Horizon Console Administration

DEC 2019
VMware Horizon 7 7.11

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

VMware Horizon Console Administration

1

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

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

Intended Audience

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

Using VMware Horizon Console

2

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

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

For more information about JMP) Integrated Workflow features, see Chapter 10 Getting Started with JMP Integrated Workflow .

This chapter includes the following topics:

Supported Horizon 7 Features

Horizon Console is based on HTML5 technology and allows you to manage your complete Horizon 7 deployment. Horizon Console replaces the Flash-based Horizon Administrator.

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

The following features are supported:

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

    - Application entitlements
    - Global entitlements
    - Global policies
- Authentication
    - Remote access authentication
    - Unauthenticated access for published applications
    - Smart card authentication
    - Role-based delegated administration
- Virtual desktops
    - Automated, dedicated-assignment pools of full virtual machines
    - Automated, instant-clone dedicated-assignment and floating-assignment pools
    - Automated linked-clone desktop pools
    - Automated, floating-assignment pools of full virtual machines
    - Manual desktop pools
    - Persistent disks
- Published desktops
    - Manual farms
    - Automated instant-clone farms
    - Automated linked-clone farms
    - RDS desktop pools
- Published applications
    - Manual application pools
    - Application pools from existing applications
- Virtual machines
    - Virtual Machines available in vCenter Server
    - Registered machines that are not available in vCenter Server
- Cloud Pod Architecture

The following features are not supported:

- ThinApp applications
- Security server
- Mirage server

Benefits of Using Horizon Console

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

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

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

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

Installing and Configuring Horizon Console

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

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

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

Log In to Horizon Console

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

Prerequisites

- Verify that Horizon Connection Server is installed on a dedicated computer.
- A user must be assigned any predefined role or a combination of predefined roles to login to Horizon Console. You cannot login to Horizon Console when the user is assigned a custom role or a combination of predefined and custom roles. For more information on configuring role-based access, see Configuring Role-Based Delegated Administration.
- Verify that you are using a Web browser supported by Horizon Console. For more information about supported Web browsers, see the *Horizon 7 Installation* document.

Procedure

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

`https://server/admin`

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

Your access to Horizon 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.

Option	Description
You configured a certificate signed by a CA for Connection Server.	When you first connect, your Web browser displays the **Welcome to VMware Horizon 7** 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 To always use the Horizon Console login page, click **Always use this option**.

Note If you click **Always use this option** and click **Launch**, the next time you open a tab in the web browser and enter **`https://server/admin`**, you will always get the Horizon Console login page. To access the **Welcome to VMware Horizon 7** page again, go to **`https://server/admin/#home`**.

3 Click **Launch** under Horizon Console to open the Horizon Console login page.

4 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.

What to do next

To identify the CPA pod or cluster name of the Connection Server you are working with, you can view the name in the Horizon Console header and in the Web browser tab.

Configuring Horizon Connection Server in Horizon Console

3

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

This chapter includes the following topics:

Configuring vCenter Server and Horizon Composer in Horizon Console

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

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

Create a User Account for Horizon Composer AD Operations

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

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

Procedure

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

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

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

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

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

What to do next

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

Install the Product License Key in Horizon Console

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

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

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

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

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

Procedure

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

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

Add vCenter Server Instances to Horizon 7 in Horizon Console

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

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

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

Prerequisites

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

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

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

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

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

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

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

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

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

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

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

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **vCenter Server** tab, click **Add**.
3. In the vCenter Server Settings **Server address** text box, type the fully qualified domain name (FQDN) of the vCenter Server instance.

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

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

4. Type the name of the vCenter Server user.

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

5. Type the vCenter Server user password.
6. (Optional) Type a description for this vCenter Server instance.

7 Type the TCP port number.

   The default port is 443.

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

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

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

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

What to do next

Configure Horizon Composer settings.

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

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

Configure Horizon Composer Settings

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

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

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

Prerequisites

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

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

Procedure

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

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

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

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

What to do next

Configure Horizon Composer domains.

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

Configure Horizon Composer Domains

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

Prerequisites

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

Procedure

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

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

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

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

What to do next

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

Add an Instant-Clone Domain Administrator in Horizon Console

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

Prerequisites

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

Procedure

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

What to do next

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

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

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

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

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

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

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

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

The following guidelines apply to the space reclamation feature:

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

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

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

Prerequisites

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

Procedure

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

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

What to do next

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

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

Configure Horizon Storage Accelerator for vCenter Server

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

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

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

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

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

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

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

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

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

Prerequisites

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

  In an ESXi cluster, verify that all the hosts are version 5.1 or later.
- Verify that the vCenter Server user was assigned the **Host > Configuration > Advanced settings** privilege in vCenter Server.

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

Procedure

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

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

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

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

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

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

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

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

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

What to do next

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

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

Concurrent Operations Limits for vCenter Server and Horizon Composer

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

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

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

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

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

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

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

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

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

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

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

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

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

Accept the Thumbprint of a Default TLS Certificate

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

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

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

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

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

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

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

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

Procedure

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

2 Examine the certificate thumbprint in the Certificate Information window.

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

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

   b Navigate to the vCenter Server or Horizon Composer certificate.

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

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

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

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

5 Determine whether to accept the certificate thumbprint.

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

Remove a vCenter Server Instance from Horizon 7

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

Prerequisites

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

Procedure

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

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

3 Click **Remove**.

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

4 Click **OK**.

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

Remove Horizon Composer from Horizon 7

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

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

Procedure

1. Remove the linked-clone desktop pools created by Horizon Composer.
   a. In Horizon Console, select **Inventory > Desktops**.
   b. Select a linked-clone desktop pool and click **Delete**.

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

      The virtual machines are deleted from vCenter Server. In addition, the associated Horizon Composer database entries and the replicas created by Horizon Composer are removed.
   d. Repeat these steps for each linked-clone desktop pool created by Horizon Composer.
2. Navigate to **Settings > Servers**.
3. On the **vCenter Servers** tab, select the vCenter Server instance with which Horizon Composer is associated.
4. Click **Edit**.
5. On the **Horizon Composer** tab, under Horizon Composer Server Settings, select **Do not use Horizon Composer**, and click **OK**.

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

What to do next

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

Conflicting vCenter Server Unique IDs

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

Problem

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

Cause

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

Solution

1. In vSphere Client, click **Administration > vCenter Server Settings > Runtime Settings**.
2. Type a new unique ID and click **OK**.

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

Backing Up Horizon Connection Server in Horizon Console

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

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

Configuring Settings for Client Sessions in Horizon Console

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

Global Settings for Client Sessions in Horizon Console

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

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 Horizon 7 Connection Server or Horizon Client.

Table 3-2. General Global Settings for Client Sessions

Setting	Description
View Administrator session timeout	Determines how long an idle Horizon Console session continues before the session times out. **Important** Setting the Horizon Console session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Console. Use caution when you allow an idle session to persist a long time. By default, the Horizon Console session timeout is 30 minutes. You can set a session timeout from 10 to 4320 minutes (72 hours). 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.
Forcibly disconnect users	Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to Horizon 7. All desktops and applications will be disconnected at the same time regardless of when the user opened them. For clients that do not support application remoting, a maximum timeout value of 1200 minutes applies if the value of this setting is **Never** or greater than 1200 minutes. The default is **After 600 minutes**.
Single sign-on (SSO)	If SSO is enabled, Horizon 7 caches a user's credentials so that the user can launch remote desktops or applications without having to provide credentials to log in to the remote Windows session. The default is **Enabled**. If you plan to use the True SSO feature, introduced in Horizon 7 or later, SSO must be enabled. With True SSO, if a user logs in using some other form of authentication than Active Directory credentials, the True SSO feature generates short-term certificates to use, rather than cached credentials, after users log in to VMware Identity Manager. **Note** If a desktop is launched from Horizon Client, and the desktop is locked, either by the user or by Windows based on a security policy, and if the desktop is running Horizon 7 Agent 6.0 or later or Horizon Agent 7.0 or later, Horizon 7 Connection Server discards the user's SSO credentials. The user must provide login credentials to launch a new desktop or a new application, or reconnect to any disconnected desktop or application. To enable SSO again, the user must disconnect from Horizon 7 Connection Server or exit Horizon Client, and reconnect to Horizon 7 Connection Server. However, if the desktop is launched from Workspace ONE or VMware Identity Manager and the desktop is locked, SSO credentials are not discarded.
Enable automatic status updates	Determines if status updates appear in the global status pane in the upper-left corner of Horizon Console every few minutes. The dashboard page of Horizon Console is also updated every few minutes. By default, this setting is not enabled.

Table 3-2. General Global Settings for Client Sessions (continued)

Setting	Description
For clients that support applications. **If the user stops using the keyboard and mouse, disconnect their applications and discard SSO credentials:**	Protects application sessions when there is no keyboard or mouse activity on the client device. If set to **After ... minutes**, Horizon 7 disconnects all applications and discards SSO credentials after the specified number of minutes without user activity. Desktop sessions are not disconnected. Users must log in again to reconnect to the applications that were disconnected or launch a new desktop or application. This setting also applies to the True SSO feature. After SSO credentials are discarded, users are prompted for Active Directory credentials. If users logged in to VMware Identity Manager without using AD credentials and do not know what AD credentials to enter, users can log out and log in to VMware Identity Manager again to access their remote desktops and applications. **Important** Users must be aware that when they have both applications and desktops open, and their applications are disconnected because of this timeout, their desktops remain connected. Users must not rely on this timeout to protect their desktops. If set to **Never**, Horizon 7 never disconnects applications or discards SSO credentials due to user inactivity. The default is **Never**.
Other clients. **Discard SSO credentials:**	Discards SSO credentials after the specified number of minutes. This setting is for clients that do not support application remoting. If set to **After ... minutes**, users must log in again to connect to a desktop after the specified number of minutes has passed since the user logged in to Horizon 7, regardless of any user activity on the client device. If set to **Never**, Horizon 7 stores SSO credentials until the user closes Horizon Client, or the **Forcibly disconnect users** timeout is reached, whichever comes first. The default is **After 15 minutes**.
Display a pre-login message	Displays a disclaimer or another message to Horizon Client users when they log in. Type your information or instructions in the text box in the Global Settings dialog box. To display no message, leave the check box unselected.
Display warning before forced logoff	Displays a warning message when users are forced to log off because a scheduled or immediate update such as a desktop-refresh operation is about to start. This setting also determines how long to wait after the warning is shown before the user is logged off. Check the box to display a warning message. Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is 5 minutes. Type your warning message. You can use the default message: `Your desktop is scheduled for an important update and will be shut down in 5 minutes. Please save any unsaved work now.`
Enable Windows Server desktops	Determines whether you can select available Windows Server 2008 R2 and Windows Server 2012 R2 machines for use as desktops. When this setting is enabled, Horizon Console displays all available Windows Server machines, including machines on which Horizon 7 server components are installed. **Note** The Horizon Agent software cannot coexist on the same virtual or physical machine with any other Horizon 7 server software component, including a security server, Horizon 7 Connection Server, or Horizon 7 Composer.

Table 3-2. General Global Settings for Client Sessions (continued)

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

Global Security Settings for Client Sessions and Connections in Horizon Console

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

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

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

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

Global Client Restriction Settings for Client Sessions in Horizon Console

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

In Horizon Console, you can configure global client restriction settings by navigating to **Settings > Global Settings > Client Restriction Settings** and entering the version for Horizon Clients.

Horizon Clients must be version 4.5.0 or later, except Horizon Client for Chrome, which must be version 4.8.0 or later. Earlier versions of Horizon Client are prevented from connecting to remote desktops and published applications when this feature is configured.

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 Horizon 7.

Table 3-4. Global Client Restriction Settings for Client Sessions

Setting	Description
Horizon Client for Windows	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for Linux	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for Mac	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for iOS	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for Android	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for UWP	Enter a Horizon Client version number that is version 4.5.0 or later.
Horizon Client for Chrome	Enter a Horizon Client version number that is version 4.8.0 or later.
Horizon Client for HTML Access	Enter a Horizon Client version number that is version 4.5.0 or later.
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`.
Message	Enter the message to display if a user tries to launch a desktop or published application from a non-whitelisted client type or version.

Disable or Enable Horizon Connection Server in Horizon Console

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

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

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

- If this is a single, standalone Connection Server instance, users cannot log in to their desktops or applications. They cannot connect to Connection Server.
- If this is a replicated Connection Server instance, your network topology determines whether users can be routed to another replicated instance. If users can access another instance, they can log in to their desktops and applications.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance.
3. Click **Disable**.

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

Edit the External URLs for Horizon Connection Server Instances

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

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

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

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

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

Procedure

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

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

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

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

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

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

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

For example: `10.20.30.40:4172`

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

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

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

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

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

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

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

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

Register Gateways in Horizon Console

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

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

Procedure

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

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

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

4 Click **OK**.

Setting Up Smart Card Authentication

4

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

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

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

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

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

This chapter includes the following topics:

Logging In with a Smart Card

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

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

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

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

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

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

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

Configure Smart Card Authentication on Horizon Connection Server

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

Procedure

1 Obtain the Certificate Authority Certificates

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

2 Obtain the CA Certificate from Windows

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

3 Add the CA Certificate to a Server Truststore File

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

4 Modify Horizon Connection Server Configuration Properties

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

5 Configure Smart Card Settings in Horizon Console

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

Obtain the Certificate Authority Certificates

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

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

Procedure

- Obtain the CA certificates from one of the following sources.
  - A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.
  - The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

Obtain the CA Certificate from Windows

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

Procedure

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

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

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

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

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

Add the CA Certificate to a Server Truststore File

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

Prerequisites

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

  Important These certificates can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.
- Verify that the `keytool` utility is added to the system path on your Connection Server or security server host. See the *Horizon 7 Installation* document for more information.

Procedure

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

For example:
`keytool –import –alias` ***`alias`*** **`–file`** ***`root_certificate`*** **`–keystore`** ***`truststorefile.key`***

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

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

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

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

What to do next

Modify Connection Server configuration properties to enable smart card authentication.

Modify Horizon Connection Server Configuration Properties

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

Prerequisites

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

Procedure

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

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

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

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

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

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

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

Example: locked.properties File

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

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

What to do next

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

Configure Smart Card Settings in Horizon Console

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

Prerequisites

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

Procedure

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

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

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

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

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

b Configure the smart card removal policy.

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

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

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

c Configure the smart card user name hints feature.

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

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

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

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

5 Click **OK**.

6 Restart the Connection Server service.

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

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

What to do next

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

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

Configure Smart Card Authentication on Third Party Solutions

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

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

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

Procedure

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

   See Configure a SAML Authenticator in Horizon Console.

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

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

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

   See the product documentation for the third-party device.

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

   See the product documentation for the third-party device.

Prepare Active Directory for Smart Card Authentication

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

- Add UPNs for Smart Card Users

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

- Add the Root Certificate to the Enterprise NTAuth Store

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

- Add the Root Certificate to Trusted Root Certification Authorities

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

- Add an Intermediate Certificate to Intermediate Certification Authorities

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

Add UPNs for Smart Card Users

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

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

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

Prerequisites

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

Procedure

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

Add the Root Certificate to the Enterprise NTAuth Store

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

Procedure

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

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

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

Add the Root Certificate to Trusted Root Certification Authorities

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

Procedure

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

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

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

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

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

5 Close the Group Policy window.

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

What to do next

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

Add an Intermediate Certificate to Intermediate Certification Authorities

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

Procedure

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

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

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

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

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

5 Close the Group Policy window.

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

Verify Your Smart Card Authentication Configuration in Horizon Console

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

Procedure

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

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

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

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

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

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

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

  a Select **Settings > Servers**.

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

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

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

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

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

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

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

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

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

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

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

Using Smart Card Certificate Revocation Checking

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

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

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

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

- Logging in with CRL Checking

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

- Logging in with OCSP Certificate Revocation Checking

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

- Configure CRL Checking

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

- Configure OCSP Certificate Revocation Checking

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

- Smart Card Certificate Revocation Checking Properties

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

Logging in with CRL Checking

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

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

Logging in with OCSP Certificate Revocation Checking

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

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

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

Configure CRL Checking

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

Prerequisites

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

Procedure

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

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

2. Add the `enableRevocationChecking` and `crlLocation` properties to the `locked.properties` file.
   a. Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.
   b. Set `crlLocation` to the location of the CRL. The value can be a URL or a file path.
3. Restart the Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

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

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

Configure OCSP Certificate Revocation Checking

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

Prerequisites

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

Procedure

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

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

2. Add the `enableRevocationChecking`, `enableOCSP`, `ocspURL`, and `ocspSigningCert` properties to the `locked.properties` file.
   a. Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.
   b. Set `enableOCSP` to **`true`** to enable OCSP certificate revocation checking.
   c. Set `ocspURL` to the URL of the OCSP Responder.
   d. Set `ocspSigningCert` to the location of the file that contains the OCSP Responder's signing certificate.
3. Restart the Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

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

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

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

Smart Card Certificate Revocation Checking Properties

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

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

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

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

Setting Up Other Types of User Authentication

5

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

This chapter includes the following topics:

Using Two-Factor Authentication

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

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

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

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

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

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

- Logging in Using Two-Factor Authentication

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

- Enable Two-Factor Authentication in Horizon Console

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

- Troubleshooting RSA SecureID Access Denied

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

- Troubleshooting RADIUS Access Denial

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

Logging in Using Two-Factor Authentication

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

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

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

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

Enable Two-Factor Authentication in Horizon Console

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

Prerequisites

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

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

Procedure

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

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

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

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

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

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

   - 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.

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

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

What to do next

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

Troubleshooting RSA SecureID Access Denied

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

Problem

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

Cause

The RSA Agent host node secret needs to be reset.

Solution

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

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

Troubleshooting RADIUS Access Denial

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

Problem

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

Cause

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

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

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

Using SAML Authentication for VMware Identity Manager Integration

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

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

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

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

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

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

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

Configure a SAML Authenticator in Horizon Console

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

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

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

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

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

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

Prerequisites

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

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

Procedure

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

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

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

4. Click **Manage SAML Authenticators** and click **Add**.
5. Configure the SAML authenticator in the Add SAML 2.0 Authenticator dialog box.

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

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

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

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

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

What to do next

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

Configure Proxy Support for VMware Identity Manager

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

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

Prerequisites

Procedure

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

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

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

Change the Expiration Period for Service Provider Metadata on Connection Server

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

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

Prerequisites

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

Procedure

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

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

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

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

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

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

Prerequisites

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

Procedure

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

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

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

This page displays the SAML metadata from Connection Server.

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

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

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

What to do next

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

Response Time Considerations for Multiple Dynamic SAML Authenticators

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

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

Configure Workspace ONE Access Policies in Horizon Console

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

Prerequisites

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

Procedure

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

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

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

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

4 Select **Enable Workspace ONE mode**.

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

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

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

Configure Biometric Authentication

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

Prerequisites

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

Procedure

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

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

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

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

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

   The following `BioMetricsTimeout` values are valid:

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

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

Authenticating Users and Groups 6

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

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

This chapter includes the following topics:

Restricting Remote Desktop Access Outside the Network

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

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

Configure Remote Access

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

Prerequisites

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

Procedure

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

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

Configuring Unauthenticated Access

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

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

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

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

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

Create Users for Unauthenticated Access

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

Prerequisites

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

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

Procedure

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

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

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

What to do next

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

Enable Unauthenticated Access for Users in Horizon Console

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.

Delete an Unauthenticated Access User

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

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

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

Procedure

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

What to do next

Remove application entitlements for the user.

Unauthenticated Access From Horizon Client

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

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

Prerequisites

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

Procedure

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

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

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.

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 Horizon 7 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 Horizon 7 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 7* document.

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. 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 7 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.

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.

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.
- The client machine must be able to communicate with the corporate Active Directory server and not use cached credentials for authentication. For example, if users log in to their client machines from

outside the corporate network, cached credentials are used for authentication. If the user then attempts to connect to a security server or a Connection Server instance without first establishing a VPN connection, the user is prompted for credentials, and the Log in as current user feature does not work.

Configuring Role-Based Delegated Administration in Horizon Console

7

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

This chapter includes the following topics:

Understanding Roles and Privileges

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

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

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

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

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

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

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

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

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

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

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

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

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

- Different Administrators for Different Access Groups

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

- Different Administrators for the Same Access Group

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

Different Administrators for Different Access Groups

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

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

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

Table 7-1. Different Administrators for Different Access Groups

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

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

Different Administrators for the Same Access Group

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

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

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

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

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

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

Understanding Permissions

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

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

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

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

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

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

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

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

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

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

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

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

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

Manage Administrators

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

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

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

- Create an Administrator in Horizon Console

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

- Remove an Administrator in Horizon Console

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

Create an Administrator in Horizon Console

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

Prerequisites

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

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Administrators and Groups** tab, click **Add User or Group**.
3. Click **Add**, select one or more search criteria, and click **Find** to filter Active Directory users or groups based on your search criteria.

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

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

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

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

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

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

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

Remove an Administrator in Horizon Console

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

Procedure

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

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

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

Manage and Review Permissions

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

- Add a Permission in Horizon Console

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

- Delete a Permission in Horizon Console

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

- Review Permissions in Horizon Console

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

Add a Permission in Horizon Console

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

Procedure

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

2 Create the permission.

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

Delete a Permission in Horizon Console

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

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

Procedure

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

2 Select the permission to delete.

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

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

Review Permissions in Horizon Console

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

Procedure

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

2 Review the permissions.

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

Manage and Review Access Groups

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

- Add an Access Group in Horizon Console

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

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

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

- Remove an Access Group in Horizon Console

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

- Review the Objects in an Access Group

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

- Review the vCenter Virtual Machines in an Access Group

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

Add an Access Group in Horizon Console

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

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

Procedure

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

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

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

The description is optional.

What to do next

Move one or more objects to the access group.

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

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

Procedure

1. In Horizon Console, select **Inventory > Desktops** or **Inventory > Farms**.
2. Select a pool or a farm.
3. Select **Change Access Group** from the **Access Group** drop-down menu.
4. Select the access group and click **OK**.

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

Remove an Access Group in Horizon Console

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

Prerequisites

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

Procedure

1. In Horizon Console, navigate to **Settings > Administrators**.
2. On the **Access Groups** tab, select the access group and click **Remove Access Group**.
3. Click **OK** to remove the access group.

Review the Objects in an Access Group

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

Procedure

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

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

Object	Action
Farms	Select **Inventory > Farms**.
Persistent Disks	Select **Inventory > Persistent Disks**.

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

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

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

Review the vCenter Virtual Machines in an Access Group

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

Procedure

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

2 Select the **vCenter VMs** tab.

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

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

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

Manage Custom Roles

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

- Add a Custom Role in Horizon Console

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

- Modify the Privileges in a Custom Role in Horizon Console

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

- Remove a Custom Role in Horizon Console

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

Add a Custom Role in Horizon Console

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

Prerequisites

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

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

Procedure

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

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

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

The new role appears in the left pane.

Modify the Privileges in a Custom Role in Horizon Console

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

Prerequisites

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

Procedure

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

2 On the **Role Privileges** tab, select the role.

3 View the privileges in the role and click **Edit**.

4 Select or deselect privileges.

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

Remove a Custom Role in Horizon Console

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

Prerequisites

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

Procedure

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

2 On the **Role Privileges** tab, select the role and click **Remove Role**.

The **Remove Role** button is not available for predefined roles or for custom roles that are included in a permission.

3 Click **OK** to remove the role.

Predefined Roles and Privileges

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

- Predefined Administrator Roles

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

- Global Privileges

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

- Object Specific Privileges

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

- Internal Privileges

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

Predefined Administrator Roles

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

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

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

Table 7-6. Predefined Roles in Horizon Console

Role	User Capabilities	Applies to an Access Group
Administrators	Perform all administrator operations, including creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role can configure and manage a pod federation and manage remote pod sessions. Administrators that have the Administrators role on the root access group are super users because they have full access to all of the inventory objects in the system. Because the Administrators role contains all privileges, you should assign it to a limited set of users. Initially, members of the local Administrators group on your Connection Server host are given this role on the root access group. **Important** An administrator must have the Administrators role on the root access group to perform the following tasks: ■ Add and delete access groups. ■ Manage ThinApp applications and configuration settings in Horizon Console. ■ Use the `vdmadmin` , `vdmimport`, and `lmvutil` commands.	Yes
Administrators (Read only)	■ View, but not modify, global settings and inventory objects. ■ View, but not modify, ThinApp applications and settings. ■ Run all PowerShell commands and command line utilities, including `vdmexport` but excluding `vdmadmin`, `vdmimport`, and `lmvutil`. In a Cloud Pod Architecture environment, administrators that have this role can view inventory objects and settings in the Global Data Layer. When administrators have this role on an access group, they can only view the inventory objects in that access group.	Yes
Agent Registration Administrators	Register unmanaged machines such as physical systems, standalone virtual machines, and RDS hosts.	No
Global Configuration and Policy Administrators	View and modify global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Global Configuration and Policy Administrators (Read only)	View, but not modify, global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Help Desk Administrators	Perform desktop and application actions such as shutdown, reset, restart, and perform remote assistance actions such as end processes for a user's desktop or application. An administrator must have permissions on the root access group to access Horizon Help Desk Tool. ■ Read-only access to Horizon Help Desk Tool. ■ Manage global sessions. ■ Can log in to Horizon Console. ■ Perform all machine and session-related commands. ■ Manage remote processes and applications. ■ Remote assistance to the virtual desktop or published desktop.	No

Table 7-6. Predefined Roles in Horizon Console (continued)

Role	User Capabilities	Applies to an Access Group
Help Desk Administrators (Read Only)	View user and session information, and drill down on session details. An administrator must have permissions on the root access group to access Horizon Help Desk Tool. ■ Read-only access to Horizon Help Desk Tool. ■ Can log in to Horizon Console.	No
Inventory Administrators	■ Perform all machine, session, and pool-related operations. ■ Manage persistent disks. ■ Resync, Refresh, and Rebalance linked-clone pools and change the default pool image. ■ Manage automated farms. When administrators have this role on an access group, they can only perform these operations on the inventory objects in that access group. Administrators with this role cannot create a manual farm or an unmanaged manual pool or add or remove RDS hosts to the farm or unmanaged manual pool.	Yes
Inventory Administrators (Read only)	View, but not modify, inventory objects. When administrators have this role on an access group, they can only view the inventory objects in that access group.	Yes
Local Administrators	Perform all local administrator operations, except for creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role cannot perform operations on the Global Data Layer or manage sessions on remote pods. **Note** An administrator with the Local Administrators role cannot access Horizon Help Desk Tool. Administrators in a non-CPA environment do not have the Manage Global Sessions privilege, which is required to perform tasks in Horizon Help Desk Tool.	Yes
Local Administrators (Read Only)	Same as the Administrators (Read Only) role, except for viewing inventory objects and settings in the Global Data Layer. Administrators that have this role have read-only rights only on the local pod. **Note** An administrator with the Local Administrators (Read Only) role cannot access Horizon Help Desk Tool. Administrators in a non-CPA environment do not have the Manage Global Sessions privilege, which is required to perform tasks in Horizon Help Desk Tool.	Yes

Global Privileges

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

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

Table 7-7. Global Privileges

Privilege	User Capabilities	Predefined Roles
Console Interaction	Log in to and use Horizon Console. **Note** Starting in Horizon 7 version 7.10, the **Console Interaction** privilege is automatically added to new roles and 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	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** Starting in Horizon 7 version 7.10, the **Direct Interaction** privilege is automatically added to new roles and does not appear in the list of global privileges in Horizon Console.	Administrators Administrators (Read only)
Manage Global Configuration and Policies	View and modify global policies and configuration settings except for administrator roles and permissions.	Administrators Global Configuration and Policy Administrators
Manage Global Sessions	Manage global sessions in a Cloud Pod Architecture environment.	Administrators
Manage Roles and Permissions	Create, modify, and delete administrator roles and permissions.	Administrators
Register Agent	Install Horizon Agent on unmanaged machines, such as physical systems, standalone virtual machines, and RDS hosts. During Horizon Agent installation, you must provide your administrator login credentials to register the unmanaged machine with the Connection Server instance.	Administrators Agent Registration Administrators
Manage vCenter Configuration (Read only)	Read only access to 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.

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

Table 7-8. Object-Specific Privileges

Privilege	User Capabilities	Object
Enable Farms and Desktop Pools	Enable and disable desktop pools.	Desktop pool, farm
Entitle Desktop and Application Pools	Add and remove user entitlements.	Desktop pool, application pool
Manage Maintenance Operations on Automated Desktops and Farms	Recompose, refresh, rebalance, schedule push image, schedule maintenance and change the default image for a desktop pool and farm.	Desktop pool, farm
Manage Machine	Perform all machine and session-related operations.	Machine
Manage Persistent Disks	Perform all Horizon Composer persistent disk operations, including attaching, detaching, and importing persistent disks.	Persistent disk
Manage Farms and Desktop and Application Pools	Add, modify, and delete farms. Add, modify, delete, and entitle desktop and application pools. Add and remove machines.	Desktop pool, application pool, farm
Manage Sessions	Disconnect and log off sessions and send messages to users.	Session
Manage Reboot Operation	Reset virtual machines or restart virtual desktops.	Machine

Internal Privileges

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

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

Table 7-9. Internal Privileges

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

Required Privileges for Common Tasks

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

Privileges for Managing Pools

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

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

Table 7-10. Pool Management Tasks and Privileges

Task	Required Privileges
Enable or disable a desktop pool.	**Enable Farms and Desktop Pools**
Entitle or unentitle users to a pool.	**Entitle Desktop and Application Pools**
Add a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Modify or delete a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for deleting an unmanaged desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Add or remove desktops from a pool.	**Manage Farms and Desktop and Application Pools** **Note** Not applicable for adding or removing unmanaged virtual desktops in the desktop pool. The administrator must also have the Global Configuration and Policy Administrators (Read only) role to perform this task.
Refresh, recompose, rebalance, or change the default Horizon Console image.	**Manage Composer Desktop Pool Image** and the **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 7-11. Machine Management Tasks and Privileges

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

Privileges for Managing Persistent Disks

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

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

Table 7-12. Persistent Disk Management Tasks and Privileges

Task	Required Privileges
Detach a disk.	■ If the disk is a secondary disk, the **Manage Persistent Disks** privilege is required. ■ If the disk is a primary disk, the **Manage Persistent Disks** and **Manage Machine** privileges are required. ■ To detach any disk on a different datastore, the **Manage vCenter Configuration (Read only)** privilege is also required for the administrator.
Attach a disk.	**Manage Persistent Disks** on the disk and **Manage Machine** on the machine.
Edit a disk.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** on the selected pool.
Change access groups.	**Manage Persistent Disks** on the source and target access groups.
Recreate a desktop.	**Manage Persistent Disks** on the disk and **Manage Farms and Desktop and Application Pools** or **Manage Machine** on the last desktop pool.
Import from vCenter.	**Manage Persistent Disks** on the disk and **Manage vCenter Configuration (Read only)**.
Delete a disk.	**Manage Persistent Disks** on the disk.

Privileges for Managing Users and Administrators

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

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

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

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

Privileges for Horizon Help Desk 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.

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

Tasks	Required Privileges
Read-only access to Horizon Help Desk Tool.	**Manage Help Desk (Read Only)**
Manage global sessions.	**Manage Global Sessions**
Can log in to Horizon Console.	**Console Interaction** **Note** Starting in Horizon 7 version 7.10, the **Console Interaction** privilege is automatically added to new roles and does not appear in the list of global privileges in Horizon Console.
Perform all machine and session-related commands.	**Manage Machine**
Reset or restart machines.	**Manage Reboot Operation**
Disconnect and log off sessions.	**Manage Sessions**
Manage remote processes and applications.	**Manage Remote Processes and Applications**
Remote assistance to the virtual desktop or published desktop.	**Remote Assistance**
Disconnect, logoff, reset, and restart operations for global sessions.	**Manage Help Desk (Read Only)** and **Manage Global Sessions**
Reset and restart operations for local sessions.	**Manage Help Desk (Read Only)** and **Manage Reboot Operation**
Remote assistance operations.	**Manage Help Desk (Read Only)** and **Remote Assistance**
End remote processes and applications.	**Manage Help Desk (Read Only)** and **Manage Remote Processes and Applications**

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

Tasks	Required Privileges
Perform all tasks in Horizon Help Desk Tool.	**Manage Help Desk (Read Only)**, **Mange Global Sessions**, **Manage Reboot Operation**, **Remote Assistance**, and **Manage Remote Processes and Applications**
Remote assistance operations and end remote processes and applications.	**Manage Help Desk (Read Only)**, **Remote Assistance**, and **Manage Remote Processes and Applications**
Disconnect and logoff operations for local sessions.	**Manage Help Desk (Read Only)** and **Manage Sessions**

Privileges for General Administration Tasks and Commands

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

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

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

Task	Required Privileges
Add or delete an access group	Must have the Local Administrators role or Administrators role on the root access group for deleting an access group. Must have the Inventory Administrators or Local Administrators or Administrators role on the root access group.
Manage ThinApp applications and settings in Horizon Administrator	Must have the Administrators role on the root access group.
Install Horizon Agent on an unmanaged machine, such as a physical system, standalone virtual machine, or RDS host	**Register Agent**
View or modify configuration settings (except for administrators) in Horizon Administrator	**Manage Global Configuration and Policies**
Run all PowerShell commands and command line utilities except for `vdmadmin` and `vdmimport`.	**Direct Interaction** **Note** Starting in Horizon 7 version 7.10, the Direct Interaction privilege is automatically added to new roles and 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 vCenter Server configuration.	**Manage vCenter Configuration (Read only)**

Best Practices for Administrator Users and Groups

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

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

Setting Policies in Horizon Console

8

You use Horizon Console to configure policies for client sessions.

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

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

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

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

This chapter includes the following topics:

Configure Global Policies

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

Procedure

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

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

Table 8-1. Horizon Policies

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

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

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

Maintaining Horizon 7 Components

9

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

This chapter includes the following topics:

Backing Up and Restoring Horizon 7 Configuration Data

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

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

Backing Up Horizon Connection Server and Horizon Composer Data

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

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

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

You can perform backups in several ways.

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

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

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

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

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

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

Schedule Horizon 7 Configuration Backups

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

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

Prerequisites

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

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance to be backed up and click **Backup Now**.
3. On the **Backup** tab, specify the Horizon 7 configuration backup settings to configure the backup frequency, maximum number of backups, and the folder location of the backup files.
4. (Optional) Change the data recovery password.
   a. Click **Change data recovery password**.
   b. Type and retype the new password.
   c. (Optional) Type a password reminder.
   d. Click **OK**.
5. Click **OK**.

Horizon 7 Configuration Backup Settings

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

Table 9-1. Horizon 7 Configuration Backup Settings

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

Export Configuration Data from Horizon Connection Server

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

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

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

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

Prerequisites

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

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

- Log in to a Connection Server instance as a user in the Administrators or Administrators (Read only) role.

Procedure

1. Select **Start > Command Prompt**.
2. At the command prompt, type the `vdmexport` command and redirect the output to a file. For example:

   ```
   vdmexport > Myexport.LDF
   ```

   By default, the exported data is encrypted.

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

   ```
   vdmexport –f Myexport.LDF
   ```

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

   ```
   vdmexport –f Myexport.LDF –v
   ```

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

   ```
   vdmexport –f Myexport.LDF –c
   ```

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

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

What to do next

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

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

Restoring Horizon Connection Server and Horizon Composer Configuration Data

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

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

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

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

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

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

Import Configuration Data into Horizon Connection Server

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

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

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

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

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

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

Prerequisites

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

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

- Log in to a Connection Server instance as a user with the Administrators role.
- Verify that you know the data recovery password. If a password reminder was configured, you can display the reminder by running the `vdmimport` command without the password option.

Procedure

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

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

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

   If you do not remember your data recovery password, type the command without the `–p` option. The utility displays the password reminder and prompts you to enter the password.
7. Import the decrypted LDIF file to restore the View LDAP configuration.

   Specify the `–f` option with the decrypted LDIF file. For example:
8. Uninstall Connection Server.

   Uninstall only the package VMware Horizon Connection Server.
9. Reinstall Connection Server.
10. Log in to Horizon Console and validate that the configuration is correct.
11. Start the Horizon Composer instances.
12. Reinstall the replica server instances.

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

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

Restore a Horizon Composer Database

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

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

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

Prerequisites

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

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

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

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

Familiarize yourself with the `SviConfig restoredata` parameters:

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

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

Procedure

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

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

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

   For example:

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

What to do next

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

Result Codes for Restoring the Horizon Console Database

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

Table 9-2. Restoredata Result Codes

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

Export Data in Horizon Composer Database

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

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

Prerequisites

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

Familiarize yourself with the `SviConfig exportdata` parameters:

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

Procedure

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

   The file is located with the Horizon Composer application.

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

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

   For example:

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

What to do next

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

Result Codes for Exporting the Horizon Composer Database

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

Table 9-3. Exportdata ExitStatus Codes

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

Monitor Horizon 7 Components

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

Horizon Console displays monitoring information about Connection Server instances, the event database, gateways, Horizon Composer services, datastores, vCenter Server instances, and domains.

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

Procedure

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

   The details pane displays the name, version and other information related to each issue.

   - 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 question mark indicates that the status of a component is unknown.

3 Make a selection to view more information about an issue.

Option	Description
Components	Displays information about service components. Click the **Connection Servers**, **Gateway Servers**, **Event Database**, **View Composer Servers**, or **True SSO** tabs to view information about service components and perform troubleshooting tasks. Select a component to perform the following tasks: ■ View status, name, version, and other details. ■ If you select a Connection Server, click the **View Services Status** tab to view information about gateway services. ■ If you select a Connection Server, click the **View Sessions Detail** tab to view information about Connection Server sessions.
RDS Farms	Displays information about farms. Click a farm ID to view more information about the farm including the RDS hosts that belongs to the farm.
vSphere	Displays information about components related to vSphere. Click the **Datastores**, **ESX Hosts**, and **vCenter Servers** tabs to view information about each component.
Other Components	Click the **Domains**, **SAML 2.0**, and **License Service** tabs to view more information about each component. This section is also applicable to Horizon Composer. **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 7 pods. **Note** This section only appears when the Cloud Pod Architecture feature is enabled.

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

5 In the **Sessions** pane, click **View** to view sessions.

The Sessions page displays information about the sessions.

6 In the **Workload** pane, click **View** to view datastores.

You can select a datastore to view additional details such as current usage 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.

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.

Note If Connection Server is not configured with a secure gateway connection with the HTTP(s) secure tunnel, PCoIP secure gateway, and Blast Secure Gateway connections, then Horizon Console does not display a percentage of Connection Server sessions and lists the number of Connection Server sessions.

3 Select a Connection Server and click **View Sessions Detail** to view Connection Server sessions, maximum number of Connection Server sessions, and display protocol sessions.

Note If Connection Server is not configured with a secure gateway connection with the HTTP(s) secure tunnel, PCoIP secure gateway, and Blast Secure Gateway connections, then Horizon Console does not display the maximum session threshold because there is no threshold on the number of sessions that can connect to 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.

Understanding Horizon 7 Services

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

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

Stop and Start Horizon 7 Services

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

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

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

Prerequisites

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

Procedure

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

Services on a Connection Server Host

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

Table 9-4. Horizon Connection Server Host Services

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

Services on a Security Server

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

Table 9-5. Security Server Services

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

Table 9-5. Security Server Services (continued)

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

Change the Product License Key or License Modes in Horizon Console

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

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

Prerequisites

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

Procedure

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

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

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

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

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

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

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

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

5 Verify the license expiration date.

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

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

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

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

Monitoring License Usage

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

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

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

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

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

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

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

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

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

Reset License Usage Data

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

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

Prerequisites

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

Procedure

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

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

Join the Customer Experience Improvement Program

You can configure Horizon 7 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**.

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 Horizon 7. Skyline Collector Appliance pulls Connection Server logs for the Horizon 7 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.

Skyline Collector Appliance can pull the Connection Server logs for this administrator user to diagnose and resolve Horizon 7 issues.

Getting Started with JMP Integrated Workflow

10

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

This chapter includes the following topics:

About JMP Integrated Workflow

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

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

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

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

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

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

Get Started with JMP Integrated Workflow

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

Prerequisites

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

Procedure

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

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

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

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

   See the *Horizon 7 Installation* document.

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

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

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

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

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

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

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

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

What to do next

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

Administering JMP Settings 11

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

This chapter includes the following topics:

Configure JMP Settings for the First Time

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

Prerequisites

- Verify that the VMware Horizon JMP Server has been successfully installed and that you have its URL. See *VMware Horizon JMP Server Installation and Setup Guide* for more information.
- Obtain the administrator account credentials for Horizon 7 version 7.5 or later that you plan to use with JMP Server.
- Obtain the Active Directory credentials that must be used with the JMP Server.
- If you are assigning applications to JMP assignments, ensure that you have the URL and administrator account credentials for the VMware App Volumes Manager instance to be used. If a load balancer manages your App Volumes Manager instances that you plan to use, obtain the URL for the load balancer and use it when configuring the App Volumes Manager information.
- If you choose to use a VMware Dynamic Environment Manager configuration share, obtain its UNC path and the administrator account credentials required to access it.

Procedure

1 In the Horizon Console, click **JMP Configuration**.

2 Enter the JMP Server information.

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

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

   c Click **Save**.

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

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

   a Click the **Horizon 7** tab.

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

   c Enter your Horizon 7 service account user name and password.

   d In the **Service Account Domain** text box, enter a valid name to be used with the JMP assignments that you are creating and press **Enter**.

   e Click **Save**.

4 Enter the information for the Active Directory that you are going to use with the JMP assignments.

   a Click the **Active Directory** tab.

   b Click **New**.

   c In the **NETBIOS Name** text box, select from the list of available NetBIOS domain names.

   The DNS Domain Name and Context text boxes are updated with default values.

   d Verify that the default value that was added in the **DNS Domain Name** text box is the correct value to use. Optionally, enter another fully qualified Active Directory domain name. For example, `mycompany.com`.

   e In the **Protocol** section, select the protocol used by your Active Directory.

   f In the **Bind Username** and **Bind Password** text boxes, enter the credentials for the Bind Distinguished Name (DN) user account. For example, ***`administrator`***.

   g Modify the value in the **Context** text box, if you want to use a value different from the default.

   The value is used as the root for the Active Directory data search.

   h (Optional) Click **Advanced Properties** and modify the default Port number value.

   The default Port value is based on the protocol you selected earlier. You can modify the Port value or leave the text box blank.

i In the **Domain Controller** text box, optionally enter one or more host names or IP addresses to use for handling the Active Directory traffic.

For example, `adserver.mycompany.com, 10.111.XXX.XXX`. If the text box is left blank, the value in the **DNS Domain Name** text box is used.

j Click **Save**.

5 If you plan to use App Volumes AppStacks when creating JMP assignments, configure the App Volumes Manager that you plan to use.

a Click the **App Volumes** tab.

b Click **New**.

c In the **Name** text box, enter a name to assign to the App Volumes instance. If you leave the text box blank, the value you enter in the **App Volumes Server URL** text box is used.

d Enter a valid URL for the App Volumes Manager that you want the JMP Server pod to be associated.

Important If a load balancer manages the App Volumes Manager that you plan to use, enter the URL for that load balancer.

e Enter the App Volumes Manager or load balancer administrator account credentials that your JMP Server can use to access your App Volumes Manager.

f Enter the domain name for the App Volumes Manager service account that is to be used for the JMP assignments.

g (Optional) If you are registering more than one App Volumes Manager, use the toggle button to indicate if the App Volumes Manager you are adding is the default server to use when creating JMP assignments. You can change the instance you want to use at the time a JMP assignment is being created.

h Click **Save**.

6 If you are going to use a Dynamic Environment Manager configuration share when you create JMP assignments, add the information for it to the JMP settings.

a Click the **UEM** tab.

b Click **New**.

c Enter a value in the **File Share UNC Path** text box in the format of `\\`*`fileserver-name`*`\`*`UEM-configuration-share-pathname`*. For example, `\\FileServer\UEMConfig`.

Important Do not include `General` in the file share UNC path that you enter.

d Enter the Dynamic Environment Manager administrator account credentials to be used to connect to the Dynamic Environment Manager configuration share.

e Select from the **Active Directory** list the domain name to be used with the Dynamic Environment Manager configuration share.

Note An Active Directory can be associated with only one Dynamic Environment Manager configuration share.

f Click **Save**.

What to do next

After successfully configuring the initial JMP settings, you can now create JMP assignments. See Creating a JMP Assignment for more information.

Managing JMP Settings

You can use the Horizon Console to modify, add, or delete information for a JMP setting.

- Have the necessary information to modify the specific JMP setting.
- To modify the JMP Settings, ensure that you have the proper administrative privileges.

Edit JMP Server Settings

You can use the Horizon Console to make changes to existing JMP Server settings.

Prerequisites

- Have the necessary information to modify the specific JMP Server settings.
- Ensure you have the proper administrative privileges to log in to Horizon Console and modify the JMP Server settings

Procedure

1. In Horizon Console, select **JMP Configuration**.
2. In the JMP Settings pane, click the **JMP Server** tab.
3. Click **Edit**.
4. Enter a new **JMP Server URL**.
5. Click **Save**.

The new JMP Server URL is validated and if it is invalid, an error message appears.

Edit Horizon 7 Credentials

Use the Horizon Console to make changes to the existing Horizon 7 Connection Server credentials.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **Horizon 7** tab.

3 Click **Edit Credentials**.

4 Enter a new user name in the **Service Account User Name**, if necessary.

5 Enter a new password in the **Service Account Password**, if necessary.

6 Change the value in the **Service Account Domain**, if necessary.

7 Click **Save**.

Edit the Horizon Connection Server URL

If you want to associate existing JMP assignments to a different Horizon Connection Server, you must modify the Horizon Connection Server URL that is registered with the JMP Server settings that is associated with those JMP assignments.

There is no user interface in Horizon Console that allows you to modify the Horizon Connection Server information. You must use the SQL Server Management Studio to modify the existing Horizon Connection Server host URL in the JMP settings.

Prerequisites

- Ensure that you have the proper system administrator privileges to log in to a SQL Server Management Studio session and access to the SQL Server database that you created for JMP Server.
- Back up your SQL Server database before proceeding with the database modifications.

Procedure

1 If you are currently logged in to a Horizon Console session, log out.

2 Log in to a SQL Server Management Studio session as the sysadmin (SA) or using a user account with SA privileges.

3 Verify that the replacement Horizon Connection Server host URL that you plan to use is not already registered to another JMP Server instance.

For example, if the replacement Horizon Connection Server host URL is `new-horizon-host.com`, use the following SQL statement to verify it is not already registered.

```
SELECT * from  xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

4 If the previous SQL statement did not return any results, proceed to the next step. Otherwise, use the following statement to delete the information for the existing Horizon Connection Server host.

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

5 Update the existing JMP Server settings using the following statements, where `new-horizon-server-host.com` is the URL of the replacement Horizon Connection Server host and the `old-horizon-host.com` is the URL of currently registered Horizon Connection Server host.

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
    AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

6 Log in to Horizon Console using the new Horizon Connection Server URL and verify that the new Horizon Connection Server host is now associated with your existing JMP assignments that were previously associated with the old Horizon Connection Server host.

Add Active Directory Domains

If you need to add another Active Directory domain after setting the initial one, use the Horizon Console.

Procedure

1 In Horizon Console, click **JMP Configuration**.

2 Click the **Active Directory** tab and click **Add**.

3 In the **NETBIOS Name** text box, select from the list of available NetBIOS domain names.

The DNS Domain Name and Context text boxes are updated with default values.

4 In the **DNS Domain Name** text field, verify the default value added after the NETBIOS Name was updated. Optionally, enter another fully qualified Active Directory domain name. For example, `mycompany.com`.

5 In the **Protocol** section, select the protocol used by your Active Directory.

6 In the **Bind Username** and **Bind Password** text fields, enter the credentials for the Bind Distinguished Name (DN) user account, such as Administrator.

7 Modify the value in the **Context** text field, if you want to use a value different from the default.

8 (Optional) Click **Advanced Properties** and modify the default Port number value.

The default Port value is based on the protocol you selected earlier. You can modify the Port value or leave the text field blank.

9 In the **Domain Controller** text field, optionally enter one or more host names or IP addresses to use for handling the Active Directory traffic.

10 Click **Save**.

Information about the newly added Active Directory domain appears in the Active Directory table.

Edit Active Directory Domain Information

If certain information has changed since you initially configured the JMP settings, use the Horizon Console to modify the Active Directory domain settings information.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **Active Directory** tab.
3. Select one of the rows in the table of Active Directory domains and click **Edit**.
4. Modify the Active Directory information that has to be updated.
5. Click **Save**.

Delete Active Directory Domain Information

Use Horizon Console if you must delete existing Active Directory (AD) domain settings information.

You can only delete information about a registered Active Directory domain from a JMP setting if that domain is not in use by any existing JMP assignments.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **Active Directory** tab.
3. Select the table row for the Active Directory domain that you want to delete from JMP Settings.
4. In the delete confirmation dialog box appears, read the message and click **Delete** to confirm that you do want to delete this Active Directory domain information.

If there are no JMP assignments that use the Active Directory domain, it is removed.

If the Active Directory domain is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the Active Directory domain. You can delete the domain information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Add App Volumes Information

Use Horizon Console to add information for any additional App Volumes Managers that can be used when creating JMP assignments.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **App Volumes** tab and click **Add**.

   The **Add App Volumes Instance** dialog box appears.

3 In the **Name** text box, enter a unique name to assign to the App Volumes instance. If you leave the text box blank, the value you enter in the **App Volumes Server URL** text box is used.

4 In the **App Volumes Server URL** text box, enter a valid URL for the App Volumes Manager that you want to associate with your JMP Server. If a load balancer manages the App Volumes Manager that you are adding, enter the URL for that load balancer.

Note If the App Volumes Managers you have added are connected to different SQL databases, information about the App Volumes Manager that you add appears in the App Volumes tab. If the App Volumes Managers are connected to the same SQL database, only the information about the previously registered App Volumes Manager appears on the App Volumes tab.

5 Enter the App Volumes administrator user name and password that your JMP Server can use to access your App Volumes Manager.

6 Enter the domain name for the App Volumes service account that is used for the JMP assignments.

7 To make the App Volumes Manager that you are currently adding as the default App Volumes Manager server to use when JMP assignments are created, click the toggle button. You can change the server you want to use at the time a JMP assignment is being created.

The toggle button changes to the blue color with a **Yes** label.

8 Click **Save**.

Edit the App Volumes Instance Information

If you must modify existing information about the App Volumes instance that is being used by the JMP assignments, use the Horizon Console to modify the information.

Procedure

1 In Horizon Console, click **JMP Configuration**.

2 Click the **App Volumes** tab and select the table row for the App Volumes instance that you want to modify.

3 Click **Edit**.

The **Add App Volumes Instance** dialog box appears.

4 Modify the App Volumes instance information that has to be updated.

5 Click **Save**.

Delete App Volumes Instance Information

Use Horizon Console if you must delete existing settings information about an App Volumes instance.

You can only delete information about a registered App Volumes instance from a JMP setting if that instance is not being used by any JMP assignments.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **App Volumes** tab.
3. Select the row for the App Volumes instance information that you want to delete from the JMP Settings.
4. Click **Delete** to confirm that you do want to delete this App Volumes instance information.

If there are no JMP assignments that use the App Volumes instance, it is removed.

If the App Volumes instance is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the App Volumes instance. You can delete the App Volumes instance information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Add Dynamic Environment Manager Configuration Share Information

Use the Horizon Console if you must add another Dynamic Environment Manager configuration share after setting the initial one.

You can add only one Dynamic Environment Manager configuration share per AD domain. So, the configuration share that you are about to add cannot have the same IP or DNS address as the configuration shares that are already included in your JMP server settings.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **UEM** tab and click **Add**.

   The **Add UEM File Share** dialog box appears.
3. Enter a value in the **File Share UNC Path** text box in the format of `\\server-name\UEM-configuration-share-pathname`.

   For example, if the configuration share location is `\\<IP-address>\uemshare\config\general\FlexRepository\..`, the path you need to enter in the **File Share UNC Path** text box is **`\\<IP-address>\uemshare\config`**.
4. Enter the Dynamic Environment Manager user name and password that must be used to connect to the Dynamic Environment Manager configuration file share.
5. From the **Active Directory** list, select the domain name to use with the Dynamic Environment Manager configuration file share.

   Note An Active Directory can be associated with only one Dynamic Environment Manager configuration file share.
6. Click **Save**.

The information about the Dynamic Environment Manager configuration file share is added to the JMP settings and a new row is added to the table in the **UEM** tab.

Edit the Dynamic Environment Manager Configuration File Share Information

Use the Horizon Console if you must modify existing information about the Dynamic Environment Manager configuration file share that is being used by the JMP assignments.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **UEM** tab and from the table of existing information, select the row for the Dynamic Environment Manager configuration file share that you want to modify.
3. Click **Edit**.

   The **Edit UEM File Share** dialog box appears.
4. Modify the Dynamic Environment Manager configuration file share information that has to be updated.
5. Click **Save**.

Delete Dynamic Environment Manager Configuration Share Information

Use Horizon Console if you must delete existing settings information about a Dynamic Environment Manager configuration share.

You can only delete information about a registered Dynamic Environment Manager configuration share from a JMP setting if that configuration share is not being used by any JMP assignments.

Procedure

1. In Horizon Console, click **JMP Configuration**.
2. Click the **UEM** tab.
3. Select the row for the Dynamic Environment Manager configuration share information that you want to delete from JMP Settings.
4. Click **Delete** to confirm that you do want to delete this Dynamic Environment Manager configuration share information.

If there are no JMP assignments that use the Dynamic Environment Manager configuration share, it is removed.

If the Dynamic Environment Manager configuration share is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the Dynamic Environment Manager configuration share. You can delete the Dynamic Environment Manager configuration share information only after you remove it from the JMP assignments or delete those JMP assignments that use it.

Administering JMP Assignments 12

After you install theJMP Server and configure the JMP settings, you can begin using the JMP Integrated Workflow features to create, modify, duplicate, or delete JMP assignments.

You must first install JMP Server and configure the JMP settings before you can start creating JMP assignments. See *VMware Horizon JMP Server Installation and Setup Guide* and Configure JMP Settings for the First Time for more information.

Ensure that the following pre-requisites are met before you create, edit, duplicate, or delete JMP assignments.

- Verify that the Horizon 7 instance that is registered with the JMP setting is up and running.
- Ensure that there is at least one Active Directory domain registered with the JMP setting.
- Verify that the App Volumes instance that you registered with the JMP setting is up and running.
- Verify that the Dynamic Environment Manager configuration share defined in the JMP setting is up and running.

Note Global entitlements are not supported.

When you are attempting to create, edit, duplicate, or delete a JMP assignment, you might receive a message saying that the attempted action did not complete successfully. For example, some problems might be encountered while attempting to reach one of the underlying JMP technology components and the assignment validation fails to complete successfully. On the JMP Assignment summary screen, you can try to correct the problem by selecting one of the following options.

- Click **Edit** to correct the issues manually.
- Click **Repair** to have the JMP Server attempt to fix the issues found on the current JMP assignment.
- Click **Force Delete** to remove the JMP assignment completely.

This chapter includes the following topics:

Creating a JMP Assignment

Using Horizon Console, you can create JMP assignments, which you use to create desktop workspaces for users or group of users.

You select the Horizon desktops pools, App Volumes AppStacks, and User Environment Manager settings to define a JMP assignment.

Prerequisites

Ensure that the pre-requisites listed in Chapter 12 Administering JMP Assignments have been met.

Procedure

1. In Horizon Console, click **Assignments (JMP)**.
2. Click **New**.
3. In the **Users** tab of the New Assignment wizard, enter a couple of characters next to the Active Directory drop list and select the users or group of users to include in the new JMP assignment .

   Your selection is added in the Selected Users/Groups section.
4. Click **Next**.
5. In the **Desktops** tab, select the desktop pool you want to include in the JMP assignment, and click **Next**.
6. In the **Applications** tab, click the check box next to the name of the application that you want to include in the JMP assignment. When done with your selection, click **Next**.
7. In the **User Environment** tab, decide whether you are going to configure the JMP assignment with any of the available user environment settings.
   - With **Disable UEM Settings?** set to **No**, clicking **Skip** means that the User Environment Manager assignment file is not going to be saved to the User Environment Manager configuration share. All the User Environment Manager settings are going to be applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.
   - With **Disable UEM Settings?** set to **No**, select the user environment settings that you want applied to the JMP assignment being created. Clicking **Next** creates the User Environment Manager assignment file with the selected user environment settings. The selected settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.
   - With **Disable UEM settings?** set to **Yes**, the list of available user environment settings are removed from view. When you click **Next**, an empty assignment file is written to the User Environment Manager configuration share. Disabling User Environment Manager settings ensures that no user environment settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently creating.
8. In the **Definitions** tab, accept the default name for the JMP assignment or replace the name with another, and optionally add a description.

9 In the **AppStack Attach** drop list, select when the AppStack is to be attached to the JMP assignment and click **Next**.

10 In the **Summary** tab, review the details for the new assignment. If they are acceptable, click **Submit**. If changes must be made, click **Back** to make the adjustments.

The new JMP assignment is queued for storage into the JMP database and is added to the list of assignments in the JMP Assignments pane. After the JMP assignment is successfully added to the JMP database, the status changes from the Pending state. It becomes selectable from the JMP assignment list so you can edit, duplicate, or delete it.

You can also verify the assignments or entitlements that were created for the new JMP assignment using the following information.

- To verify information about the Horizon desktop pool created for the JMP assignment, use Horizon Console. Select **Inventory > Desktops** and locate the desktop pool created by JMP Server.
- To view the AppStacks information created by JMP Server for the new JMP assignment, use the App Volumes Manager console. Select **Volumes > AppStacks** and locate the AppStacks created by JMP Server.
- To verify the user environment settings you configured for the JMP assignment, use the Dynamic Environment Manager Management Console and click the **User Environment** tab. From the left-side pane, select the user environment setting used by the JMP assignment and click the **Assignments** tab from the resulting dialog box to view the JMP assignment information for that user environment setting.

Editing a JMP Assignment

You might need to modify an existing JMP assignment due to changes with the components that were used to define it. You can use Horizon Console to make the necessary changes to the JMP assignment.

Prerequisites

- Ensure that the pre-requisites listed in Chapter 12 Administering JMP Assignments have been met.
- The JMP assignment you plan to edit must not be in a "Pending" state.

Procedure

1 In Horizon Console, click **Assignments (JMP)**.

2 Select the JMP assignment you want to edit either by clicking the check box or the JMP assignment's name in the list.

3 Click **Edit**.

4 In the Edit Assignment wizard, modify the current settings.

Click **Cancel** if you want to discontinue at any point during the editing process.

a If you want to remove any of the currently selected users or groups, click the delete icon (**X**).

b Click **Next**.

c In the **Desktops** tab, select a desktop pool that you want included in the JMP assignment. Click **Next**.

d In the **Applications** tab, select the available applications that you want added to the JMP assignment or deselect the ones that were previously selected. Click **Next**.

e In the **User Environment** tab, decide whether you are going to configure the JMP assignment with any of the available user environment settings.

- With **Disable UEM Settings?** set to **No**, clicking **Skip** means that the User Environment Manager assignment file is not going to be saved to the User Environment Manager configuration share. All the User Environment Manager settings are going to be applied on the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.
- With **Disable UEM Settings?** set to **No**, select the user environment settings that you want applied to the JMP assignment being created. Clicking **Next** creates the User Environment Manager assignment file with the selected user environment settings. The selected settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.
- With **Disable UEM settings?** set to **Yes**, the list of available user environment settings are removed from view. When you click **Next**, an empty assignment file is written to the User Environment Manager configuration share. Disabling User Environment Manager settings ensures that no user environment settings are applied to the virtual desktop workspaces created for the users using the JMP assignment you are currently editing.

f In the **Definitions** tab, if applicable, modify the current values in the **Name**, **Description**, or when to attach the AppStack to the JMP assignment.

g Click **Next**.

h Review the summary of the changes you made and click **Submit** to save the modifications.

If successful, the changes are saved. If there are any problems encountered, additional information is provided and any possible action that you can take are displayed.

Duplicating a JMP Assignment

You can create JMP assignments more quickly by duplicating existing JMP assignments that are similar to what you want to create.

Prerequisites

- Ensure that the pre-requisites listed in Chapter 12 Administering JMP Assignments have been met.
- The JMP assignment you plan to duplicate must not be in a "Pending" or "Error" state.

Procedure

1. From Horizon Console, select **Assignments (JMP)**.
2. Select the JMP assignment you want to duplicate and click **Duplicate**.
3. In the New Assignment wizard, modify the duplicated JMP assignment as needed.
   a. Select new users or groups, or remove any of the currently selected users or groups. Click **Next**.
   b. In the Desktops pane, select a new desktop pool or remove any of the desktop pools that was included in the duplicated JMP assignment. Click **Next**.
   c. Select additional applications to include in the new JMP assignment and deselect ones that are currently selected. Click **Next**.
   d. In the User Environment pane, select the User Environment Manager setting you want to apply to the new JMP assignment. Click **Next**.
   e. In the Definitions name, replace the default name created, if you want. Add a description and specify when you want the AppStack to be attached to the new JMP assignment.
   f. Click **Next** and review the summary of the details of the new JMP assignment.
   g. If the information is satisfactory, click **Submit**. Otherwise, click **Back** to make any corrections.

The new JMP assignment is validated, which can take some time. After it is successfully validated, the newly created JMP assignment is added to the list on the JMP Assignments pane. When you point over its name, you see that it is in a pending state until it is successfully saved to the JMP database. After the JMP assignment is no longer in a pending state, you can take any additional action on the assignment.

Deleting a JMP Assignment

Use the Horizon Console to delete a JMP assignment.

When a JMP assignment is deleted, the Horizon pool entitlement, AppStack assignment, and UEM entitlement associated with the JMP assignment are deleted. However, if the Horizon pool entitlement or AppStack assignment used by the JMP assignment existed before the JMP assignment creation, they are not deleted. After you delete a JMP assignment, it no longer applies to users or desktops.

Prerequisites

- Verify that the pre-requisites listed in Chapter 12 Administering JMP Assignments have been met.
- The JMP assignment you plan to delete must not be in a "Pending" state.

Procedure

1. In Horizon Console, click **Assignments (JMP)**.

2 In the JMP Assignments pane, select one or more of the JMP assignments and click **Delete**.

3 In the confirmation dialog box, click **Delete** to confirm that you want to delete the assignment permanently.

If successful, the Horizon pool entitlement is removed from the JMP database and removed from the list in the JMP Assignments pane.

If a part of the delete operation fails, the JMP assignment is not deleted. Clicking the status indicators can provide more information on why the delete operation failed.

Configuring Event Reporting in Horizon Console

13

You can create an event database to record information about Horizon 7 events. In addition, if you use a Syslog server, you can configure Connection Server to send events to a Syslog server or create a flat file of events written in `Syslog` format.

This chapter includes the following topics:

Add a Database and Database User for Horizon 7 Events in Horizon Console

You create an event database by adding it to an existing database server. You can then use reporting software to analyze the events in the database.

Deploy the database server for the event database on a dedicated server, so that event logging activity does not affect provisioning and other activities that are critical for Horizon 7 deployments.

Note You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server or Oracle database server on a system that a Connection Server instance has access to.

  For the most up-to-date information about supported databases, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. For **Solution/Database Interoperability**, after you select the product and version, for the Add Database step, to see a list of all supported databases, select **Any** and click **Add**.

- Verify that you have the required database privileges to create a database and user on the database server.

- If you are not familiar with the procedure to create databases on Microsoft SQL Server database servers, see "Add a View Composer Database to the SQL Server," in the *Horizon 7 Installation* document.
- If you are not familiar with the procedure to create databases on Oracle database servers, see "Add a View Composer Database to Oracle 12c or 11g," in the *Horizon 7 Installation* document.

Procedure

1. Add a database to the server and give it a descriptive name such as HorizonEvents.

   For an Oracle 12c or Oracle 11g database, also provide an Oracle System Identifier (SID), which you use when you configure the event database in Horizon Console.
2. Add a user for this database that has permission to create tables, views, and, Oracle triggers and sequences, and permission to read from and write to these objects.

   For a Microsoft SQL Server database, do not use the Integrated Windows Authentication security model method of authentication. Verify that you use the SQL Server Authentication method of authentication.

The database is created, but the schema is not installed until you configure the database in Horizon Console.

What to do next

Follow the instructions in Configure the Event Database in Horizon Console.

Prepare an SQL Server Database for Event Reporting in Horizon Console

Before you can use Horizon Console to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites

- Create an SQL Server database for event reporting. See Add a Database and Database User for Horizon 7 Events in Horizon Console.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure

1. Open SQL Server Configuration Manager and expand **SQL Server *YYYY* Network Configuration**.
2. Select **Protocols for *server_name***.
3. In the list of protocols, right-click **TCP/IP** and select **Properties.**
4. Set the **Enabled** property to **Yes.**

5 Verify that a port is assigned or, if necessary, assign one.

   For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.

6 Verify that this port is not blocked by a firewall.

What to do next

Use Horizon Console to connect the database to Connection Server. Follow the instructions in Configure the Event Database in Horizon Console.

Configure the Event Database in Horizon Console

The event database stores information about Horizon 7 events as records in a database rather than in a log file.

You configure an event database after installing a Connection Server instance. You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

Note The security of the database connection between the Connection Server instance and an external database is the responsibility of the administrator, although event traffic is limited to information about the health of the Horizon 7 environment. If you want to take extra precautions, you can secure this channel through IPSec or other means, or you can deploy the database locally on the Connection Server computer.

You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *Horizon 7 Integration* document.

You can also generate Horizon 7 events in `Syslog` format so that the event data can be accessible to third-party analytics software. You use the `vdmadmin` command with the `-I` option to record Horizon 7 event messages in `Syslog` format in event log files. See "Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option" in the *Horizon 7 Administration* document.

Prerequisites

You need the following information to configure an event database:

- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server or Oracle.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See Add a Database and Database User for Horizon 7 Events in Horizon Console.

  For an Oracle 12c or 11g database, you must use the Oracle System Identifier (SID) as the database name when you configure the event database in Horizon Console.

- The username and password of the user you created for this database. See Add a Database and Database User for Horizon 7 Events in Horizon Console.

  Use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.

- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among Horizon 7 installations.

  Note You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

Procedure

1. In Horizon Console, select **Settings > Event Configuration**.
2. In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.

   To clear the event database information, click **Clear**.
3. (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

   These settings pertain to the length of time the events are listed in the Horizon Console interface. After this time, the events are only available in the historical database tables.
4. Select **Monitoring > Events** to verify that the connection to the event database is successful.

   If the connection is unsuccessful, an error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

Configure Event Logging to File or Syslog Server in Horizon Console

You can generate Horizon 7 events in `Syslog` format so that the event data can be accessible to analytics software.

You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

If you enable file-based logging of events, events are accumulated in a local log file. If you specify a file share, these log files are moved to that share.

- The maximum size of the local directory for event logs, including closed log files, before the oldest files are deleted, is 300MB. The default destination of the Syslog output is `%PROGRAMDATA%\VMware\VDM\events\`.

- Use a UNC path to save log files for a long-term record of events, or if you do not have a Syslog server or event database, or if your current Syslog server does not meet your needs.

You can alternatively use a `vdmadmin` command to configure file-based logging of events in Syslog format. See the topic about generating Horizon 7 event log messages in Syslog format using the `–I` option of the `vdmadmin` command, in the *Horizon 7 Administration* document.

Important When sending to a Syslog server, Syslog data is sent across the network without software-based encryption, and might contain sensitive data, such as user names. VMware recommends using link-layer security, such as IPSEC, to avoid the possibility of this data being monitored on the network.

Prerequisites

You need the following information to configure Connection Server so that events can be recorded in Syslog format or sent to a Syslog server, or both:

- If you plan to use a Syslog server to listen for the Horizon 7 events on a UDP port, you must have the DNS name or IP address of the Syslog server and the UDP port number. The default UDP port number is 514.
- If you plan to collect logs in a flat-file format, you must have the UNC path to the file share and folder in which to store the log files, and you must have the user name, domain name, and password of an account that has permission to write to the file share.

Procedure

1. In Horizon Console, select **Settings > Event Configuration**.
2. (Optional) In the **Syslog** area, to configure Connection Server to send events to a Syslog server, click **Add** below **Send to syslog servers**, and supply the server name or IP address and the UDP port number.
3. (Optional) In the **Events to File System** area, choose whether or not to enable event log messages to be generated and stored in Syslog format in log files.

Option	Description
Always	Always generate and store event log messages in Syslog format in log files.
Log to file on error (default)	Log audit events to a log file when there is a problem writing events to the event database or the Syslog server. This option is enabled by default.
Never	Never generate and store event log messages in Syslog format in log files.

The log files are retained locally unless you specify a UNC path to a file share.

4 (Optional) To store the Horizon 7 event log messages on a file share, click **Add** below **Copy to location**, and supply the UNC path to the file share and folder in which to store the log files, along with the user name, domain name, and password of an account that has permission to write to the file share.

An example of a UNC path is:

```
\\syslog-server\folder\file
```

Monitor Events in Horizon 7

The event database stores information about events that occur in the Connection Server host or group, Horizon Agent, and Horizon Console, and notifies you of the number of events on the dashboard. You can examine the events in detail on the **Events** page.

Note Events are listed in the Horizon Console interface for a limited time period. After this time, the events are only available in the historical database tables. You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *Horizon 7 Integration* document.

Note If the event database becomes unavailable, Horizon 7 maintains the audit trail of the events that occur during this period of unavailability and saves them to event database once it becomes available. You must restart the event database and Connection Server to view these events in the Horizon Console interface.

In addition to monitoring events in Horizon Console, you can generate Horizon 7 events in `Syslog` format so that the event data can be accessible to analytics software. See Configure Event Logging to File or Syslog Server in Horizon Console and "Generating Horizon 7 Event Log Messages in Syslog Format Using the -l Option," in the *Horizon 7 Installation* document.

If you configure an event database for multiple Connection Servers, Horizon Console displays the events for all Connection Servers on the **Events** page. Horizon Console filters events based on the tasks that you perform and displays these events on relevant pages such as the **Desktop Pools** or **Application Pools** pages.

Prerequisites

Create and configure the event database as described in the *Horizon 7 Installation* document.

Procedure

1 In Horizon Console, select **Monitor > Events**.

2 (Optional) On the **Events** page, you can select the time range of the events, apply filtering to the events, and sort the listed events by one or more of the columns.

What to do next

In Horizon Console, navigate to a desktop or application pool, virtual machine, persistent disk, or a user or group and click the **Events** tab to view specific events.

Horizon 7 Event Messages

Horizon 7 reports events whenever the state of the system changes or it encounters a problem. You can use the information in the event messages to take the appropriate action.

The following table shows the types of events that Horizon 7 reports.

Table 13-1. Types of Event Reported by Horizon 7

Event Type	Description
Audit Failure or Audit Success	Reports the failure or success of a change that an administrator or user makes to the operation or configuration of Horizon 7.
Error	Reports a failed operation by Horizon 7.
Information	Reports normal operations within Horizon 7.
Warning	Reports minor problems with operations or configuration settings that might lead to more serious problems over time.

You might need to take some action if you see messages that are associated with Audit Failure, Error, or Warning events. You do not need to take any action for Audit Success or Information events.

Using Horizon Help Desk Tool in Horizon Console

14

Horizon Help Desk Tool is a Web application that you can use to get the status of Horizon 7 user sessions and to perform troubleshooting and maintenance operations.

In Horizon Help Desk Tool, you can look up user sessions to troubleshoot problems and perform desktop maintenance operations such as restart or reset desktops.

To configure Horizon Help Desk Tool, you must meet the following requirements:

- Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon 7. To verify that you have the correct license, see the *Horizon 7 Administration* document.
- An event database to store information about Horizon 7 components. For more information about configuring an event database, see the *Horizon 7 Administration* document.
- The Help Desk Administrator role or the Help Desk Administrator (Read Only) role to log in to Horizon Help Desk Tool. For more information on these roles, see the *Horizon 7 Administration* document.
- Enable the timing profiler on each Connection Server instance to view 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}
  ```

This chapter includes the following topics:

Start Horizon Help Desk Tool in Horizon Console

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

Procedure

1 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 14-1. 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 14-2. 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.
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 14-3. 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 14-4. Activities

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

Session Details for Horizon Help Desk Tool

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

Horizon Client

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

Note If you upgraded Horizon Agent, you must also upgrade Horizon Client to the latest version. Else, no version is displayed for Horizon Client. For more information about upgrading Horizon Client, see the *Horizon 7 Upgrades* document.

VM

Displays information about virtual desktops or published desktops.

Table 14-5. 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 14-6. PCoIP Display Protocol Details

Option	Description
Tx Bandwidth	The transmission bandwidth, in kilobits per second, in a PCoIP session.
Frame Rate	The frame rate, in frames per second, in a PCoIP session.

Table 14-6. PCoIP Display Protocol Details (continued)

Option	Description
Packet Loss	Percentage of packet loss in a PCoIP session.
Skype Status	The Skype for Business status in a PCoIP session. ■ Optimized ■ Fallback ■ Optimized (version-mismatch) ■ Fallback (version-mismatch) ■ Connecting ■ Disconnected ■ Undefined This option appears as N/A for Linux desktop sessions.

Table 14-7. Blast Display Protocol Details

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

CPU and Memory Usage and Network and Disk Performance

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

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

Table 14-8. 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 14-9. 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 14-10. 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 14-11. 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 14-12. Session Logon Segments

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

Use the following guidelines when you use the information in logon segments for troubleshooting:

- If the session is a new virtual desktop session, all the logon segments appear. If no global policy is configured, the **GPO Load** logon segment time is 0.
- If the virtual desktop session is a reconnected session from a disconnected session, the **Logon Duration**, **Interactive**, and **Brokering** logon segments appear.
- If the session is a published desktop session, the **Logon Duration**, **GPO Load**, or the **Profile load** logon segments appear. The **GPO Load** and **Profile load** logon segment appear for new sessions. If these logon segments do not appear for new sessions, you must restart the RDS host.
- If the session is a Linux desktop session, the **GPO Load** and **Profile load** segments do not appear.

- Logon data might not be immediately available when the desktop session connects. The logon data appears after a few minutes.

Session Processes for Horizon Help Desk Tool

The session processes appear on the **Processes** tab when you click a user name in the **Computer Name** option on the **Sessions** tab.

Processes

For each session, you can view additional details about CPU and memory related processes. For example, if you notice that the CPU and memory usage for a session is abnormally high, you can view the details for the process on the **Processes** tab.

For RDS host sessions, the **Processes** tab displays the current RDS host session processes started by the current user or current system process.

Table 14-13. Session Process Details

Option	Description
Process Name	Name of the session process. For example, chrome.exe.
CPU	CPU usage of the process in percent.
Memory	Memory usage of the process in KB.
Disk	Memory disk IOPs. Calculated using the following formula: (Total I/O bytes of current time) - (Total I/O bytes one second before the current time). This calculation can display a value of 0 KB per second if the Task Manager displays a positive value.
Username	User name of the user who owns the process.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Processes	Count of processes in the virtual machine
Refresh	The refresh icon refreshes the list of processes.
End Process	Ends a process that is running. **Note** You must have the Help Desk Administrator role to end a process. To end a process, select a process and click the **End Process** button. You cannot end critical processes such as Windows core processes that might be listed in the **Processes** tab. If you end a critical process, Horizon Help Desk Tool displays a message that states it cannot end the system process.

Application Status for Horizon Help Desk Tool

You can view the status and details of an application on the **Applications** tab when you click a user name in the **Computer Name** option on the **Sessions** tab. You cannot access the **Applications** tab for Linux desktop sessions.

Applications

For each application, you can view the current status and other details.

You can end an application process for the end user. To end an application process, click **End Application** and click **OK** to confirm the change.

Note The end application process can fail if the application is pending a user interaction such as unsaved data or because of other exceptions. However, Horizon Help Desk Tool does not display any success or failure message when you end an application.

Table 14-14. Application Details

Option	Description
Application	Name of the application.
Description	Description of the application.
Status	Status of the application. Displays whether the application is running or not.
Host CPU	CPU usage of the virtual machine to which the session is assigned.
Host Memory	Memory usage of the virtual machine to which the session is assigned.
Applications	List of applications that are running.
Refresh	The refresh icon refreshes the list of applications.

Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool

In Horizon Help Desk Tool, you can troubleshoot desktop or application sessions based on a user's connection status.

Prerequisites

- Start Horizon Help Desk Tool.

Procedure

1. On the user card, click the **Sessions** tab.

   A performance card appears that displays CPU and memory usage and includes information about Horizon Client, and the virtual or published desktop.

2 Choose a troubleshooting option.

Option	Action
Send Message	Sends a message to the user on the published desktop or virtual desktop. You can choose the severity of the message to include Warning, Info, or Error. Click **Send Message** and enter the type of severity and the message details, and then click **Submit**.
Remote Assistance	You can generate remote assistance tickets for connected desktop or application sessions. Administrators can use the remote assistance ticket to take control of a user's desktop and troubleshoot problems. **Note** This feature is not available for Linux desktop users. Click **Remote Assistance** and download the Help Desk ticket file. Open the ticket and wait for the ticket to be accepted by the user on the remote desktop. You can open the ticket only on a Windows desktop. After the user accepts the ticket, you can chat with the user and request control of the user's desktop. **Note** The Help Desk remote assistance feature is based on Microsoft Remote Assistance. You must install Microsoft Remote Assistance and enable the Remote Assistance feature on the published desktop. Help Desk remote assistance might not start if Microsoft Remote Assistance has connection or upgrade issues. For more information, see the Microsoft Remote Assistance documentation on the Microsoft Web site.
Restart	Initiates the Windows Restart process on the virtual desktop. This feature is not available for a published desktop or application session. Click **Restart VDI**.
Disconnect	Disconnect the desktop or application session. Click **More > Disconnect**.
Log Off	Initiates the log off process for a published desktop or virtual desktop, or the log off process for an application session. Click **More > Log Off**.
Reset	Initiates a reset of the virtual machine. This feature is not available for a published desktop or application session. Click **More > Reset VM**. **Note** The user can lose unsaved work.

Using the vdmadmin Command 15

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 Horizon 7 components, and to display the details of a specific health monitor or monitor instance.

- Listing and Displaying Reports of Horizon 7 Operation Using the -I Option

  You can use the `vdmadmin` command with the `-I` option to list the available reports of Horizon 7 operation and to display the results of running one of these reports.

- Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option

  You can use the `vdmadmin` command with the `-I` option to record Horizon 7 event messages in `Syslog` format in event log files. Many third-party analytics products require flat-file `Syslog` data as input for their analytics operations.

- Assigning Dedicated Machines Using the -L Option

  You can use the `vdmadmin` command with the `-L` option to assign machines from a dedicated pool to users.

- Displaying Information About Machines Using the -M Option

  You can use the `vdmadmin` command with the `-M` option to display information about the configuration of virtual machines or physical computers.

- Reclaiming Disk Space on Virtual Machines Using the -M Option

  You can use the `vdmadmin` command with the `-M` option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.

- Configuring Domain Filters Using the -N Option

  You can use the `vdmadmin` command with the `-N` option to control the domains that Horizon 7 makes available to end users.

- Configuring Domain Filters

  You can configure domain filters to limit the domains that a Connection Server instance or security server makes available to end users.

- Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options

  You can use the `vdmadmin` command with the `-O` and `-P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.

- Configuring Clients in Kiosk Mode Using the -Q Option

  You can use the `vdmadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

- Displaying the First User of a Machine Using the -R Option

  You can use the `vdmadmin` command with the `-R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.

- Removing the Entry for a Connection Server Instance or Security Server Using the -S Option

  You can use the `vdmadmin` command with the `-S` option to remove the entry for a Connection Server instance or security server from the Horizon 7 configuration.

- Providing Secondary Credentials for Administrators Using the -T Option

  You can use the `vdmadmin` command with the `-T` option to provide Active Directory secondary credentials to administrator users.

- Displaying Information About Users Using the -U Option

  You can use the `vdmadmin` command with the `-U` option to display detailed information about users.

- Unlocking or Locking Virtual Machines Using the -V Option

  You can use the `vdmadmin` command with the `-V` option to unlock or lock virtual machines in the data center.

- Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option

  You can use the `vdmadmin` command with the `-X` option to detect and resolve LDAP entry collisions and LDAP schema collisions on replicated Connection Server instances in a group. You can also use this option to detect and resolve LDAP schema collisions in a Cloud Pod Architecture environment.

vdmadmin Command Usage

The syntax of the `vdmadmin` command controls its operation.

Use the following form of the `vdmadmin` command from a Windows command prompt.

```
vdmadmin command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option.

By default, the path to the `vdmadmin` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid having to enter the path on the command line, add the path to your *PATH* environment variable.

- vdmadmin Command Authentication

  You must run the `vdmadmin` command as a user who is in the **Administrators** role for a specified action to succeed.

- vdmadmin Command Output Format

  Some `vdmadmin` command options allow you to specify the format of the output information.

- vdmadmin Command Options

  You use the command options of the `vdmadmin` command to specify the operation that you want it to perform.

vdmadmin Command Authentication

You must run the `vdmadmin` command as a user who is in the **Administrators** role for a specified action to succeed.

You can use Horizon Administrator to assign the **Administrators** role to a user. See #unique_9.

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 15-1. Options for Selecting Output Format

Option	Description
–csv	Formats the output as comma-separated values.
–n	Display the output using ASCII (UTF-8) characters. This is the default character set for comma-separated values and plain text output.
–w	Display the output using Unicode (UTF-16) characters. This is the default character set for XML output.
–xml	Formats the output as XML.

vdmadmin Command Options

You use the command options of the vdmadmin command to specify the operation that you want it to perform.

The following table shows the command options that you can use with the vdmadmin command to control and examine the operation of Horizon 7.

Table 15-2. Vdmadmin Command Options

Option	Description
–A	Administers the information that Horizon Agent records in its log files. See Configuring Logging in Horizon Agent Using the -A Option. Overrides the IP address reported by Horizon Agent. See Overriding IP Addresses Using the -A Option
–C	Sets the name for a Connection Server group. See #unique_186.
–F	Updates the Foreign Security Principals (FSPs) in Active Directory for all users or for specified users. See Updating Foreign Security Principals Using the -F Option.
–H	Displays health information about Horizon 7 services. See Listing and Displaying Health Monitors Using the -H Option.
–I	Generates reports about Horizon 7 operation. See Listing and Displaying Reports of Horizon 7 Operation Using the -I Option.
–L	Assigns a dedicated desktop to a user or removes an assignment. See Assigning Dedicated Machines Using the -L Option.
–M	Displays information about a virtual machine or physical computer. See Displaying Information About Machines Using the -M Option.
–N	Configures the domains that a Connection Server instance or group makes available to Horizon Client. See Configuring Domain Filters Using the -N Option.
–O	Displays the remote desktops that are assigned to users who are no longer entitled to those desktops. See Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options.
–P	Displays the user policies that are associated with the remote desktops of unentitled users. See Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options.
–Q	Configures the account in Active Directory account and Horizon 7 configuration of a client device in kiosk mode. See Configuring Clients in Kiosk Mode Using the -Q Option.
–R	Reports the first user who accessed a remote desktop. See Displaying the First User of a Machine Using the -R Option.
–S	Removes a configuration entry for a Connection Server instance from the configuration of Horizon 7. See Removing the Entry for a Connection Server Instance or Security Server Using the -S Option.
–T	Provides Active Directory secondary credentials to administrator users. See Providing Secondary Credentials for Administrators Using the -T Option.
–U	Displays information about a user including their remote desktop entitlements and ThinApp assignments, and Administrator roles. See Displaying Information About Users Using the -U Option.
–V	Unlocks or locks virtual machines. See Unlocking or Locking Virtual Machines Using the -V Option.
–X	Detects and resolves duplicated LDAP entries on replicated Connection Server instances. See Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option.

Configuring Logging in Horizon Agent Using the -A Option

You can use the `vdmadmin` command with the `–A` option to configure logging by Horizon Agent.

Syntax

```
vdmadmin -A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getlogfile logfile -outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

Usage Notes

To assist VMware Technical Support in troubleshooting Horizon Agent, you can create a Data Collection Tool (DCT) bundle. You can also change the logging level, display the version and status of Horizon Agent, and save individual log files to your local disk.

Options

The following table shows the options that you can specify to configure logging in Horizon Agent.

Table 15-3. 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 15-3. 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 15-4. Options for Overriding IP Addresses

Option	Description
`-d` *desktop*	Specifies the desktop pool.
`-i` *ip_or_dns*	Specifies the IP address or resolvable domain name in DNS.
`-m` *machine*	Specifies the name of the machine in a desktop pool.
`-override`	Specifies an operation for overriding IP addresses.
`-r`	Removes an overridden IP address.

Examples

Override the IP address for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

Display the IP addresses that are defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -list -d dtpool2 -m machine2
```

Remove the IP addresses that is defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -r -d dtpool2 -m machine2
```

Remove the IP addresses that are defined for the desktops in the desktop pool dtpool3.

```
vdmadmin -A -override -r -d dtpool3
```

Updating Foreign Security Principals Using the -F Option

You can use the vdmadmin command with the –F option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.

Syntax

```
vdmadmin –F [–b authentication_arguments] [–u domain\user]
```

Usage Notes

If you trust domains outside of your local domains, you allow access by security principals in the external domains to the local domains' resources. Active Directory uses FSPs to represent security principals in trusted external domains. You might want to update the FSPs of users if you modify the list of trusted external domains.

Options

The –u option specifies the name and domain of the user whose FSP you want to update. If you do not specify this option, the command updates the FSPs of all users in Active Directory.

Examples

Update the FSP of the user Jim in the EXTERNAL domain.

```
vdmadmin –F –u EXTERNAL\Jim
```

Update the FSPs of all users in Active Directory.

```
vdmadmin –F
```

Listing and Displaying Health Monitors Using the -H Option

You can use the vdmadmin command –H to list the existing health monitors, to monitor instances for Horizon 7 components, and to display the details of a specific health monitor or monitor instance.

Syntax

```
vdmadmin –H [–b authentication_arguments] –list –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –list –monitorid monitor_id –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –monitorid monitor_id –instanceid instance_id –xml [–w | –n]
```

Usage Notes

The following table shows the health monitors that Horizon 7 uses to monitor the health of its components.

Table 15-5. Health Monitors

Monitor	Description
CBMonitor	Monitors the health of Connection Server instances.
DBMonitor	Monitors the health of the events database.
DomainMonitor	Monitors the health of the Connection Server host's local domain and all trusted domains.
SGMonitor	Monitors the health of security gateway services and security servers.
VCMonitor	Monitors the health of vCenter servers.

If a component has several instances, Horizon 7 creates a separate monitor instance to monitor each instance of the component.

The command outputs all information about health monitors and monitor instances in XML format.

Options

The following table shows the options that you can specify to list and display health monitors.

Table 15-6. Options for Listing and Displaying Health Monitors

Option	Description
`–instanceid` *instance_id*	Specifies a health monitor instance
`–list`	Displays the existing health monitors if a health monitor ID is not specified.
`–list –monitorid` *monitor_id*	Displays the monitor instances for the specified health monitor ID.
`–monitorid` *monitor_id*	Specifies a health monitor ID.

Examples

List all existing health monitors in XML using Unicode characters.

```
vdmadmin –H –list –xml
```

List all instances of the vCenter monitor (VCMonitor) in XML using ASCII characters.

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

Display the health of a specified vCenter monitor instance.

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

Listing and Displaying Reports of Horizon 7 Operation Using the -I Option

You can use the `vdmadmin` command with the `-I` option to list the available reports of Horizon 7 operation and to display the results of running one of these reports.

Syntax

```
vdmadmin -I [-b authentication_arguments] -list [-xml] [-w | -n]
```

```
vdmadmin -I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

Usage Notes

You can use the command to display the available reports and views, and to display the information that Horizon 7 has recorded for a specified report and view.

You can also use the `vdmadmin` command with the `-I` option to generate Horizon 7 log messages in `syslog` format. See Generating Horizon 7 Event Log Messages in Syslog Format Using the -I Option.

Options

The following table shows the options that you can specify to list and display reports and views.

Table 15-7. 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 Horizon 7 Event Log Messages in Syslog Format Using the -I Option

You can use the `vdmadmin` command with the `-I` option to record Horizon 7 event messages in `Syslog` format in event log files. Many third-party analytics products require flat-file `Syslog` data as input for their analytics operations.

Syntax

```
vdmadmin -I -eventSyslog -disable
```

```
vdmadmin -I -eventSyslog -enable -localOnly
```

```
vdmadmin -I -eventSyslog -enable -path path
```

```
vdmadmin -I -eventSyslog -enable -path path
 -user DomainName\username -password password
```

Usage Notes

You can use the command to generate Horizon 7 event log messages in `Syslog` format. In a `Syslog` file, Horizon 7 event log messages are formatted in key-value pairs, which makes the logging data accessible to analytics software.

You can also use the `vdmadmin` command with the `-I` option to list the available reports and views and to display the contents of a specified report. See Listing and Displaying Reports of Horizon 7 Operation Using the -I Option.

Options

You can disable or enable the `eventSyslog` option. You can direct the `Syslog` output to the local system only or to another location. Direct UDP connection to a `Syslog` server is supported with Horizon 7 5.2 or later. See "Configure Event Logging for Syslog Servers" in the *Horizon 7 Installation* document.

Table 15-8. Options for Generating Horizon 7 Event Log Messages in Syslog Format

Option	Description
`-disable`	Disables `Syslog` logging.
`-e|-enable`	Enables `Syslog` logging.
`-eventSyslog`	Specifies that Horizon 7 events are generated in `Syslog` format.
`-localOnly`	Stores the `Syslog` output on the local system only. When you use the `-localOnly` option, the default destination of the `Syslog` output is `%PROGRAMDATA%\VMware\VDM\events\`.

Table 15-8. Options for Generating Horizon 7 Event Log Messages in Syslog Format (continued)

Option	Description
`–password` *password*	Specifies the password for the user that authorizes access to the specified destination path for the `Syslog` output.
`–path`	Determines the destination UNC path for the `Syslog` output.
`–u|–user` *DomainName\username*	Specifies the domain and username that can access the destination path for the `Syslog` output.

Examples

Disable generating Horizon 7 events in `Syslog` format.

```
vdmadmin –I –eventSyslog –disable
```

Direct `Syslog` output of Horizon 7 events to the local system only.

```
vdmadmin –I –eventSyslog –enable –localOnly
```

Direct `Syslog` output of Horizon 7 events to a specified path.

```
vdmadmin –I –eventSyslog –enable –path path
```

Direct `Syslog` output of Horizon 7 events to a specified path that requires access by an authorized domain user.

```
vdmadmin –I –eventSyslog –enable –path \\logserver\share\ViewEvents –user mydomain\myuser
 –password mypassword
```

Assigning Dedicated Machines Using the -L Option

You can use the `vdmadmin` command with the `–L` option to assign machines from a dedicated pool to users.

Syntax

```
vdmadmin –L [–b authentication_arguments] –d desktop –m  machine –u domain\user
```

```
vdmadmin –L [–b authentication_arguments] –d desktop [–m machine | –u domain\user] –r
```

Usage Notes

Horizon 7 assigns machines to users when they first connect to a dedicated desktop pool. Under some circumstances, you might want to preassign machines to users. For example, you might want to prepare their system environments in advance of their initial connection. After a user connects to a remote desktop that Horizon 7 assigns from a dedicated pool, the virtual machine that hosts the desktop remains assigned to the user for the life span of the virtual machine. You can assign a user to a single machine in a dedicated pool.

You can assign a machine to any entitled user. You might want to do this when recovering from the loss of View LDAP data on a Connection Server instance, or when you want to change ownership of a particular machine.

After a user connects to a remote desktop that Horizon 7 assigns from a dedicated pool, that remote desktop remains assigned to the user for the life span of the virtual machine that hosts the desktop. You might want to remove the assignment of a machine to a user who has left the organization, who no longer requires access to the desktop, or who will use a desktop in a different desktop pool. You can also remove assignments for all users who access a desktop pool.

Note The `vdmadmin -L` command does not assign ownership to View Composer persistent disks. To assign linked-clone desktops with persistent disks to users, use the **Assign User** menu option in Horizon Administrator.

If you do use `vdmadmin -L` to assign a linked-clone desktop with a persistent disk to a user, unexpected results can occur in certain situations. For example, if you detach a persistent disk and use it to recreate a desktop, the recreated desktop is not assigned to the owner of the original desktop.

Options

The following table shows the options that you can specify to assign a desktop to a user or to remove an assignment.

Table 15-9. Options for Assigning Dedicated Desktops

Option	Description
`-d` *desktop*	Specifies the name of the desktop pool.
`-m` *machine*	Specifies the name of the virtual machine that hosts the remote desktop.
`-r`	Removes an assignment to a specified user, or all assignments to a specified machine.
`-u` *domain\user*	Specifies the login name and domain of the user.

Examples

Assign the machine machine2 in the desktop pool dtpool1 to the user Jo in the CORP domain.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Remove the assignments for the user Jo in the CORP domain to desktops in the pool dtpool1.

```
vdmadmin –L –d dtpool1 –u Corp\Jo –r
```

Remove all user assignments to the machine machine1 in the desktop pool dtpool3.

```
vdmadmin –L –d dtpool3 –m machine1 –r
```

Displaying Information About Machines Using the -M Option

You can use the `vdmadmin` command with the `–M` option to display information about the configuration of virtual machines or physical computers.

Syntax

```
vdmadmin –M [–b authentication_arguments] [–m machine | [–u domain\user][–d desktop]] [–xml | –csv] [–w | –n]
```

Usage Notes

The command displays information about a remote desktop's underlying virtual machine or physical computer.

- Display name of the machine.
- Name of the desktop pool.
- State of the machine.

  The machine state can be one of the following values: `UNDEFINED, PRE_PROVISIONED, CLONING, CLONINGERROR, CUSTOMIZING, READY, DELETING, MAINTENANCE, ERROR, LOGOUT`.

  The command does not display all dynamic machine states, such as `Connected` or `Disconnected`, that are displayed in Horizon Administrator.
- SID of the assigned user.
- Account name of the assigned user.
- Domain name of the assigned user.
- Inventory path of the virtual machine (if applicable).
- Date on which the machine was created.
- Template path of the machine (if applicable).
- URL of the vCenter Server (if applicable).

Options

The following table shows the options that you can use to specify the machine whose details you want to display.

Table 15-10. Options for Displaying Information About Machines

Option	Description
–d *desktop*	Specifies the name of the desktop pool.
–m *machine*	Specifies the name of the virtual machine.
–u *domain\user*	Specifies the login name and domain of the user.

Examples

Display information about the underlying machine for the remote desktop in the pool dtpool2 that is assigned to the user Jo in the CORP domain and format the output as XML using ASCII characters.

```
vdmadmin –M –u CORP\Jo –d dtpool2 –xml –n
```

Display information about the machine machine3 and format the output as comma-separated values.

```
vdmadmin –M –m machine3 –csv
```

Reclaiming Disk Space on Virtual Machines Using the -M Option

You can use the vdmadmin command with the –M option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.

Syntax

```
vdmadmin –M [–b authentication_arguments] –d desktop –m machine –markForSpaceReclamation
```

Usage Notes

With this option, you can initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes.

Space reclamation does not take place if you run this command when a blackout period is in effect.

The following prerequisites must be met before you can reclaim disk space by using the vdmadmin command with the –M option:

- Verify that Horizon 7 is using vCenter Server and ESXi version 5.1 or later.

- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on the virtual machine.
- Verify that the virtual machine is virtual hardware version 9 or later.
- In Horizon Administrator, verify that the **Enable space reclamation** option is selected for vCenter Server. See #unique_203.
- In Horizon Administrator, verify that the **Reclaim VM disk space** option was selected for the desktop pool. See "Reclaim Disk Space on View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.
- Verify that the virtual machine is powered on before you initiate the space reclamation operation.
- Verify that a blackout period is not in effect. See "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.

Options

Table 15-11. Options for Reclaiming Disk Space on Virtual Machines

Option	Description
`–d` *desktop*	Specifies the name of the desktop pool.
`–m` *machine*	Specifies the name of the virtual machine.
`–MarkForSpaceReclamation`	Marks the virtual machine for disk space reclamation.

Example

Marks the virtual machine `machine3` in the desktop pool `pool1` for disk space reclamation.

```
vdmadmin –M –d pool1 –m machine3 –markForSpaceReclamation
```

Configuring Domain Filters Using the -N Option

You can use the `vdmadmin` command with the `–N` option to control the domains that Horizon 7 makes available to end users.

Syntax

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -add [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

Usage Notes

Specify one of the `-exclude`, `-include`, or `-search` options to apply an operation to the exclusion list, inclusion list, or search exclusion list respectively.

If you add a domain to a search exclusion list, the domain is excluded from an automated domain search.

If you add a domain to an inclusion list, the domain is included in the results of the search.

If you add a domain to an exclusion list, the domain is excluded from the results of the search.

Options

The following table shows the options that you can specify to configure domain filters.

Table 15-12. 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.

Table 15-12. Options for Configuring Domain Filters (continued)

Option	Description
–remove	Removes a domain from a list.
–removeall	Removes all domains from a list.
–s *connsvr*	Specifies that the operation applies to the domain filters on a Connection Server instance. You can specify the Connection Server instance by its name or IP address. If you do not specify this option, any change that you make to the search configuration applies to all Connection Server instances in the group.
–search	Specifies an operation on a search exclusion list.

Examples

Add the domain FARDOM to the search exclusion list for the Connection Server instance csvr1.

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

Add the domain NEARDOM to the exclusion list for a Connection Server group.

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

Display the domain search configuration on both Connection Server instances in the group, and for the group.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

Horizon 7 limits the domain search on each Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that Horizon 7 excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

Display the domain filters in XML using ASCII characters.

```
vdmadmin –N –domains –list –xml –n
```

Display the domains that are available to Horizon 7 on the local Connection Server instance.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Display the available domains in XML using ASCII characters.

```
vdmadmin –N –domains –list –active –xml –n
```

Remove the domain NEARDOM from the exclusion list for a Connection Server group.

```
vdmadmin –N –domains –exclude –domain NEARDOM –remove
```

Remove all domains from the inclusion list for the Connection Server instance csvr1.

```
vdmadmin –N –domains –include –removeall –s csvr1
```

Configuring Domain Filters

You can configure domain filters to limit the domains that a Connection Server instance or security server makes available to end users.

Horizon 7 determines which domains are accessible by traversing trust relationships, starting with the domain in which a Connection Server instance or security server resides. For a small, well-connected set of domains, Horizon 7 can quickly determine a full list of domains, but the time that this operation takes increases as the number of domains increases or as the connectivity between the domains decreases. Horizon 7 might also include domains in the search results that you would prefer not to offer to users when they log in to their remote desktops.

If you have previously set the value of the Windows registry key that controls recursive domain enumeration (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) to false, recursive domain searching is disabled, and the Connection Server instance uses only the primary domain. To use the domain filtering feature, delete the registry key or set its value to true, and restart the system. You must do this for every Connection Server instance on which you have set this key.

The following table shows the types of domain lists that you can specify to configure domain filtering.

Table 15-13. Types of Domain List

Domain List Type	Description
Search exclusion list	Specifies the domains that Horizon 7 can traverse during an automated search. The search ignores domains that are included in the search exclusion list, and does not attempt to locate domains that the excluded domain trusts. You cannot exclude the primary domain from the search.
Exclusion list	Specifies the domains that Horizon 7 excludes from the results of a domain search. You cannot exclude the primary domain.
Inclusion list	Specifies the domains that Horizon 7 does not exclude from the results of a domain search. All other domains are removed apart from the primary domain.

The automated domain search retrieves a list of domains, excluding those domains that you specify in the search exclusion list and domains that are trusted by those excluded domains. Horizon 7 selects the first non-empty exclusion or inclusion list in this order.

1 Exclusion list configured for the Connection Server instance.

2 Exclusion list configured for the Connection Server group.

3 Inclusion list configured for the Connection Server instance.

4 Inclusion list configured for the Connection Server group

Horizon 7 applies only the first list that it selects to the search results.

If you specify a domain for inclusion, and its domain controller is not currently accessible, Horizon 7 does not include that domain in the list of active domains.

You cannot exclude the primary domain to which a Connection Server instance or security server belongs.

Example of Filtering to Include Domains

You can use an inclusion list to specify the domains that Horizon 7 does not exclude from the results of a domain search. All other domains, apart from the primary domain, are removed.

A Connection Server instance is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX domain.

Display the currently active domains for the Connection Server instance.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains appear in the list because they are trusted domains of the DEPTX domain.

Specify that the Connection Server instance should make only the YOURDOM and DEPTX domains available, in addition to the primary MYDOM domain.

```
vdmadmin –N –domains –include –domain YOURDOM –add
vdmadmin –N –domains –include –domain DEPTX –add
```

Display the currently active domains after including the YOURDOM and DEPTX domains.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 applies the include list to the results of a domain search. If the domain hierarchy is very complex or network connectivity to some domains is poor, the domain search can be slow. In such cases, use search exclusion instead.

Example of Filtering to Exclude Domains

You can use an exclusion list to specify the domains that Horizon 7 excludes from the results of a domain search.

A group of two Connection Server instances, CONSVR-1 and CONSVR-2, is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX and FARDOM domains.

The FARDOM domain is in a remote geographical location, and network connectivity to that domain is over a slow, high-latency link. There is no requirement for users in the FARDOM domain to be able to access the Connection Server group in the MYDOM domain.

Display the currently active domains for a member of the Connection Server group.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains are trusted domains of the DEPTX domain.

To improve connection performance for Horizon Client, exclude the FARDOM domain from being searched by the Connection Server group.

```
vdmadmin –N –domains –search –domain FARDOM –add
```

The command displays the currently active domains after excluding the FARDOM domain from the search.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Extend the search exclusion list to exclude the DEPTX domain and all its trusted domains from the domain search for all Connection Server instances in a group. Also, exclude the YOURDOM domain from being available on CONSVR-1.

```
vdmadmin –N –domains –search –domain DEPTX –add
vdmadmin –N –domains –exclude –domain YOURDOM –add –s CONSVR–1
```

Display the new domain search configuration.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

Horizon 7 limits the domain search on each Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that Horizon 7 excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

On CONSVR-1, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

On CONSVR-2, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options

You can use the `vdmadmin` command with the `-O` and `-P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.

Syntax

```
vdmadmin -O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

```
vdmadmin -P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

Usage Notes

If you revoke a user's entitlement to a persistent virtual machine or to a physical system, the associated remote desktop assignment is not automatically revoked. This condition might be acceptable if you have temporarily suspended a user’s account or if the user is on a sabbatical. When you reenable entitlement, the user can continue using the same virtual machine as previously. If a user has left the organization, other users cannot access the virtual machine, and it is considered to be orphaned. You might also want to examine any policies that are assigned to unentitled users.

Options

The following table shows the options that you can specify to display the virtual machines and policies of unentitled users.

Table 15-14. Options for Displaying the Machines and Policies of Unentitled Users

Option	Description
`-ld`	Orders output entries by machine.
`-lu`	Orders output entries by user.
`-noxslt`	Specifies that the default stylesheet should not be applied to the XML output.
`-xsltpath` *path*	Specifies the path to the stylesheet that is used to transform XML output.

Table 15-15. 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 15-15. XSL Stylesheets

Stylesheet File Name	Description
`unentitled-machines.xsl`	Transforms reports containing a list of unentitled virtual machines, grouped either by user or system, and which are currently assigned to a user. This is the default stylesheet.
`unentitled-policies.xsl`	Transforms reports containing a list of virtual machines with user-level policies that are applied to unentitled users.

Examples

Display the virtual machines that are assigned to unentitled users, grouped by virtual machine in text format.

```
vdmadmin -O -ld
```

Display virtual machines that are assigned to unentitled users, grouped by user, in XML format using ASCII characters.

```
vdmadmin -O -lu -xml -n
```

Apply your own stylesheet `C:\tmp\unentitled-users.xsl` and redirect the output to the file `uu-output.html`.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

Display the user policies that are associated with unentitled users' virtual machinse, grouped by desktop, in XML format using Unicode characters.

```
vdmadmin -P -ld -xml -w
```

Apply your own stylesheet `C:\tmp\unentitled-policies.xsl` and redirect the output to the file `up-output.html`.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

Configuring Clients in Kiosk Mode Using the -Q Option

You can use the `vdmadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

Syntax

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id
[-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name |
-nogroup] [-description "description_text"]
```

```
vdmadmin -Q -disable [-b authentication_arguments] -s connection_server
```

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdmadmin -Q -clientauth -getdefaults [-b authentication_arguments] [-xml]
```

```
vdmadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

```
vdmadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdmadmin -Q -clientauth -removeall [-b authentication_arguments] [-force]
```

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword |
-noexpirepassword ] [-group group_name | -nogroup]
```

```
vdmadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id
[-password "password" | -genpassword] [-description "description_text"]
```

Usage Notes

You must run the `vdmadmin` command on one of the Connection Server instances in the group that contains the Connection Server instance that clients use to connect to their remote desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all Connection Server instances in a group.

When you add a client in kiosk mode, Horizon 7 creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with the characters "custom-" or with one of the alternate strings that you can define in ADAM, and it cannot be more than 20 characters long. You should use each specified name with no more than one client device.

You can define alternate prefixes to "custom-" in the `pae-ClientAuthPrefix` multi-valued attribute under `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM on a Connection Server instance. Avoid using these prefixes with ordinary user accounts.

If you do not specify a name for a client, Horizon 7 generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with Connection Server instances that you enable to authenticate clients.

Some thin clients allow only account names that start with the characters "custom-" or "cm-" to be used with kiosk mode.

An automatically generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, you must use the `-password` option to specify the password.

If you use the `-group` option to specify a group or you have previously set a default group, Horizon 7 adds the client's account to this group. You can specify the `-nogroup` option to prevent the account being added to any group.

If you enable a Connection Server instance to authenticate clients in kiosk mode, you can optionally specify that clients must provide a password. If you disable authentication, clients cannot connect to their remote desktops.

Although you enable or disable authentication for an individual Connection Server instance, all Connection Server instances in a group share all other settings for client authentication. You need only add a client once for all Connection Server instances in a group to be capable of accepting requests from the client.

If you specify the `-requirepassword` option when enabling authentication, the Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a Connection Server instance to specify this option, such clients cannot authenticate themselves, and they fail with the error message `Unknown username or bad password`.

Options

The following table shows the options that you can specify to configure clients in kiosk mode.

Table 15-16. 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.
`-remove`	Removes the account for a client in kiosk mode.
`-removeall`	Removes the accounts of all clients in kiosk mode.

Table 15-16. Options for Configuring Clients in Kiosk Mode (continued)

Option	Description
`-requirepassword`	Specifies that clients in kiosk mode must provide passwords. Horizon 7 will not accept generated passwords for new connections.
`-s` *connection_server*	Specifies the NetBIOS name of the Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
`-setdefaults`	Sets the default values that are used for adding client accounts.
`-update`	Updates an account for a client in kiosk mode.

Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Get the current default values for clients in plain text format.

```
vdmadmin -Q -clientauth -getdefaults
```

Get the current default values for clients in XML format.

```
vdmadmin -Q -clientauth -getdefaults -xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-
ou,DC=myorg,DC=com" -group kc-grp
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -
description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin –Q –clientauth –removeall –force
```

Enable authentication of clients for the Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Disable authentication of clients for the Connection Server instance csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password, and requires the end user to provide this. The Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Displaying the First User of a Machine Using the -R Option

You can use the `vdmadmin` command with the `-R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.

Note The `vdmadmin` command with the `-R` option works only on virtual machines that are earlier than View Agent 5.1. On virtual machines that run View Agent 5.1 and later and Horizon Agent 7.0 and later versions, this option does not work. To locate the first user of a virtual machine, use the Events database to determine which users logged into the machine.

Syntax

```
vdmadmin -R -i network_address
```

Usage Notes

You cannot use the `-b` option to run this command as a privileged user. You must be logged in as a user in the **Administrator** role.

Options

The `-i` option specifies the IP address of the virtual machine.

Examples

Display the first user who accessed the virtual machine at the IP address 10.20.34.120.

```
vdmadmin -R -i 10.20.34.120
```

Removing the Entry for a Connection Server Instance or Security Server Using the -S Option

You can use the `vdmadmin` command with the `-S` option to remove the entry for a Connection Server instance or security server from the Horizon 7 configuration.

Syntax

```
vdmadmin -S [-b authentication_arguments] -r -s server
```

Usage Notes

To ensure high availability, Horizon 7 allows you to configure one or more replica Connection Server instances in a Connection Server group. If you disable a Connection Server instance in a group, the entry for the server persists within the Horizon 7 configuration.

You can also use the `vdmadmin` command with the `-S` option to remove a security server from your Horizon 7 environment. You do not have to use this option if you intend to upgrade or reinstall a security server without removing it permanently.

To make the removal permanent, perform these tasks:

1 Uninstall the Connection Server instance or security server from the Windows Server computer by running the Connection Server installer.

2 Remove the Adam Instance VMwareVDMDS program from the Windows Server computer by running the Add or Remove Programs tool.

3 On another Connection Server instance, use the `vdmadmin` command to remove the entry for the uninstalled Connection Server instance or security server from the configuration.

If you want to reinstall Horizon 7 on the removed systems without replicating the Horizon 7 configuration of the original group, restart all the Connection Server hosts in the original group before performing the reinstallation. This prevents the reinstalled Connection Server instances from receiving configuration updates from their original group.

Options

The `-s` option specifies the NetBIOS name of the Connection Server instance or security server to be removed.

Examples

Remove the entry for the Connection Server instance connsvr3.

```
vdmadmin -S -r -s connsvr3
```

Providing Secondary Credentials for Administrators Using the -T Option

You can use the `vdmadmin` command with the `-T` option to provide Active Directory secondary credentials to administrator users.

Syntax

```
vdmadmin -T [-b authentication_arguments] -domainauth
 {-add | -update | -remove | -removeall | -list} -owner domain\user -user domain\user [-password password]
```

Usage Notes

If your users and groups are in a domain with a one-way trust relationship with the Connection Server domain, you must provide secondary credentials for the administrator users in Horizon Administrator. Administrators must have secondary credentials to give them access to the one-way trusted domains. A one-way trusted domain can be an external domain or a domain in a transitive forest trust.

Secondary credentials are required only for Horizon Administrator sessions, not for end users' desktop or application sessions. Only administrator users require secondary credentials.

With the `vdmadmin` command, you configure secondary credentials on a per-user basis. You cannot configure globally specified secondary credentials.

For a forest trust, you typically configure secondary credentials only for the forest root domain. Connection Server can then enumerate the child domains in the forest trust.

Active Directory account lock, disable, and logon hours checks can be performed only when a user in a one-way trusted domain first logs on.

PowerShell administration and smart card authentication of users is not supported in one-way trusted domains. SAML authentication of users in one-way trusted domains is not supported.

Secondary credential accounts require the following permissions. A standard user account should have these permissions by default.

- List Contents
- Read All Properties
- Read Permissions
- Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

Limitations

- PowerShell administration and smart card authentication of users in one-way trusted domains is not supported.
- SAML authentication of users in one-way trusted domains is not supported.

Options

Table 15-17. 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.

Table 15-17. Options for Providing Secondary Credentials (continued)

Option	Description
`-list`	Displays the security credentials for the owner account. Passwords are not displayed.
`-remove`	Removes a security credential from the owner account.
`-removeall`	Removes all security credentials from the owner account.

Examples

Add a secondary credential for the specified owner account. A Windows logon is performed to verify that the specified credentials are valid.

```
vdmadmin -T -domainauth -add -owner domain\user -user domain\user -password password
```

Update a secondary credential for the specified owner account. A Windows logon is performed to verify that the updated credentials are valid.

```
vdmadmin -T -domainauth -update -owner domain\user -user domain\user -password password
```

Remove a secondary credential for the specified owner account.

```
vdmadmin -T -domainauth -remove -owner domain\user -user domain\user
```

Remove all secondary credentials for the specified owner account.

```
vdmadmin -T -domainauth -removeall -owner domain\user
```

Display all secondary credentials for the specified owner account. Passwords are not displayed.

```
vdmadmin -T -domainauth -list -owner domain\user
```

Displaying Information About Users Using the -U Option

You can use the `vdmadmin` command with the `-U` option to display detailed information about users.

Syntax

```
vdmadmin -U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

Usage Notes

The command displays information about a user obtained from Active Directory and Horizon 7.

- Details from Active Directory about the user's account.
- Membership of Active Directory groups.

- Machine entitlements including the machine ID, display name, description, folder, and whether a machine has been disabled.
- ThinApp assignments.
- Administrator roles including the administrative rights of a user and the folders in which they have those rights.

Options

The `-u` option specifies the name and domain of the user.

Examples

Display information about the user Jo in the CORP domain in XML using ASCII characters.

```
vdmadmin -U -u CORP\Jo -n -xml
```

Unlocking or Locking Virtual Machines Using the -V Option

You can use the `vdmadmin` command with the `-V` option to unlock or lock virtual machines in the data center.

Syntax

```
vdmadmin -V [-b authentication_arguments] -e -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -e -vcdn vCenter_dn -vmpath inventory_path
```

```
vdmadmin -V [-b authentication_arguments] -p -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -p -vcdn vCenter_dn -vmpath inventory_path
```

Usage Notes

You should only use the `vdmadmin` command to unlock or lock a virtual machine if you encounter a problem that has left a remote desktop in an incorrect state. Do not use the command to administer remote desktops that are operating normally.

If a remote desktop is locked and the entry for its virtual machine no longer exists in ADAM, use the `–vmpath` and `–vcdn` options to specify the inventory path of the virtual machine and the vCenter Server. You can use vCenter Client to find out the inventory path of a virtual machine for a remote desktop under `Home/Inventory/VMs and Templates`. You can use ADAM ADSI Edit to find out the distinguished name of the vCenter Server under the `OU=Properties` heading.

Options

The following table shows the options that you can specify to unlock or lock virtual machines.

Table 15-18. Options for Unlocking or Locking Virtual Machines

Option	Description
`–d` *desktop*	Specifies the desktop pool.
`–e`	Unlocks a virtual machine.
`–m` *machine*	Specifies the name of the virtual machine.
`–p`	Locks a virtual machine.
`–vcdn` *vCenter_dn*	Specifies the distinguished name of the vCenter Server.
`–vmpath` *inventory_path*	Specifies the inventory path of the virtual machine.

Examples

Unlock the virtual machines machine 1 and machine2 in desktop pool dtpool3.

```
vdmadmin –V –e –d dtpool3 –m machine1 –m machine2
```

Lock the virtual machine machine3 in desktop pool dtpool3.

```
vdmadmin –V –p –d dtpool3 –m machine3
```

Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option

You can use the `vdmadmin` command with the `–X` option to detect and resolve LDAP entry collisions and LDAP schema collisions on replicated Connection Server instances in a group. You can also use this option to detect and resolve LDAP schema collisions in a Cloud Pod Architecture environment.

Syntax

```
vdmadmin –X [–b authentication_arguments] –collisions [–resolve]
vdmadmin –X [–b authentication_arguments] –schemacollisions [–resolve] [–global]
```

Usage Notes

Duplicate LDAP entries on two or more Connection Server instances can cause problems with the integrity of LDAP data in Horizon 7. This condition can occur during an upgrade, while LDAP replication is inoperative. Although Horizon 7 checks for this error condition at regular intervals, you can run the `vdmadmin` command on one of the Connection Server instances in the group to detect and resolve LDAP entry collisions manually.

LDAP schema collisions can also occur during an upgrade, while LDAP replication is inoperative. Because Horizon 7 does not check for this error condition, you must run the `vdmadmin` command to detect and resolve LDAP schema collisions manually.

Options

The following table shows the options that you can specify to detect and resolve LDAP entry collisions.

Table 15-19. 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 15-20. Options for Detecting and Resolving LDAP Schema Collisions

Option	Description
`-schemacollisions`	Specifies an operation for detecting LDAP schema collisions in a Connection Server group or Cloud Pod Architecture environment.
`-resolve`	Resolves all LDAP schema collisions in the LDAP instance. If you do not specify this option, the command only lists the problems that it finds.
`-global`	Applies the checks and fixes to the global LDAP instance in a Cloud Pod Architecture environment. If you do not specify this option, the checks are run against the local LDAP instance.

Examples

Detect LDAP entry collisions in a Connection Server group.

```
vdmadmin -X -collisions
```

Detect and resolve LDAP entry collisions in the local LDAP instance.

```
vdmadmin -X -collisions -resolve
```

Detect and resolve LDAP schema collisions in the global LDAP instance.

```
vdmadmin –X –schemacollisions –resolve –global
```