUIRED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: No co-management availability for protocol ${ProtocolId}
BROKER_POOL_EMPTY	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: The Desktop Pool is empty
BROKER_POOL_NO_MACHINE_ASSIGNED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: No machine assigned to this user
BROKER_POOL_NO_RESPONSES	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: No machines in the Desktop Pool are responsive
BROKER_POOL_OVERLOADED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: All responding machines are currently in use
BROKER_POOL_POLICY_VIOLATION	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: This Desktop Pool does not allow online sessions
BROKER_POOL_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: There were no machines available that support protocol ${ProtocolId}

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_POOL_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: There were no machines available that reported protocol ${ProtocolId} as ready
BROKER_POOL_TUNNEL_NOT_SUPPORTED	AUDIT_FAIL	Unable to launch from Pool ${DesktopId} for user ${UserDisplayName}: Tunnelling is not supported for protocol ${ProtocolId}
BROKER_PROVISIONING_ERROR_CONFIG_CLEARED	INFO	The previously reported configuration problem is no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_CONFIG_SET	ERROR	Provisioning error occurred on Pool ${DesktopId} because of a configuration problem
BROKER_PROVISIONING_ERROR_DISK_CLEARED	INFO	The previously reported disk problem is no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_DISK_SET	WARNING	Provisioning error occurred on Pool ${DesktopId} because of a disk problem
BROKER_PROVISIONING_ERROR_LICENCE_CLEARED	INFO	The previously reported licensing problem is no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_LICENCE_SET	ERROR	Provisioning error occurred on Pool ${DesktopId} because of a licensing problem
BROKER_PROVISIONING_ERROR_NETWORKING_CLEARED	INFO	The previously reported networking problems with Horizon Agent are no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_NETWORKING_SET	ERROR	Provisioning error occurred on Pool ${DesktopId} because of a networking problem with Horizon Agent
BROKER_PROVISIONING_ERROR_RESOURCE_CLEARED	INFO	The previously reported resource problem is no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_RESOURCE_SET	ERROR	Provisioning error occurred on Pool ${DesktopId} because of a resource problem
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_CLEARED	INFO	The previously reported timeout while customizing is no longer present on Pool ${DesktopId}
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_SET	ERROR	Provisioning error occurred on Pool ${DesktopId} because of a timeout while customizing
BROKER_PROVISIONING_ERROR_VM_CLONING	ERROR	Provisioning error occurred for Machine ${MachineName}: Cloning failed for Machine
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_ERROR	ERROR	Provisioning error occurred for Machine ${MachineName}: Customization failed for Machine
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_NETWORKING	ERROR	Provisioning error occurred for Machine ${MachineName}: Customization error due to no network communication between Horizon Agent and Connection Server

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_TIMEOUT	ERROR	Provisioning error occurred for Machine ${MachineName}: Customization operation timed out
BROKER_PROVISIONING_SVI_ERROR_RECONFIG_FAILED	ERROR	Provisioning error occurred for Machine ${MachineName}: Reconfigure operation failed
BROKER_PROVISIONING_SVI_ERROR_REFIT_ FAILED	ERROR	Provisioning error occurred for Machine ${MachineName}: Refit operation ${SVIOperation} failed
BROKER_PROVISIONING_SVI_ERROR_ REMOVING_VM	ERROR	Provisioning error occurred for Machine ${MachineName}: Unable to remove Machine from inventory
BROKER_PROVISIONING_VERIFICATION_ FAILED_USER_ASSIGNED	WARNING	Provisioning verification failed for Machine ${MachineName}: User is already assigned to a machine in Pool ${DesktopId}
BROKER_PROVISIONING_VERIFICATION_ FAILED_USER_CANNOT_BE_ASSIGNED	WARNING	Provisioning verification failed for Machine ${MachineName}: A user cannot be assigned because Pool ${DesktopId} is not persistent
BROKER_PROVISIONING_VERIFICATION_ FAILED_VMNAME_IN_USE	WARNING	Provisioning verification failed for Machine ${MachineName}: A machine already exists in Pool ${DesktopId} with name ${MachineName}
BROKER_SVI_ARCHIVE_UDD_FAILED	AUDIT_FAIL	Failed to archive user data disk ${UserDiskName} to location ${SVIPath}
BROKER_SVI_ARCHIVE_UDD_SUCCEEDED	AUDIT_SUCCESS	Archived user data disk ${UserDiskName} to location ${SVIPath}
BROKER_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Failed to attach user data disk ${UserDiskName} to VM ${SVIVMID}
BROKER_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Attached user data disk ${UserDiskName} to VM ${SVIVMID}
BROKER_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Failed to detach user data disk ${UserDiskName} from VM ${SVIVMID}
BROKER_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Detached user data disk ${UserDiskName} from VM ${SVIVMID}
BROKER_USER_AUTHFAILED_ACCOUNT_ DISABLED	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because the account is disabled
BROKER_USER_AUTHFAILED_ACCOUNT_ EXPIRED	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because the account has expired
BROKER_USER_AUTHFAILED_ACCOUNT_ LOCKED_OUT	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because the account is locked out
BROKER_USER_AUTHFAILED_ACCOUNT_ RESTRICTION	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because of an account restriction
BROKER_USER_AUTHFAILED_BAD_USER_ PASSWORD	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because of a bad username or password

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_USER_AUTHFAILED_GENERAL	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate
BROKER_USER_AUTHFAILED_NO_LOGON_ SERVERS	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because there are no logon servers
BROKER_USER_AUTHFAILED_PASSWORD_ EXPIRED	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because the password has expired
BROKER_USER_AUTHFAILED_PASSWORD_ MUST_CHANGE	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because the password must change
BROKER_USER_AUTHFAILED_SECUREID_ ACCESS_DENIED	AUDIT_FAIL	SecurID access denied for user ${UserDisplayName}
BROKER_USER_AUTHFAILED_SECUREID_ NEWPIN_REJECTED	AUDIT_FAIL	SecurID access denied for user ${UserDisplayName} because new pin was rejected
BROKER_USER_AUTHFAILED_SECUREID_ WRONG_NEXTTOKEN	AUDIT_FAIL	SecurID access denied for user ${UserDisplayName} because wrong next token entered
BROKER_USER_AUTHFAILED_SECUREID_ WRONG_STATE	AUDIT_FAIL	SecurID access denied for user ${UserDisplayName} because of incorrect state
BROKER_USER_AUTHFAILED_TIME_ RESTRICTION	AUDIT_FAIL	User ${UserDisplayName} failed to authenticate because of a time restriction
BROKER_USER_NOT_AUTHORIZED	AUDIT_FAIL	User ${UserDisplayName} has authenticated, but is not authorized to perform the operation
BROKER_USER_NOT_ENTITLED	AUDIT_FAIL	User ${UserDisplayName} has authenticated, but is not entitled to any Pools
BROKER_USERCHANGEDPASSWORD	AUDIT_SUCCESS	Password for ${UserDisplayName} has been changed by the user
BROKER_USERLOGGEDIN	AUDIT_SUCCESS	User ${UserDisplayName} has logged in
BROKER_USERLOGGEDOUT	AUDIT_SUCCESS	User ${UserDisplayName} has logged out
BROKER_VC_DISABLED	INFO	vCenter at address ${VCAddress} has been temporarily disabled
BROKER_VC_ENABLED	INFO	vCenter at address ${VCAddress} has been enabled
BROKER_VC_STATUS_CHANGED_CANNO T_ LOGIN	WARNING	Cannot log in to vCenter at address ${VCAddress}
BROKER_VC_STATUS_CHANGED_DOWN	INFO	vCenter at address ${VCAddress} is down
BROKER_VC_STATUS_CHANGED_INVALI D_ CREDENTIALS	WARNING	vCenter at address ${VCAddress} has invalid credentials
BROKER_VC_STATUS_CHANGED_NOT_Y ET_ CONNECTED	INFO	Not yet connected to vCenter at address ${VCAddress}
BROKER_VC_STATUS_CHANGED_ RECONNECTING	INFO	Reconnecting to vCenter at address ${VCAddress}

Table 14-5. Connection Server Events (continued)

Event Type	Severity	ModuleAndEventText
BROKER_VC_STATUS_CHANGED_UNKNOWN	WARNING	The status of vCenter at address ${VCAddress} is unknown
BROKER_VC_STATUS_CHANGED_UP	INFO	vCenter at address ${VCAddress} is up
BROKER_USER_LOCK_SSO		Indicates that the Connection Server's SSO credentials have been discarded due to timeout or screen lock. Event text: SSO credentials locked for user <domain name\user name>.
BROKER_LMV_REMOTE_POD_DESKTOP_LAUNCH		Indicates that a user's session was redirected to a remote pod for launching a desktop session, in a CPA environment. Event text: Remote pod <Pod name> has launched a desktop for user <User Name> from global entitlement <Global Entitlement Name>.

Horizon Agent Events

Horizon Agent events report Horizon Agent-related information, such as the users who have logged in to or disconnected from a specific machine, whether Horizon Agent has shut down on a specific machine, and whether Horizon Agent has sent a start up message from a specific machine to Horizon Connection Server.

Table 14-6. Horizon Agent Events

Event Type	Severity	ModuleAndEventText
AGENT_CONNECTED	INFO	User ${UserDisplayName} has logged in to a new session on machine ${MachineName}
AGENT_DISCONNECTED	INFO	User ${UserDisplayName} has disconnected from machine ${MachineName}
AGENT_ENDED	INFO	User ${UserDisplayName} has logged off machine ${MachineName}
AGENT_PENDING	INFO	The agent running on machine ${MachineName} has accepted an allocated session for user ${UserDisplayName}
AGENT_PENDING_ EXPIRED	WARNING	The pending session on machine ${MachineName} for user ${UserDisplayName} has expired
AGENT_RECONFIGURED	INFO	Machine ${MachineName} has been successfully reconfigured
AGENT_RECONNECTED	INFO	User ${UserDisplayName} has reconnected to machine ${MachineName}
AGENT_RESUME	INFO	The agent on machine ${MachineName} sent a resume message
AGENT_SHUTDOWN	INFO	The agent running on machine ${MachineName} has shut down, this machine will be unavailable

Table 14-6. Horizon Agent Events (continued)

Event Type	Severity	ModuleAndEventText
AGENT_STARTUP	INFO	The agent running on machine ${MachineName} has contacted the connection server and sent a startup message
AGENT_SUSPEND	INFO	The agent on machine ${MachineName} sent a suspend message

Horizon Console Events

Horizon Console events report information about actions that users initiate in Horizon Console.

Table 14-7. Horizon Console Events

EventType	Severity	ModuleAndEventText
ADMIN_ADD_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	${EntitlementDisplay} was entitled to Pool ${DesktopId} by ${UserDisplayName}
ADMIN_ADD_LICENSE	AUDIT_SUCCESS	${UserDisplayName} added license
ADMIN_ADD_LICENSE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add license
ADMIN_ADD_PM	AUDIT_SUCCESS	${UserDisplayName} added physical machine ${MachineName} to Pool ${DesktopId}
ADMIN_ADD_PM_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add physical machine ${MachineName} to Pool ${DesktopId}
ADMIN_ADMINSTRATOR_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove all permissions for Administrator ${AdminPermissionEntity}
ADMIN_ADMINSTRATOR_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed all permissions for Administrator ${AdminPermissionEntity}
ADMIN_CONNECTION_BROKER_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update connection broker ${BrokerId}
ADMIN_CONNECTION_BROKER_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated connection broker ${BrokerId}: (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_CONNECTION_SERVER_BACKUP_FAILED	AUDIT_FAIL	${UserDisplayName} failed to initiate a backup of connection broker ${BrokerId}
ADMIN_CONNECTION_SERVER_BACKUP_INITIATED	AUDIT_SUCCESS	${UserDisplayName} initiated a backup of connection broker ${BrokerId}

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_CONNECTION_SERVER_DISABLE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to disable connection broker ${BrokerId}
ADMIN_CONNECTION_SERVER_DISABLED	AUDIT_SUCCESS	${UserDisplayName} is disabling connection broker ${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to enable connection broker ${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLED	AUDIT_SUCCESS	${UserDisplayName} is enabling connection broker ${BrokerId}
ADMIN_DATABASE_CONFIGURATION_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add database configuration
ADMIN_DATABASE_CONFIGURATION_ ADDED	AUDIT_SUCCESS	${UserDisplayName} has added database configuration
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to delete database configuration
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_SUCCESS	${UserDisplayName} has deleted database configuration
ADMIN_DATABASE_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update database configuration
ADMIN_DATABASE_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} has updated database configuration
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN	AUDIT_SUCCESS	${UserDisplayName} assigned Pool ${DesktopId} for default desktop to ${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} failed to assign Pool ${DesktopId} for default desktop to ${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN	AUDIT_SUCCESS	${UserDisplayName} removed pool assignment for default desktop to ${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove Pool assignment for default desktop to ${UserName}
ADMIN_DESKTOP_ADDED	AUDIT_SUCCESS	${UserDisplayName} added Pool ${DesktopId}
ADMIN_DESKTOP_ASSIGN	AUDIT_SUCCESS	${UserDisplayName} assigned Desktop ${MachineName} to ${UserName}
ADMIN_DESKTOP_ASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} failed to assign Desktop ${MachineName} to ${UserName}
ADMIN_DESKTOP_EDITED	AUDIT_SUCCESS	${UserDisplayName} edited Pool ${DesktopId} (${AttrChangeType}: ${AttrName} = ${AttrValue})

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update desktop ${MachineName} to ${MaintenanceMode} maintenance mode
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated desktop ${MachineName} to ${MaintenanceMode} maintenance mode
ADMIN_DESKTOP_UNASSIGN	AUDIT_SUCCESS	${UserDisplayName} removed assignment for Desktop ${MachineName}
ADMIN_DESKTOP_UNASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove assignment for Desktop ${MachineName}
ADMIN_ENABLE_DESKTOP_FAILED	AUDIT_FAIL	${UserDisplayName} failed to set Pool ${DesktopId} to ${EnableStatus}
ADMIN_ENABLE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} set Pool ${DesktopId} to ${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_FAILED	AUDIT_FAIL	${UserDisplayName} failed to set provisioning for Pool ${DesktopId} to ${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} set provisioning for Pool ${DesktopId} to ${EnableStatus}
ADMIN_EVENT_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update event configuration
ADMIN_EVENT_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} has updated global configuration
ADMIN_FOLDER_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add folder ${AdminFolderName}
ADMIN_FOLDER_ADDED	AUDIT_SUCCESS	${UserDisplayName} added folder ${AdminFolderName}
ADMIN_FOLDER_CHANGE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to change object ${ObjectID}(type=${ObjectType}) to folder ${AdminFolderName}
ADMIN_FOLDER_CHANGED	AUDIT_SUCCESS	${UserDisplayName} changed object ${ObjectID}(type=${ObjectType}) to folder ${AdminFolderName}
ADMIN_FOLDER_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to delete folder ${AdminFolderName}
ADMIN_FOLDER_DELETED	AUDIT_SUCCESS	${UserDisplayName} deleted folder ${AdminFolderName}

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_GLOBAL_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update global configuration
ADMIN_GLOBAL_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated global configuration (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_GLOBAL_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update global policies
ADMIN_GLOBAL_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated global policy (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_PERFMON_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update performance monitoring configuration
ADMIN_PERFMON_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} has updated performance monitoring configuration
ADMIN_PERMISSION_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add Permission to ${AdminPermissionEntity} with Role ${AdminRoleName} on Folder ${AdminFolderName}
ADMIN_PERMISSION_ADDED	AUDIT_SUCCESS	${UserDisplayName} added Permission to ${AdminPermissionEntity} with Role ${AdminRoleName} on Folder ${AdminFolderName}
ADMIN_PERMISSION_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove Permission to ${AdminPermissionEntity} with Role ${AdminRoleName} on Folder ${AdminFolderName}
ADMIN_PERMISSION_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed Permission to ${AdminPermissionEntity} with Role ${AdminRoleName} on Folder ${AdminFolderName}
ADMIN_POOL_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update Pool ${DesktopId} policies
ADMIN_POOL_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated Pool ${DesktopId} policy (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_REMOVE_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	${EntitlementDisplay} was unentitled from Pool ${DesktopId} by ${UserDisplayName}

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_REMOVE_DESKTOP_FAILED	AUDIT_FAIL	${UserDisplayName} failed to removed Pool ${DesktopId}
ADMIN_REMOVE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} removed Pool ${DesktopId}
ADMIN_ROLE_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add Role ${AdminRoleName} with privileges ${AdminPrivilegeName}
ADMIN_ROLE_ADDED	AUDIT_SUCCESS	${UserDisplayName} added Role ${AdminRoleName} with privileges ${AdminPrivilegeName}
ADMIN_ROLE_PRIV_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update Role ${AdminRoleName} to privileges ${AdminPrivilegeName}
ADMIN_ROLE_PRIV_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated Role ${AdminRoleName} to privileges ${AdminPrivilegeName}
ADMIN_ROLE_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove Role ${AdminRoleName}
ADMIN_ROLE_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed Role ${AdminRoleName}
ADMIN_ROLE_RENAME_FAILED	AUDIT_FAIL	${UserDisplayName} failed to rename Role ${AdminRoleName} to ${AdminRoleNewName}
ADMIN_ROLE_RENAMED	AUDIT_SUCCESS	${UserDisplayName} renamed Role ${AdminRoleName} to ${AdminRoleNewName}
ADMIN_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add security server ${SecurityServerId}
ADMIN_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	${UserDisplayName} added security server ${SecurityServerId}
ADMIN_SECURITY_SERVER_EDIT_FAILED	AUDIT_FAIL	${UserDisplayName} failed to edit security server ${SecurityServerId}
ADMIN_SECURITY_SERVER_EDITED	AUDIT_SUCCESS	${UserDisplayName} edited security server ${SecurityServerId} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_SECURITY_SERVER_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove security server ${SecurityServerId}
ADMIN_SECURITY_SERVER_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed security server ${SecurityServerId}

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_SESSION_SENDMSG	AUDIT_SUCCESS	${UserDisplayName} sent message (${SessionMessage}) to session (User ${UserName}, Desktop ${MachineName})
ADMIN_SESSION_SENDMSG_FAILED	AUDIT_FAIL	${UserDisplayName} failed to send message (${SessionMessage}) to session ${ObjectId}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Failed to add deployment group for ${SVIParentVM} : ${SVISnapshot}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Added deployment group ${SVIDeploymentGroupID} for ${SVIParentVM} : ${SVISnapshot}
ADMIN_SVI_ADD_UDD_FAILED	AUDIT_FAIL	Failed to add user data disk ${UserDiskName}
ADMIN_SVI_ADD_UDD_SUCCEEDED	AUDIT_SUCCESS	Added user data disk ${UserDiskName}
ADMIN_SVI_ADMIN_ADDED	AUDIT_SUCCESS	${UserDisplayName} added SVI QuickPrep domain ${SVIAdminFqdn} (${SVIAdminName})
ADMIN_SVI_ADMIN_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed SVI QuickPrep domain (id=${SVIAdminID})
ADMIN_SVI_ADMIN_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated SVI QuickPrep domain ${SVIAdminFqdn} (${SVIAdminName})
ADMIN_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Failed to request attach user data disk ${UserDiskName} to VM ${SVIVMID}
ADMIN_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Requested attach user data disk ${UserDiskName} to VM ${SVIVMID}
ADMIN_SVI_DELETE_UDD_FAILED	AUDIT_FAIL	Failed to delete user data disk ${UserDiskName}
ADMIN_SVI_DELETE_UDD_SUCCEEDED	AUDIT_SUCCESS	Deleted user data disk ${UserDiskName}
ADMIN_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Failed to request detach user data disk ${UserDiskName} from VM ${SVIVMID}
ADMIN_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Requested detach user data disk ${UserDiskName} from VM ${SVIVMID}
ADMIN_SVI_REBALANCE_VM_FAILED	AUDIT_FAIL	Failed to rebalance VM ${SVIVMID}
ADMIN_SVI_REBALANCE_VM_SUCCEEDED	AUDIT_SUCCESS	Rebalanced VM ${SVIVMID}

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_SVI_REFRESH_VM_FAILED	AUDIT_FAIL	Failed to refresh VM ${SVIVMID}
ADMIN_SVI_REFRESH_VM_SUCCEEDED	AUDIT_SUCCESS	Refreshed VM ${SVIVMID}
ADMIN_SVI_RESYNC_VM_FAILED	AUDIT_FAIL	Failed to resync VM ${SVIVMID} to deployment group ${SVIDeploymentGroupID}
ADMIN_SVI_RESYNC_VM_SUCCEEDED	AUDIT_SUCCESS	Resyncd VM ${SVIVMID} to deployment group ${SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Failed to update pool ${DesktopId} to deployment group ${SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Updated pool ${DesktopId} to deployment group ${SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_UDD_FAILED	AUDIT_FAIL	Failed to update user data disk ${UserDiskName}
ADMIN_SVI_UPDATE_UDD_SUCCEEDED	AUDIT_SUCCESS	Set user data disk ${UserDiskName} pool to ${DesktopId} and user to ${UserName}
ADMIN_UNREGISTER_PM	AUDIT_SUCCESS	${UserDisplayName} unregistered physical machine ${MachineName})
ADMIN_UNREGISTER_PM_FAILED	AUDIT_FAIL	${UserDisplayName} fails to unregister physical machine ${MachineName})
ADMIN_USER_INFO_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update user info with AD server for ${UserName}
ADMIN_USER_INFO_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated user info with AD server for ${UserName}
ADMIN_USER_POLICY_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to delete Pool ${DesktopId} override policies for user ${UserName}
ADMIN_USER_POLICY_DELETED	AUDIT_SUCCESS	${UserDisplayName} deleted Pool ${DesktopId} override policy for user ${UserName} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_USER_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to update Pool ${DesktopId} policies for user ${UserName}
ADMIN_USER_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} updated Pool ${DesktopId} policy for user ${UserName} (${AttrChangeType}: ${AttrName} = ${AttrValue})

Table 14-7. Horizon Console Events (continued)

EventType	Severity	ModuleAndEventText
ADMIN_USERLOGGEDIN	AUDIT_SUCCESS	User ${UserDisplayName} has logged in to Horizon Console
ADMIN_USERLOGGEDOUT	AUDIT_SUCCESS	User ${UserDisplayName} has logged out from Horizon Console
ADMIN_VC_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} failed to add VC server ${VCAddress}
ADMIN_VC_ADDED	AUDIT_SUCCESS	${UserDisplayName} added VC server ${VCAddress}
ADMIN_VC_EDITED	AUDIT_SUCCESS	${UserDisplayName} edited VC server ${VCAddress} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_VC_LICINV_ALARM_DISABLED	AUDIT_SUCCESS	Alarm on VC server ${VCAddress} for License Inventory monitoring was disabled as all Hosts have desktop licenses
ADMIN_VC_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} failed to remove VC server ${VCAddress}
ADMIN_VC_REMOVED	AUDIT_SUCCESS	${UserDisplayName} removed VC server ${VCAddress}

Event Message Attributes

ModuleAndEventText messages use certain attributes. To determine the data type for an attribute, you can examine its value in the type column in the event_data or event_data_historical table.

Table 14-8. Attributes that ModuleAndEventText Messages Use

Attribute Name	Description
AdminFolderName	Name of a folder that requires privileged access.
AdminPermissionEntity	Name of an object that requires privileged access.
AdminPrivilegeName	Name of an administrative privilege.
AdminRoleName	Name of an administrative role.
AdminRoleNewName	New name of an administrative role.
AttrChangeType	Type of change that was applied to a generic attribute.
AttrName	Name of a generic attribute.
AttrValue	Value of a generic attribute.
BrokerId	Identifier of a Connection Server instance.

Table 14-8. Attributes that ModuleAndEventText Messages Use (continued)

Attribute Name	Description
BrokerName	Name of a Connection Server instance.
DesktopDisplayName	Display name of a desktop pool.
DesktopId	Identifier of a desktop pool.
EntitlementDisplay	Display name of a desktop entitlement.
MachineId	Name of a physical or virtual machine.
MachineName	Name of a physical or virtual machine.
MaintenanceMode	Maintenance mode state.
ObjectID	Identifier of an inventory object.
ObjectType	Type of an inventory object.
PolicyDisplayName	Display name of a policy.
PolicyObject	Identifier of a policy object.
PolicyValue	Value of a policy object.
ProtocolId	Identifier of a display protocol.
SecurityServerId	Identifier of a security server.
SVIAdminFqdn	FQDN of a QuickPrep domain.
SVIAdminID	Identifier of a QuickPrep domain.
SVIAdminName	Name of a QuickPrep domain.
Time	Date and time value.
UserCount	Maximum number of desktop users over a 24-hour period.
UserDiskName	Name of a user data disk.
UserDisplayName	User name in the form DOMAIN\username.
UserName	Name of a user in Active Directory.
VCAddress	URL of a vCenter Server.

Sample Database Queries and Views

You can query the event_historical database to display error events, warning events, and specific recent events.

Note Replace the dbo.VE_ prefix in the following examples with the appropriate prefix for your event database.

List Error Events

The following query displays all error events from the event_historical table.

```
CREATE VIEW error_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
        FROM dbo.VE_event_historical AS ev
        WHERE ev.Severity = ‘ERROR’
    );
```

List Warning Events

The following query displays all warning events from the event_historical table.

```
CREATE VIEW warning_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
        FROM dbo.VE_event_historical AS ev
        WHERE ev.Severity = ‘WARNING’
    );
```

List Recent Events

The following query lists all recent events that are associated with the user fred in the domain MYDOM.

```
CREATE VIEW user_fred_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.Severity, ev.Acknowledged
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed
        WHERE ev.EventID = ed.EventID AND ed.Name = 'UserDisplayName' AND ed.StrValue =
            ‘MYDOM\fred’
    );
```

The following query lists all recent events where the agent on a machine shut down.

```
CREATE VIEW agent_shutdown_events AS
    (
    SELECT ev.EventID, ev.Time, ed.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed
```

```
        WHERE ev.EventID = ed.EventID AND ev.EventType = 'AGENT_SHUTDOWN' AND
            ed.Name = 'MachineName'
    );
```

The following query lists all recent events where a desktop failed to launch because the desktop pool was empty.

```
CREATE VIEW desktop_launch_failure_events AS
    (
    SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed1,
            dbo.VE_event_data_historical AS ed2
        WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
            ev.EventType = 'BROKER_POOL_EMPTY' AND
            ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
    );
```

The following query lists all recent events where an administrator removed a desktop pool.

```
CREATE VIEW desktop_pool_removed_events AS
    (
    SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed1,
            dbo.VE_event_data_historical AS ed2
        WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
            ev.EventType = 'ADMIN_DESKTOP_REMOVED' AND
            ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
);
```

Customizing LDAP Data

15

You can use VMware and Microsoft command-line tools to import and export LDAP configuration data to and from VMware Horizon. These command-line tools import and export LDAP configuration data in LDAP Data Interchange Format (LDIF) configuration files.

This feature is intended for use by advanced administrators who want to perform automatic bulk configuration operations. To create scripts to update the VMware Horizon configuration, use Horizon PowerCLI Module.

This chapter includes the following topics:

Introduction to LDAP Configuration Data

All VMware Horizonconfiguration data is stored in an LDAP directory. Each Horizon Connection Server standard or replica instance contains a local LDAP configuration repository and a replication agreement between each of the Connection Server instances. This arrangement ensures that changes to one repository are automatically replicated to all other repositories.

When you use Horizon Console to modify the VMware Horizon configuration, the appropriate LDAP data is updated in the repository. For example, if you add a desktop pool, VMware Horizon stores information about users, user groups, and entitlements in LDAP. Connection Server instances manage other LDAP configuration data automatically, and they use the information in the repository to control VMware Horizon operations.

You can use LDIF configuration files to perform a number of tasks, including transferring configuration data between Connection Server instances and backing up your VMware Horizon configuration so that you can restore the state of a Connection Server instance.

You can also use LDIF configuration files to define a large number of VMware Horizon objects, such as desktop pools, and add those objects to your Connection Server instances without having to use Horizon Console to perform the task manually.

VMware Horizon performs regular backups of the LDAP repository.

LDAP configuration data is transferred as plain ASCII text and conforms to the Internet Engineering Task Force (IETF) RFC 2849 standard.

Modifying LDAP Configuration Data

You can export LDAP configuration data on a Horizon Connection Server instance to an LDIF configuration file, modify the LDIF configuration file, and import the modified LDIF configuration file into other Connection Server instances to perform automatic bulk configuration operations.

You can obtain examples of LDIF syntax for any item of LDAP configuration data in Horizon by examining the contents of an exported LDIF configuration file. For example, you can extract the data for a desktop pool and use that data as a template to create a large number of desktop pools.

Export LDAP Configuration Data

You can use the `vdmexport` command-line utility to export configuration data from a standard or replica Connection Server instance to an LDIF configuration file.

Procedure

1. Log in to a standard or replica Connection Server instance as a user in the Administrators or Administrators (Read only) role.

   You must be logged in as a user in the Administrators or Administrators (Read only) role to export configuration data from the Horizon configuration repository.

2. At the command prompt, type the `vdmexport` command.

   By default, the `vdmexport` command-line utility is installed in the `C:\Program Files\VMware\VMware View\Server\tools\bin` directory.

   The `vdmexport` command has the following options.

Option	Description
-f	Output file name for LDAP backup.
-v	The output file is verbatim (not encrypted).
-c	Similar to the –v option, but sensitive attribute values are not included in the output file.
-k	Outputs only kiosk client entries and related FSPs.
-g	Take a backup of the Cloud Pod Architecture global LDAP, rather than of local LDAP.

   For example, the following command exports a local LDIF configuration file.

```
vdmexport –f mylocalexport.LDF
```

The following command takes a backup of the Cloud Pod Architecture global LDAP.

```
vdmexport –f myglobalexport.LDF –g
```

Results

The `vdmexport` command writes the configuration of your Connection Server instance to the file that you specify. The command displays errors if your role has insufficient privileges to view the data in the configuration repository.

Defining a Desktop Pool in an LDIF Configuration File

You can define a desktop pool in an LDIF configuration file and import the customized LDIF configuration file to create a large number of desktop pools.

Note You can also create customized LDIF configuration files for other objects that are defined in the LDAP repository, including global configuration settings, configuration settings for a specific Horizon Connection Server instance or security server, and configuration settings for a specific user.

To define a desktop pool in an LDIF configuration file, you must add the following entries to the file.

- A Virtual Desktop VM entry for each virtual desktop in the desktop pool
- A VM Pool entry for each desktop pool
- A Desktop Application entry that defines the entitlement of the desktop pool

You associate each VM Pool entry with one Desktop Application entry in a one-to-one relationship. A Desktop Application entry cannot be shared between VM Pool entries, and a VM Pool entry can only be associated with one Desktop Application entry.

The following table describes the attributes you must specify when you modify a desktop pool definition in an LDIF configuration file.

Table 15-1. Important Attributes for Defining a Desktop Pool

Entry	Attribute	Description
Virtual Desktop VM VM Pool Desktop Application	cn	Common name of an entry. If you require names to be generated automatically, specify globally unique identifier (GUID) strings. You can use any reliable GUID generator, such as the mechanism provided by .NET (for example, by calling System.Guid.NewGuid().ToString() in Visual Basic).
Desktop Application	member	A list of Active Directory (AD) users and groups who are entitled to access the desktop pool. The attribute is specified in the form of a Windows Security Identifier (SID) reference. A member value of <SID=S-1-2-3-4> represents an AD user or group with the SID value S-1-2-3-4. In LDIF format, the left angle (<) character is reserved, so you must place two colons (::) after the attribute name and specify the SID value in base 64 format (for example, PFNJRD1TLTEtMi0zLTQ+IA==). Because this attribute is multivalued, you can use it on multiple lines to represent each entry in a list of SIDs.

Sample LDIF Configuration File Desktop Pool Entries

The following example is an excerpt from an LDIF configuration file. It shows sample entries for a desktop pool named Pool1, which contains two virtual desktops named VM1 and VM2. The desktop pool entry is paired with the Desktop Application entry, which is also named Pool1.

```
#
# Virtual Desktop VM entry VM1
#
DN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm1
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-1
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 1
pae-TunneledConnection: 1
pae-pwdEncryption: KERB5
ipHostNumber: vm1
pae-ClientProtVersion: 1
pae-WinDomain: NULL
pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-1
pae-OptSuspendTimeout: 0
```

```
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0

#
# Virtual Desktop VM entry VM2
#
DN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm2
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-2
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 2
pae-TunneledConnection: 1
pae-pwdEncryption: KERB5
ipHostNumber: vm2
pae-ClientProtVersion: 1
pae-WinDomain: NULL
pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-2
pae-OptSuspendTimeout: 0
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0
#
# Further Virtual Desktop VM entries as required
#
#
# VM Pool entry Pool1
#
DN: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-ServerPool
cn: Pool1
pae-VCDN: CN=b180b93b-2dd3-4b58-8a81-b8534a4b7565,OU=VirtualCenter,OU=Properties,DC=vdi,
DC=vmware,DC=int
pae-MemberDN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-MemberDN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-VmPowerPolicy: remainon
pae-VmProvEnabled: 1
pae-VmProvSuspendOnError: 1
pae-VmStartClone: 1
pae-VmPoolCalculatedValues: 1
```

```
pae-ServerPoolType: 0
pae-VmMinimumCount: 0
pae-VmHeadroomCount: 0
pae-VmMaximumCount: 0
pae-Disabled: 0

#
# Desktop Application entry Pool1 -- one entry is required for each VM Pool
#
DN: CN=Pool1,OU=Applications,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Entity
objectClass: pae-App
objectClass: pae-WinApp
objectClass: pae-ThinWinApp
objectClass: pae-DesktopApplication
cn: Pool1
member:: PFNJRD1TLTEtMi0zLTQ+IA==
pae-Icon: /thinapp/icons/desktop.gif
pae-URL: \
pae-Servers: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
pae-ServerProtocolLevel: OSX_NETOP
pae-ServerProtocolLevel: OS2_NETOP
pae-ServerProtocolLevel: NT4_NETOP
pae-ServerProtocolLevel: WIN2K_NETOP
pae-ServerProtocolLevel: NT4_RDP
pae-ServerProtocolLevel: WIN2K_RDP
pae-ServerProtocolLevel: XP_RDP
pae-Disabled: 0
```

Import LDAP Configuration Data

You can use the `vdmimport` command to import configuration data from an LDIF configuration file into a standard or replica Connection Server instance.

Prerequisites

- Export LDAP configuration data to an LDIF configuration file. See Export LDAP Configuration Data.
- If you are importing a Cloud Pod Architecture global LDIF configuration file, verify that the Cloud Pod Architecture feature is initialized on the Connection Server instance.

Procedure

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

You must be logged in as a user in the Administrators role to import configuration data into the Horizon configuration repository.

2 At the command prompt, type the `vdmimport` command.

By default, the `vdmimport` command-line utility is installed in the `C:\Program Files\VMware\VMware View\Server\tools\bin` directory.

The `vdmimport` command has the following options.

Option	Description
-f	Input file name.
-i	Shows file information about the specified LDIF configuration file.
-d	Decrypts the specified LDIF configuration file.
-p	Specifies the recovery password for decryption of an encrypted LDIF configuration file. Type **""** to enter the password at the prompt.
-g	Specifies that the restore is for a Cloud Pod Architecture environment.

For example, the following commands decrypt and import a local LDIF configuration file.

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

```
vdmimport –f MyDecryptedexport.LDF
```

The following commands decyrypt and import a Cloud Pod Architecture global LDIF configuration file.

```
vdmimport –d –p mypassword –f MyEncryptedCPAexport.LDF > MyDecryptedCPAexport.LDF
```

```
vdmimport –g –f MyDecryptedCPAexport.LDF
```

Results

After the `vdmimport` command runs, the configuration of your Connection Server instance is updated with the data from the file, and the number of records that have been successfully updated is displayed. Errors appear if some records could not be updated because your role has insufficient privileges.

Connecting the VMware Horizon Deployment to the Horizon Control Plane

16

VMware Horizon offers the flexibility of deploying virtual desktops and applications on-premises, in a cloud-hosted environment, or a hybrid mix of both.

Regardless of where your virtual desktops and applications are running, you can optionally connect your VMware Horizon instance to the Horizon Control Plane and access the following services and benefits.

- The Horizon Cloud Administrator Console provides a single unified console across on-premise and multi-cloud deployments for working with your tenant's fleet of cloud-connected pods.

  Note For multi-location pods, Horizon assigns the deployment type of the connection server as the pod type and the location of the connection server as the pod location.

- The Horizon Universal Broker is the cloud-based brokering technology used to manage and allocate virtual resources from multi-cloud assignments to your end users.
- The Cloud Monitoring Service (CMS) is one of the central services provided in Horizon Control Plane. The CMS gives you the ability to monitor capacity, usage, and health within and across your fleet of cloud-connected pods, regardless of the deployment environments in which those individual pods reside.
- The Horizon Image Management Service is a cloud-based service that simplifies and automates the management of system images used by desktop assignments, such as desktop pools and farms, across your cloud-connected Horizon pods.

Horizon Control Plane is enabled with a subscription license. You must also use the Horizon Cloud Connector virtual appliance to connect your VMware Horizon deployment with the Horizon Control Plane. For more information about the subscription license, see "Enabling VMware Horizon for Subscription Licenses and Horizon Control Plane Services" in the *Horizon Installation* document.

The *Horizon Architecture Planning* document provides an overview and requirements of deploying VMware Horizon. For information about Horizon Control Plane, see Introduction to Horizon Cloud in the VMware Horizon Cloud Service documentation.

Using the Horizon PowerCLI Module

17

The Horizon PowerCLI Module includes Horizon PowerCLI cmdlets that you can use to perform various administration tasks on Horizon components. You can use Horizon PowerCLI with API specifications to create community-based open-source scripts.

You can install the Horizon PowerCLI module when you install VMware PowerCLI.

For more information about Horizon PowerCLI cmdlets, read the *VMware PowerCLI Cmdlets Reference* document available at https://code.vmware.com/docs/6978/cmdlet-reference.

For information on the API specifications to create advanced functions and scripts to use with Horizon PowerCLI, see the View API Reference at https://code.vmware.com/apis/405/view .

For more information on sample scripts that you can use to create your own Horizon PowerCLI scripts, visit the PowerCLI community at https://github.com/vmware/PowerCLI-Example-Scripts.

This chapter includes the following topics:

Set Up the Horizon PowerCLI Module

You can setup the Horizon PowerCLI module with VMware PowerCLI and use the Horizon PowerCLI cmdlets to connect or disconnect from Connection Server. After you connect to the Connection Server, you can write PowerShell scripts that invoke the Horizon APIs.

Procedure

1 Install VMware PowerCLI.

   Install VMware PowerCLI from the PowerShell Gallery. To install VMware PowerCLI, run the following command in the Windows PowerShell prompt:

   ```
   Install-Module -Name Vmware.PowerCLI
   ```

   This command installs all the VMware PowerCLI modules into Windows PowerShell. The `VMware.VimAutomation.HorizonView` module is the Horizon PowerCLI module.

You can also download and install VMware PowerCLI from https://code.vmware.com/web/dp/tool/vmware-powercli.

For more information on how to install VMware PowerCLI, see the *VMware PowerCLI User's Guide* available at https://code.vmware.com/web/dp/tool/vmware-powercli.

2 Import the Horizon PowerCLI module named `VMware.VimAutomation.HorizonView` in the Windows PowerShell session.

Use the following command to import `VMware.VimAutomation.HorizonView` into the Windows PowerShell session:

```
Import-Module -Name VMware.VimAutomation.HorizonView
```

`VMware.VimAutomation.HorizonView` contains the `Connect-HVServer` and `Disconnect-HVServer` cmdlets that you can use to connect to a Connection Server or disconnect from a Connection Server.

3 Pull sample scripts from the github repository.

After you use the `Connect-HVServer` cmdlet to connect to the Horizon API service of the Connection Server, you can run PowerShell scripts that invoke the Horizon APIs. For more information about Horizon APIs, see the *View API Reference* documentation available at https://code.vmware.com/apis/405/view.

Example scripts for the Horizon PowerCLI module are available as the `VMware.Hv.Helper` module in the Modules section at https://github.com/vmware/PowerCLI-Example-Scripts.

What to do next

Use the example scripts directly or modify the scripts to suit your automation needs. Apart from example scripts, you can also develop new scripts that invoke Horizon APIs based on your needs. See, Run Example Horizon PowerCLI Scripts.

Run Example Horizon PowerCLI Scripts

You can use example scripts that invoke Horizon APIs and use these scripts to perform administrator tasks. You can also modify these scripts to perform administrative tasks based on your requirements.

Prerequisites

- Complete the steps to install VMware PowerCLI and set up the Horizon PowerCLI module. See, Set Up the Horizon PowerCLI Module .

Procedure

1 Download the `VMware.Hv.Helper` module from the Modules section at https://github.com/vmware/PowerCLI-Example-Scripts.

2 Use the `$env:PSModulePath` command to find out the modules path in your Windows PowerShell session and copy the `VMware.Hv.Helper` module to that location.

3 Use the following command to load the `VMware.Hv.Helper` module into your Windows PowerShell session and start using the scripts.

```
 Get-Module -ListAvailable 'Vmware.Hv.Helper' | Import-Module Get-Command -Module
'VMware.Hv.Helper'
```