Administering Cloud Pod Architecture in Horizon 7

VMware Horizon 7 Version 7.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002429-02

vmware®

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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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

Administering Cloud Pod Architecture in Horizon 7

Administering Cloud Pod Architecture in Horizon 7 describes how to configure and administer a Cloud Pod Architecture environment in VMware Horizon® 7, including how to plan a Cloud Pod Architecture topology and set up, monitor, and maintain a Cloud Pod Architecture configuration.

Intended Audience

This information is intended for anyone who wants to set up and maintain a Cloud Pod Architecture environment. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Introduction to Cloud Pod Architecture

1

The Cloud Pod Architecture feature uses standard Horizon components to provide cross-datacenter administration, global and flexible user-to-desktop mapping, high availability desktops, and disaster recovery capabilities.

This chapter includes the following topics:

Understanding Cloud Pod Architecture

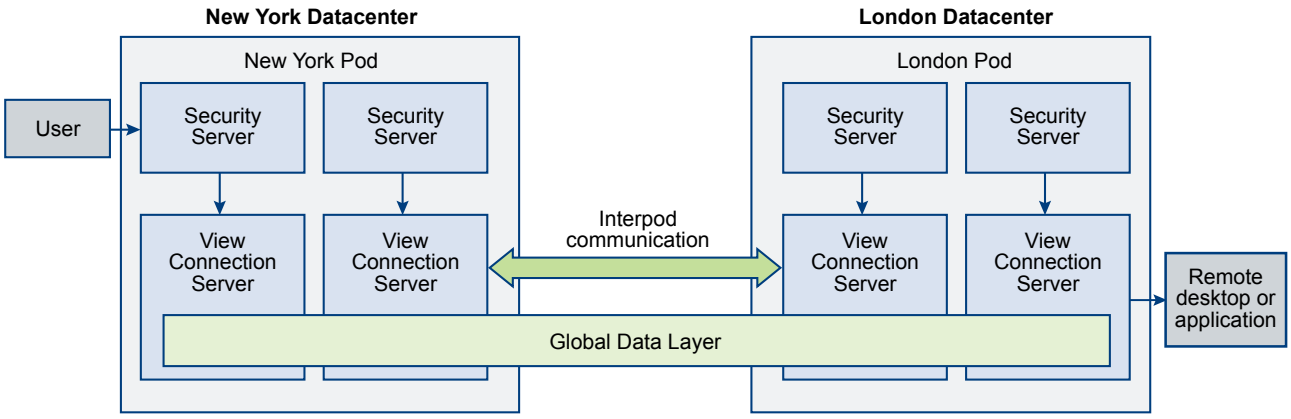
With the Cloud Pod Architecture feature, you can link together multiple pods to provide a single large desktop and application brokering and management environment.

A pod consists of a set of Connection Server instances, shared storage, a database server, and the vSphere and network infrastructures required to host desktop and application pools. In a traditional Horizon implementation, you manage each pod independently. With the Cloud Pod Architecture feature, you can join together multiple pods to form a single Horizon implementation called a pod federation.

A pod federation can span multiple sites and datacenters and simultaneously simplify the administration effort required to manage a large-scale Horizon deployment.

The following diagram is an example of a basic Cloud Pod Architecture topology.

Figure 1-1. Basic Cloud Pod Architecture Topology



In the example topology, two previously standalone pods in different datacenters are joined together to form a single pod federation. An end user in this environment can connect to a Connection Server instance in the New York datacenter and receive a desktop or application in the London data center.

Sharing Key Data in the Global Data Layer

Connection Server instances in a pod federation use the Global Data Layer to share key data. Shared data includes information about the pod federation topology, user and group entitlements, policies, and other Cloud Pod Architecture configuration information.

In a Cloud Pod Architecture environment, shared data is replicated on every Connection Server instance in a pod federation. Entitlement and topology configuration information stored in the Global Data Layer determines where and how desktops are allocated across the pod federation.

Horizon sets up the Global Data Layer on each Connection Server instance in a pod federation when you initialize the Cloud Pod Architecture feature.

Sending Messages Between Pods

Connection Server instances communicate in a Cloud Pod Architecture environment by using an interpod communication protocol called the View InterPod API (VIPA).

Connection Server instances use the VIPA communication channel to launch new desktops, find existing desktops, and share health status data and other information. Horizon configures the VIPA communication channel when you initialize the Cloud Pod Architecture feature.

Configuring and Managing a Cloud Pod Architecture Environment

You use Horizon Administrator and the `lmvutil` command-line interface to configure and manage a Cloud Pod Architecture environment. `lmvutil` is installed as part of the Horizon installation. You can also use Horizon Administrator to view pod health and session information.

Cloud Pod Architecture Limitations

The Cloud Pod Architecture feature has certain limitations.

- The Cloud Pod Architecture feature is not supported in an IPv6 environment.
- Kiosk mode clients are not supported in a Cloud Pod Architecture implementation unless you implement a workaround. For instructions, see VMware Knowledge Base (KB) article 2148888.

Designing a Cloud Pod Architecture Topology

2

Before you begin to configure the Cloud Pod Architecture feature, you must make decisions about your Cloud Pod Architecture topology. Cloud Pod Architecture topologies can vary, depending on your goals, the needs of your users, and your existing Horizon implementation. If you are joining existing Horizon pods to a pod federation, your Cloud Pod Architecture topology is typically based on your existing network topology.

This chapter includes the following topics:

Creating Cloud Pod Architecture Sites

In a Cloud Pod Architecture environment, a site is a collection of well-connected pods in the same physical location, typically in a single datacenter. The Cloud Pod Architecture feature treats pods in the same site equally.

When you initialize the Cloud Pod Architecture feature, it places all pods into a default site called Default First Site. If you have a large implementation, you might want to create additional sites and add pods to those sites.

The Cloud Pod Architecture feature assumes that pods in the same site are on the same LAN, and that pods in different sites are on different LANs. Because WAN-connected pods have slower network performance, the Cloud Pod Architecture feature gives preference to desktops and applications that are in the local pod or site when it allocates desktops and applications to users.

Sites can be a useful part of a disaster recovery solution. For example, you can assign pods in different datacenters to different sites and entitle users and groups to pools that span those sites. If a datacenter in one site becomes unavailable, you can use desktops and applications from the available site to satisfy user requests.

Entitling Users and Groups in the Pod Federation

In a traditional Horizon environment, you use Horizon Administrator to create local entitlements. These local entitlements entitle users and groups to a specific desktop or application pool on a Connection Server instance.

In a Cloud Pod Architecture environment, you create global entitlements to entitle users or groups to multiple desktops and applications across multiple pods in the pod federation. When you use global entitlements, you do not need to configure and manage local entitlements. Global entitlements simplify administration, even in a pod federation that contains a single pod.

Global entitlements are stored in the Global Data Layer. Because global entitlements are shared data, global entitlement information is available on all Connection Server instances in the pod federation.

You entitle users and groups to desktops by creating global desktop entitlements. Each global desktop entitlement contains a list of member users or groups, a list of the desktop pools that can provide desktops for entitled users, and a scope policy. The desktop pools in a global entitlement can be either floating or dedicated pools. You specify whether a global entitlement is floating or dedicated during global entitlement creation.

You entitle users and groups to applications by creating global application entitlements. Each global application entitlement contains a list of the member users or groups, a list of the application pools that can provide applications for entitled users, and a scope policy.

A global entitlement's scope policy specifies where Horizon looks for desktops or applications when it allocates desktops or applications to users in the global entitlement. It also determines whether Horizon looks for desktops or applications in any pod in the pod federation, in pods that reside in the same site, or only in the pod to which the user is connected.

As a best practice, you should not configure local and global entitlements for the same desktop pool. For example, if you create both local and global entitlements for the same desktop pool, the same desktop might appear as a local and a global entitlement in the list of desktops and applications that Horizon Client shows to an entitled user. Similarly, you should not configure both local and global entitlements for application pools created from the same farm.

Finding and Allocating Desktops and Applications in the Pod Federation

Connection Server instances in a Cloud Pod Architecture environment use shared global entitlement and topology configuration information from the Global Data Layer to determine where to search for and how to allocate desktops and applications across the pod federation.

When a user requests a desktop or application from a global entitlement, Horizon searches for an available desktop or application in the pools that are associated with that global entitlement. By default, Horizon gives preference to the local pod, the local site, and pods in other sites, in that order.

For global desktop entitlements that contain dedicated desktop pools, Horizon uses the default search behavior only the first time a user requests a desktop. After Horizon allocates a dedicated desktop, it returns the user directly to the same desktop.

You can modify the search and allocation behavior for individual global entitlements by setting the scope policy and configuring home sites.

Understanding the Scope Policy

When you create a global desktop entitlement or global application entitlement, you must specify its scope policy. The scope policy determines the scope of the search when Horizon looks for desktops or applications to satisfy a request from the global entitlement.

You can set the scope policy so that Horizon searches only on the pod to which the user is connected, only on pods within the same site as the user's pod, or across all pods in the pod federation.

For global desktop entitlements that contain dedicated pools, the scope policy affects where Horizon looks for desktops the first time a user requests a dedicated desktop. After Horizon allocates a dedicated desktop, it returns the user directly to the same desktop.

Understanding the Multiple Sessions Per User Policy

When you create a global desktop entitlement, you can specify whether users can initiate separate desktop sessions from different client devices. The multiple sessions per user policy applies only to global desktop entitlements that contain floating desktop pools.

When you enable the multiple sessions per user policy, users that connect to the global entitlement from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not enable this policy, users are always reconnected to their existing desktop sessions, regardless of the client device that they use.

If you enable the multiple sessions per user policy for a global entitlement, all of the desktop pools associated with the global entitlement must also support multiple users per session.

Using Home Sites

A home site is a relationship between a user or group and a Cloud Pod Architecture site. With home sites, Horizon begins searching for desktops and applications from a specific site rather than searching for desktops and applications based on the user's current location.

If the home site is unavailable or does not have resources to satisfy the user's request, Horizon continues searching other sites according to the scope policy set for the global entitlement.

For global desktop entitlements that contain dedicated pools, the home site affects where Horizon looks for desktops the first time a user requests a dedicated desktop. After Horizon allocates a dedicated desktop, it returns the user directly to the same desktop.

The Cloud Pod Architecture feature includes the following types of home site assignments.

Global home site

A home site that is assigned to a user or group.

If a user who has a home site belongs to a group that is associated with a different home site, the home site associated with the user takes precedence over the group home site assignment.

Global homes sites are useful for controlling where roaming users receive desktops and applications. For example, if a user has a home site in New York but is visiting London, Horizon begins looking in the New York site to satisfy the user's desktop request rather than allocating a desktop closer to the user. Global home site assignments apply for all global entitlements.

Important Global entitlements do not recognize home sites by default. To make a global entitlement use home sites, you must select the **Use home site** option when you create or modify the global entitlement.

Per-global-entitlement home site (home site override)

A home site that is associated with a global entitlement.

Per-global-entitlement home sites override global home site assignments. For this reason, per-global-entitlement home sites are also referred to as home site overrides.

For example, if a user who has a home site in New York accesses a global entitlement that associates that user with the London home site, Horizon begins looking in the London site to satisfy the user's application request rather than allocating an application from the New York site.

Configuring home sites is optional. If a user does not have a home site, Horizon searches for and allocates desktops and applications as described in "Finding and Allocating Desktops and Applications in the Pod Federation," on page 10.

Considerations for Unauthenticated Users

A Horizon administrator can create users for unauthenticated access to published applications on a Connection Server instance. In a Cloud Pod Architecture environment, you can entitle these unauthenticated users to applications across the pod federation by adding them to global application entitlements.

Following are considerations for unauthenticated users in a Cloud Pod Architecture environment.

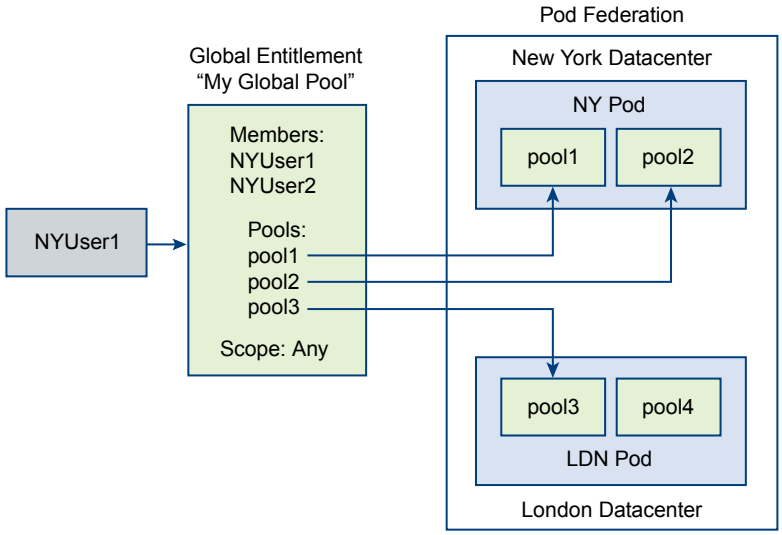
- Unauthenticated users can have only global application entitlements. If an unauthenticated user is included in a global desktop entitlement, a warning icon appears next to the name on the **Users and Groups** tab for the global desktop entitlement in Horizon Administrator.
- When you join a pod to the pod federation, unauthenticated user data is migrated to the Global Data Layer. If you unjoin or eject a pod that contains unauthenticated users from the pod federation, unauthenticated user data for that pod is removed from the Global Data Layer.
- You can have only one unauthenticated user for each Active Directory user. If the same user alias is mapped to more than one Active Directory user, Horizon Administrator displays an error message on the **Unauthenticated Access** tab on the Users and Groups pane.
- You can assign home sites to unauthenticated users.
- Unauthenticated users can have multiple sessions.

For information about setting up unauthenticated users, see the *View Administration* document.

Global Entitlement Example

In this example, NYUser1 is a member of the global desktop entitlement called My Global Pool. My Global Pool provides an entitlement to three floating desktop pools, called pool1, pool2, and pool3. pool1 and pool2 are in a pod called NY Pod in the New York datacenter and pool3 and pool4 are in a pod called LDN Pod in the London datacenter.

Figure 2-1. Global Entitlement Example



Because My Global Pool has a scope policy of ANY, the Cloud Pod Architecture feature looks for desktops across both NY Pod and LDN Pod when NYUser1 requests a desktop. The Cloud Pod Architecture feature does not try to allocate a desktop from pool4 because pool4 is not part of My Global Pool.

If NYUser1 logs into NY Pod, the Cloud Pod Architecture feature allocates a desktop from pool1 or pool2, if a desktop is available. If a desktop is not available in either pool1 or pool2, the Cloud Pod Architecture feature allocates a desktop from pool3.

For an example of restricted global entitlements, see "Restricted Global Entitlement Example," on page 14.

Restricting Access to Global Entitlements

You can configure the restricted global entitlements feature to restrict access to global entitlements based on the Connection Server instance that users initially connect to when they select global entitlements.

With restricted global entitlements, you assign one or more tags to a Connection Server instance. Then, when you configure a global entitlement, you specify the tags of the Connection Server instances that you want to have access to the global entitlement.

You can add tags to global desktop entitlements and global application entitlements.

Tag Matching

The restricted global entitlements feature uses tag matching to determine whether a Connection Server instance can access a particular global entitlement.

At the most basic level, tag matching determines that a Connection Server instance that has a specific tag can access a global entitlement that has the same tag.

The absence of tag assignments can also affect whether users that connect to a Connection Server instance can access a global entitlement. For example, Connection Server instances that do not have any tags can only access global entitlements that also do not have any tags.

Table 2-1 shows how tag matching determines when a Connection Server instance can access a global entitlement.

Table 2-1. Tag Matching Rules

Connection Server	Global Entitlement	Access Permitted?
No tags	No tags	Yes
No tags	One or more tags	No
One or more tags	No tags	Yes
One or more tags	One or more tags	Only when tags match

The restricted global entitlements feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular Connection Server instance.

Considerations and Limitations for Restricted Global Entitlements

Before implementing restricted global entitlements, you must be aware of certain considerations and limitations.

- A single Connection Server instance or global entitlement can have multiple tags.
- Multiple Connection Server instances and global entitlements can have the same tag.
- Any Connection Server instance can access a global entitlement that does not have any tags.
- Connection Server instances that do not have any tags can access only global entitlements that also do not have any tags.
- If you use a security server, you must configure restricted entitlements on the Connection Server instance with which the security server is paired. You cannot configure restricted entitlements on a security server.
- Restricted global entitlements take precedence over other entitlements or assignments. For example, even if a user is assigned to a particular machine, the user cannot access that machine if the tag assigned to the global entitlement does not match the tag assigned to the Connection Server instance to which the user is connected.
- If you intend to provide access to your global entitlements through VMware Identity Manager and you configure Connection Server restrictions, the VMware Identity Manager app might display global entitlements to users when the global entitlements are actually restricted. When a VMware Identity Manager user attempts to connect to a global entitlement, the desktop or application does not start if the tag assigned to the global entitlement does not match the tag assigned to the Connection Server instance to which the user is connected.

Restricted Global Entitlement Example

This example shows a Cloud Pod Architecture environment that includes two pods. Both pods contain two Connection Server instances. The first Connection Server instance supports internal users and the second Connection Server instance is paired with a security server and supports external users.

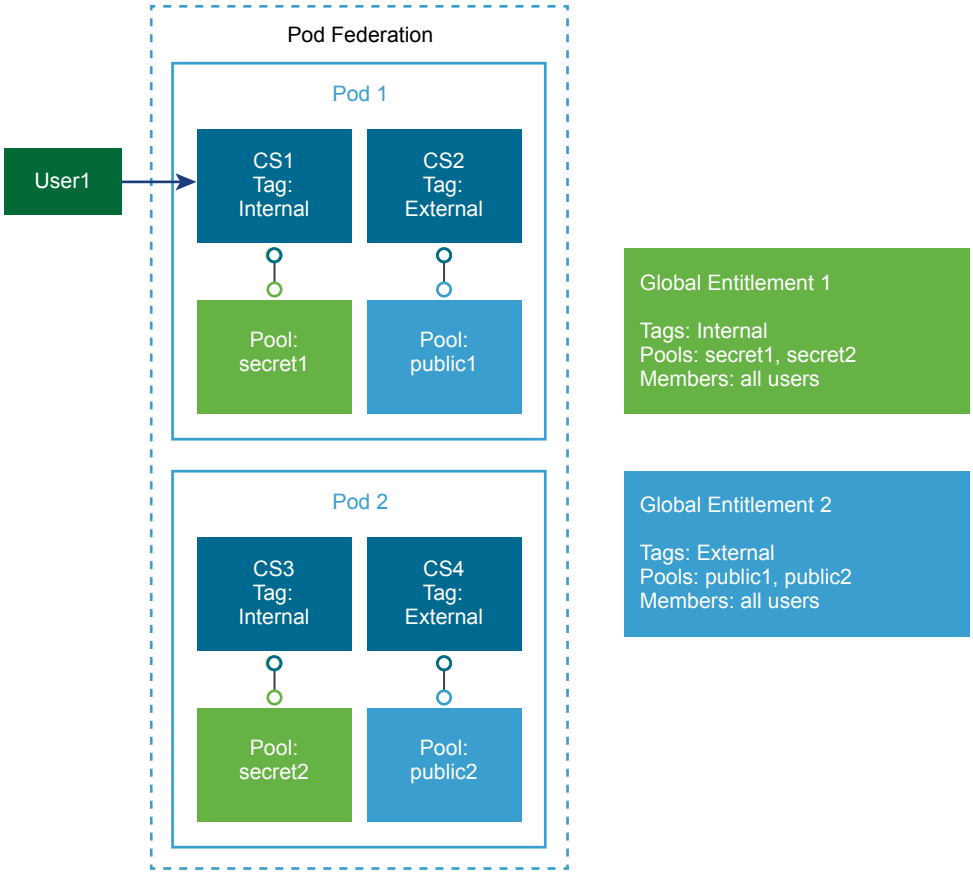
To prevent external users from accessing certain desktop and application pools, you could assign tags as follows:

- Assign the tag "Internal" to the Connection Server instance that support your internal users.
- Assign the tag "External" to the Connection Server instances that support your external users.
- Assign the "Internal" tag to the global entitlements that should be accessible only to internal users.
- Assign the "External" tag to the global entitlements that should be accessible only to external users.

External users cannot see the global entitlements that are tagged as Internal because they log in through the Connection Server instances that are tagged as External. Internal users cannot see the global entitlements that are tagged as External because they log in through the Connection Server instances that are tagged as Internal.

In the following diagram, User1 connects to the Connection Server instance called CS1. Because CS1 is tagged Internal and Global Entitlement 1 is also tagged internal, User1 can only see Global Entitlement 1. Because Global Entitlement 1 contains pools secret1 and secret2, User1 can only receive desktops or applications from the secret1 and secret2 pools.

Figure 2-2. Restricted Global Entitlement Example



Cloud Pod Architecture Topology Limits

A typical Cloud Pod Architecture topology consists of two or more pods, which are linked together in a pod federation. Pod federations are subject to certain limits.

Table 2-2. Pod Federation Limits

Object	Limit
Sessions	75,000
Pods	25
Sites	5
Connection Server instances	175

Cloud Pod Architecture Port Requirements

Certain network ports must be opened on the Windows firewall for the Cloud Pod Architecture feature to work. When you install Connection Server, the installation program can optionally configure the required firewall rules for you. These rules open the ports that are used by default. If you change the default ports after installation, or if your network has other firewalls, you must manually configure the Windows firewall.

Table 2-3. Ports Opened During Connection Server Installation

Protocol	TCP Port	Description
HTTP	22389	Used for Global Data Layer LDAP replication. Shared data is replicated on every Connection Server instance in a pod federation. Each Connection Server instance in a pod federation runs a second LDAP instance to store shared data.
HTTPS	22636	Used for secure Global Data Layer LDAP replication.
HTTPS	8472	Used for View Interpod API (VIPA) communication. Connection Server instances use the VIPA communication channel to launch new desktops and applications, find existing desktops, and share health status data and other information.

Security Considerations for Cloud Pod Architecture Topologies

To use Horizon Administrator or the `lmvutil` command to configure and manage a Cloud Pod Architecture environment, you must have the Administrators role. Users who have the Administrators role on the root access group are super users.

When a Connection Server instance is part of a replicated group of Connection Server instances, the rights of super users are extended to other Connection Server instances in the pod. Similarly, when a pod is joined to a pod federation, the rights of super users are extended to all of the Connection Server instances in all of the pods in the pod federation. These rights are necessary to modify global entitlements and perform other operations on the Global Data Layer.

If you do not want certain super users to be able to perform operations on the Global Data Layer, you can remove the Administrators role assignment and assign the Local Administrators role instead. Users who have the Local Administrators role have super user rights only on their local Connection Server instance and on any instances in a replicated group.

For information about assigning roles in Horizon Administrator, see the *View Administration* document.

Setting Up a Cloud Pod Architecture Environment

3

Setting up a Cloud Pod Architecture environment involves initializing the Cloud Pod Architecture feature, joining pods to the pod federation, and creating global entitlements.

You must create and configure at least one global entitlement to use the Cloud Pod Architecture feature. You can optionally create sites and assign home sites.

This chapter includes the following topics:

Initialize the Cloud Pod Architecture Feature

Before you configure a Cloud Pod Architecture environment, you must initialize the Cloud Pod Architecture feature.

You need to initialize the Cloud Pod Architecture feature only once, on the first pod in a pod federation. To add pods to the pod federation, you join the new pods to the initialized pod.

During the initialization process, Horizon sets up the Global Data Layer on each Connection Server instance in the pod, configures the VIPA communication channel, and establishes a replication agreement between each Connection Server instance.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod.

You can initialize the Cloud Pod Architecture feature from any Connection Server instance in a pod.

2 In Horizon Administrator, select **View Configuration > Cloud Pod Architecture** and click **Initialize the Cloud Pod Architecture feature**.

3 When the Initialize dialog box appears, click **OK** to begin the initialization process.

Horizon Administrator shows the progress of the initialization process. The initialization process can take several minutes.

After the Cloud Pod Architecture feature is initialized, the pod federation contains the initialized pod and a single site. The default pod federation name is Horizon Cloud Pod Federation. The default pod name is based on the host name of the Connection Server instance. For example, if the host name is CS1, the pod name is Cluster-CS1. The default site name is Default First Site.

4 When Horizon Administrator prompts you to reload the client, click **OK**.

After the Horizon Administrator user interface is refreshed, **Global Entitlements** appears under **Catalog** and **Sites** appears under **View Configuration** in the Horizon Administrator Inventory panel.

5 (Optional) To change the default name of the pod federation, select **View Configuration > Cloud Pod Architecture**, click **Edit**, type the new name in the **Name** text box, and click **OK**.

6 (Optional) To change the default name of the pod, select **View Configuration > Sites**, select the pod, click **Edit**, type the new name in the **Name** text box, and click **OK**.

7 (Optional) To change the default name of the site, select **View Configuration > Sites**, select the site, click **Edit**, type the new name in the **Name** text box, and click **OK**.

What to do next

To add more pods to the pod federation, see "Join a Pod to the Pod Federation," on page 18.

Join a Pod to the Pod Federation

During the Cloud Pod Architecture initialization process, the Cloud Pod Architecture feature creates a pod federation that contains a single pod. You can use Horizon Administrator to join additional pods to the pod federation. Joining additional pods is optional.

Important Do not stop or start a Connection Server instance while you are joining it to a pod federation. The Connection Server service might not restart correctly. You can stop and start the Connection Server after it is successfully joined to the pod federation.

Prerequisites

- Make sure the Connection Server instances that you want to join have different host names. You cannot join servers that have the same name, even if they are in different domains.
- Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 17.

Procedure

1 Log in to the Horizon Administrator user interface for a Connection Server instance in the pod that you are joining to the pod federation.

2 In Horizon Administrator, select **View Configuration > Cloud Pod Architecture** and click **Join the pod federation**.

3 In the **Connection Server** text box, type the host name or IP address of any Connection Server instance in any pod that has been initialized or is already joined to the pod federation.

4 In the **User name** text box, type the name of a Horizon administrator user on the already initialized pod.

Use the format *domain**username*.

5 In the **Password** text box, type the password for the Horizon administrator user.

6 Click **OK** to join the pod to the pod federation.

Horizon Administrator shows the progress of the join operation. The default pod name is based on the host name of the Connection Server instance. For example, if the host name is CS1, the pod name is Cluster-CS1.

7 When Horizon Administrator prompts you to reload the client, click **OK**.

After the Horizon Administrator user interface is refreshed, **Global Entitlements** appears under **Catalog** and **Sites** appears under **View Configuration** in the Horizon Administrator Inventory panel.

8 (Optional) To change the default name of the pod, select **View Configuration > Sites**, select the pod, click **Edit**, type the new name in the **Name** text box, and click **OK**.

After the pod is joined to the pod federation, it begins to share health data. You can view this health data on the dashboard in Horizon Administrator. See "View Pod Federation Health in Horizon Administrator," on page 33.

Note A short delay might occur before health data is available in Horizon Administrator.

What to do next

You can repeat these steps to join additional pods to the pod federation.

Create and Configure a Global Entitlement

You use global entitlements to entitle users and groups to desktops and applications in a Cloud Pod Architecture environment. Global entitlements provide the link between users and their desktops and applications, regardless of where those desktops and applications reside in the pod federation.

A global entitlement contains a list of member users or groups, a list of the pools that can provide desktops or applications for entitled users, and a set of policies. You can add both users and groups, only users, or only groups, to a global entitlement. You can add a particular pool to only one global entitlement.

Prerequisites

- Decide which type of global desktop entitlement to create, the users, groups, and pools to include in the global entitlement, and the scope of the global entitlement. See "Entitling Users and Groups in the Pod Federation," on page 10.
- Decide whether the global entitlement should use home sites. See "Using Home Sites," on page 11.
- Create the desktop or application pools to include in the global entitlement. For information about creating pools, see the *Setting Up Virtual Desktops in Horizon 7* and *Setting Up Published Desktops and Applications in Horizon 7* documents.
- Decide which users and groups to include in the global entitlement.
- Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 17.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements** and click **Add**.

3 Select the type of global entitlement to add and click **Next**.

Option	Description
Desktop Entitlement	Adds a global desktop entitlement.
Application Entitlement	Adds a global application entitlement.

4 Configure the global entitlement.

a Type a name for the global entitlement in the **Name** text box.

The name can contain between 1 and 64 characters. This is the name that appears in the list of available desktops and applications in Horizon Client for an entitled user.

b (Optional) Type a description of the global entitlement in the **Description** text box.

The description can contain between 1 and 1024 characters.

c If you are configuring a global desktop entitlement, select a user assignment policy.

The user assignment policy specifies the type of desktop pool that a global desktop entitlement can contain. You can select only one user assignment policy.

Option	Description
Floating	Creates a floating desktop entitlement. A floating desktop entitlement can contain only floating desktop pools.
Dedicated	Creates a dedicated desktop entitlement. A dedicated desktop entitlement can contain only dedicated desktop pools.

d Select a scope policy for the global entitlement.

The scope policy specifies where to look for desktops or applications to satisfy a request from the global entitlement. You can select only one scope policy.

Option	Description
All sites	Look for desktops or applications on any pod in the pod federation.
Within site	Look for desktops or applications only on pods in the same site as the pod to which the user is connected.
Within pod	Look for desktops or applications only in the pod to which the user is connected.

e (Optional) If users have home sites, configure a home site policy for the global entitlement.

Option	Description
Use home site	Begin searching for desktops or applications in the user's home site. If the user does not have a home site and the **Entitled user must have home site** option is not selected, the site to which the user is currently connected is assumed to be the home site.
Entitled user must have home site	Make the global entitlement available only if the user has a home site. This option is available only when the **Use home site** option is selected.

f (Optional) Use the **Automatically clean up redundant sessions** option to specify whether to automatically clean up redundant sessions.

Note This option is available only for floating desktop entitlements and global application entitlements.

Multiple sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When multiple sessions occur, Horizon Client prompts the user to select a session. This option determines what happens to sessions that the user does not select. If you do not select this option, users must manually end their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.

g Select the default display protocol for desktops or applications in the global entitlement and specify whether to allow users to override the default display protocol.

h If you are configuring a global desktop entitlement, select whether to allow users to reset desktops in the global desktop entitlement.

i Select whether to allow users to use the HTML Access feature to access desktops or applications in the global entitlement.

With HTML Access, end users can use a Web browser to connect to remote desktops and applications and are not required to install any client software on their local systems.

j Select whether to allow users to initiate separate desktop sessions from different client devices (multiple sessions per user policy).

If you enable this setting, users that connect to the global entitlement from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not enable this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. You can enable this setting only for floating desktop entitlements.

Note If you enable this setting, all of the desktop pools in the global entitlement must also support multiple sessions per user.

5 Click **Next** and add users or groups to the global entitlement.

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

You can select the **Unauthenticated Users** check box to find and add unauthenticated access users to global application entitlements. You cannot add unauthenticated access users to global desktop entitlements. If you attempt to add an unauthenticated access user to a global desktop entitlement, Horizon Administrator returns an error message.

b Select the user or group to add to the global entitlement and click **OK**.

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

6 Click **Next**, review the global entitlement configuration, and click **Finish** to create the global entitlement.

The global entitlement appears on the Global Entitlements page.

7 Select the pools that can provide desktops or applications for the users in the global entitlement you created.

a Log in to the Horizon Administrator user interface for any Connection Server instance in the pod that contains the pool to add to the global entitlement.

b In Horizon Administrator, select **Catalog > Global Entitlements**.

c Double-click the global entitlement.

d On the **Local Pools** tab, click **Add**, select the pools to add, and click **Add**.

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

Pools that are already associated with a global entitlement, or that do not meet the criteria for the policies you selected for the global entitlement, are not displayed. For example, if you enabled the HTML Access policy, you cannot select pools that do not allow HTML Access.

Important If you add multiple application pools to a global application entitlement, you must add the same application. For example, do not add Calculator and Microsoft Office PowerPoint to the same global application entitlement. If you add different applications to the same global application entitlement, entitled users might receive different applications at different times.

e Repeat these steps on a Connection Server instance in each pod that contains a pool to add to the global entitlement.

The Cloud Pod Architecture feature stores the global entitlement in the Global Data Layer, which replicates the global entitlement on every pod in the pod federation. When an entitled user uses Horizon Client to connect to a Connection Server instance in the pod federation, the global entitlement name appears in the list of available desktops and applications.

Note If a Horizon administrator changes the pool-level display protocol or protocol override policy after a desktop pool is associated with a global desktop entitlement, users can receive a desktop launch error when they select the global desktop entitlement. If a Horizon administrator changes the pool-level virtual machine reset policy after a desktop pool is associated with the global desktop entitlement, users can receive an error if they try to reset the desktop.

What to do next

Assign tags to the global entitlement to restrict access to particular Connection Server instances. See "Restrict Access to a Global Entitlement," on page 22.

Restrict Access to a Global Entitlement

You can restrict access to a global entitlement based on the Connection Server instance that users initially connect to when they select global entitlements. Restricting access to a global entitlement is optional.

Prerequisites

- Become familiar with the restricted global entitlements feature. See "Restricting Access to Global Entitlements," on page 13.
- Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See "lmvutil Command Use," on page 43.
- Become familiar with the syntax of the `lmvutil` command `--updateGlobalEntitlement` and `--updateGlobalApplicationEntitlement` options. See "Modifying a Global Entitlement," on page 55.

To restrict a global entitlement, you assign one or more tags to your Connection Server instances in Horizon Administrator. Then, when you create or edit the global entitlement, you run the `lmvutil` command to specify the tags of the Connection Server instances that you want to have access to the global entitlement.

Note You cannot use Horizon Administrator to assign tags to a global entitlement.

Procedure

1 Assign one or more tags to a Connection Server instance.

a Log in to Horizon Administrator for the Connection Server instance.

b Select **View Configuration > Servers**.

c Click the **Connection Servers** tag, select the Connection Server instance, and click **Edit**.

d Type one or more tags in the **Tags** text box.

Separate multiple tags with a comma or semicolon.

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

Repeat this step for each Connection Server instance to which you want to assign tags.

2 Log in to any Connection Server instance in the pod federation and use the `lmvutil` command to assign one or more tags to the global entitlement.

To specify multiple tags, type a quoted list of tags separated by commas or semicolons.

Option	Action
Assign one or more tags to an existing global desktop entitlement	Run the `lmvutil` command with the `--updateGlobalEntitlement` and `--tags` options. The following example assigns a single tag named **`Internal`** to a global desktop entitlement named Windows 8 Desktop: `lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalEntitlement --entitlementName "Windows 8 Desktop" --tags "Internal"`
Assign one or more tags to an existing global application entitlement	Run the `lmvutil` command with the `--updateGlobalApplicationEntitlement` and `--tags` options. The following example assigns a single tag named **`External`** to a global application entitlement named Microsoft Office PowerPoint: `lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --tags "External"`
Assign one or more tags when you create a new global desktop entitlement	Run the `lmvutil` command with the `--createGlobalEntitlement` and `--tags` options. The following example assigns a single tag named Internal to a global desktop entitlement named Windows 8 desktop: `lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createGlobalEntitlement --entitlementName "Windows 8 Desktop" --tags "Internal"`
Assign one or more tags when you create a new global application entitlement	Run the `lmvutil` command with the `--createGlobalApplicationEntitlement` and `--tags` options. The following example assigns a single tag named External to a global application entitlement named Microsoft Office PowerPoint: `lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --tags "External"`

Repeat this step for each global entitlement to which you want to assign tags.

Create and Configure a Site

If your Cloud Pod Architecture topology contains multiple pods, you might want to group those pods into different sites. The Cloud Pod Architecture feature treats pods in the same site equally.

Prerequisites

- Decide whether your Cloud Pod Architecture topology should include sites. See "Creating Cloud Pod Architecture Sites," on page 9.
- Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 17.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 Create the site.

   a In Horizon Administrator, select **View Configuration > Sites** and click **Add**.

   b Type a name for the site in the **Name** text box.

      The site name can contain between 1 and 64 characters.

   c (Optional) Type a description of the site in the **Description** text box.

      The site name can contain between 1 and 1024 characters.

   d Click **OK** to create the site.

3 Add a pod to the site.

   Repeat this step for each pod to add to the site.

   a In Horizon Administrator, select **View Configuration > Sites** and select the site that currently contains the pod to add to the site.

      The names of the pods in the site appear in the lower pane.

   b Select the pod to add to the site and click **Edit**.

   c Select the site from the **Site** drop-down menu and click **OK**.

Assign a Home Site to a User or Group

A home site is the relationship between a user or group and a Cloud Pod Architecture site. With home sites, Horizon begins searching for desktops and applications from a specific site rather than searching for desktops and applications based on the user's current location. Assigning home sites is optional.

You can associate a global entitlement with a home site so that the global entitlement's home site overrides a user's own home site when a user selects the global entitlement. For more information, see "Create a Home Site Override," on page 25.

Prerequisites

- Decide whether to assign home sites to users or groups in your Cloud Pod Architecture environment. See "Using Home Sites," on page 11.
- Group the pods in your pod federation into sites. See "Create and Configure a Site," on page 24.
- Global entitlements do not use home sites by default. When creating a global entitlement, you must select the **Use home site** option to cause Horizon to use a user's home site when allocating desktops from that global entitlement. See "Create and Configure a Global Entitlement," on page 19.

- Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 17.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Users and Groups** and click the **Home Site** tab.

3 On the **Home Site** tab, click **Add**.

4 Select one or more search criteria and click **Find** to filter the users or groups based on your search criteria.

You can select the **Unauthenticated Users** check box to find unauthenticated access users in the pod federation.

5 Select a user or group and click **Next**.

6 Select the home site to assign to the user or group from the **Home Site** drop-down menu and click **Finish**.

Create a Home Site Override

You can associate a global entitlement with a home site so that the global entitlement's home site overrides a user's own home site when the user selects the global entitlement.

To create a home site override, you associate a home site with a global entitlement and a particular user or group. When the user (or a user in the selected group) accesses the global entitlement, the global entitlement's home site overrides the user's own home site.

For example, if a user who has a home site in New York accesses a global entitlement that associates that user with the London home site, Horizon looks in the London site to satisfy the user's application request rather than allocating an application from the New York site.

Prerequisites

- Verify that the global entitlement has the **Use home site** policy enabled. For more information, see "Modify Attributes or Policies for a Global Entitlement," on page 36.
- Verify that the user or group is included in the global entitlement. For more information, see "Add a User or Group to a Global Entitlement," on page 35.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Double-click the global entitlement to associate with a home site.

4 On the **Home Site Override** tab, click **Add**.

Note The **Add** button is not available if the **Use home site** policy is not enabled for the global entitlement.

---

5 Select one or more search criteria and click **Find** to filter Active Directory users and groups based on your search criteria.

6 Select the Active Directory user or group that has a home site you want to override.

The user or group must already be included in the global entitlement you selected.

7 Select the home site to associate with the global entitlement from the **Home Site** drop-down menu.

8 Click **Finish** to create the home site override.

Test a Cloud Pod Architecture Configuration

After you initialize and configure a Cloud Pod Architecture environment, perform certain steps to verify that your environment is set up properly.

Prerequisites

- Install the latest version of Horizon Client on a supported computer or mobile device.
- Verify that you have credentials for a user in one of your newly created global entitlements.

Procedure

1 Start Horizon Client.

2 Connect to any Connection Server instance in the pod federation by using the credentials of a user in one of your new global entitlements.

After you connect to the Connection Server instance, the global entitlement name appears in the list of available desktops and applications.

3 Select the global entitlement and connect to a desktop or application.

The desktop or application starts successfully. Which desktop or application starts depends on the individual configuration of the global entitlement, pods, and desktop and application pools. The Cloud Pod Architecture feature attempts to allocate a desktop or application from the pod to which you are connected.

What to do next

If the global entitlement does not appear when you connect to the Connection Server instance, use Horizon Administrator to verify that the entitlement is configured correctly. If the global entitlement appears but a desktop or application does not start, all desktop or application pools might be fully assigned to other users.

Example: Setting Up a Basic Cloud Pod Architecture Configuration

This example demonstrates how you can use the Cloud Pod Architecture feature to complete a Cloud Pod Architecture configuration.

In this example, a health insurance company has a mobile sales force that operates across two regions, the Central region and the Eastern region. Sales agents use mobile devices to present insurance policy quotes to customers and customers view and sign digital documents.

Rather than store customer data on their mobile devices, sales agents use standardized floating desktops. Access to customer data is kept secure in the health insurance company's datacenters.

The health insurance company has a data center in each region. Occasional capacity problems cause sales agents to look for available desktops in a non-local data center, and WAN latency problems sometimes occur. If sales agents disconnect from desktops but leave their sessions logged in, they must remember which datacenter hosted their sessions to reconnect to their desktops.

To solve these problems, the health insurance company designs a Cloud Pod Architecture topology, initializes the Cloud Pod Architecture feature, joins its existing pods to the pod federation, creates sites for each of its data centers, entitles its sales agents to all of its desktop pools, and implements a single URL.

1 Designing the Example Topology on page 27

The insurance company designs a Cloud Pod Architecture topology that includes a site for each region.

2 Initializing the Example Configuration on page 28

To initialize the Cloud Pod Architecture feature, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in East Pod 1, selects **View Configuration > Cloud Pod Architecture**, and clicks **Initialize the Cloud Pod Architecture feature**.

3 Joining Pods in the Example Configuration on page 28

The Horizon administrator uses Horizon Administrator to join Central Pod 1 and Central Pod 2 to the pod federation.

4 Creating Sites in the Example Configuration on page 28

The Horizon administrator uses Horizon Administrator to create a site for the Eastern and Central datacenters and adds pods to those sites.

5 Creating Global Desktop Entitlements in the Example Configuration on page 29

The Horizon administrator uses Horizon Administrator to create a single global desktop entitlement that entitles all sales agents to all desktops in the sales agent desktop pools across all pods in the pod federation.

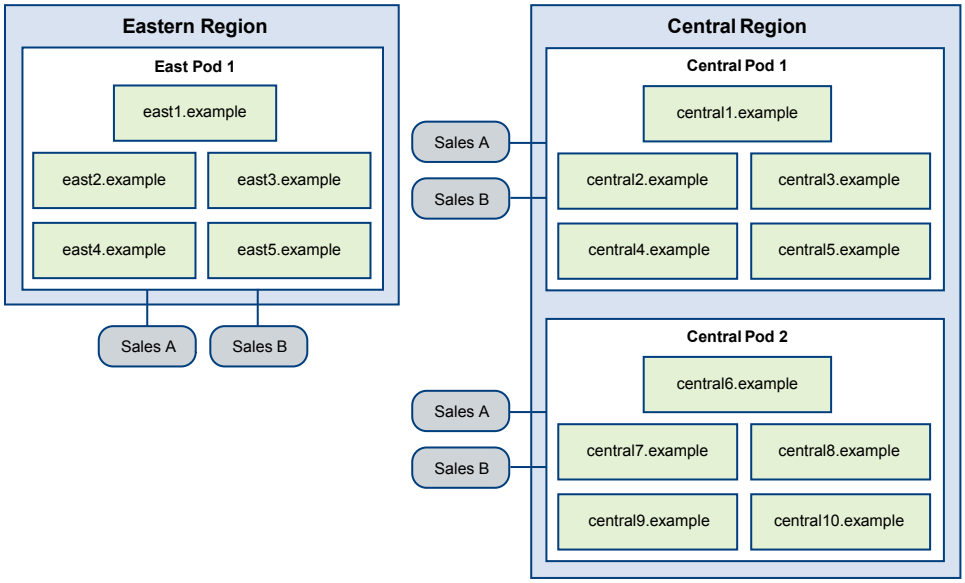
6 Creating a URL for the Example Configuration on page 29

The insurance company uses a single URL and employs a DNS service to resolve sales.example to the nearest pod in the nearest data center. With this arrangement, sales agents do not need to remember different URLs for each pod and are always directed to the nearest data center, regardless of where they are located.

Designing the Example Topology

The insurance company designs a Cloud Pod Architecture topology that includes a site for each region.

Figure 3-1. Example Cloud Pod Architecture Topology



In this topology, the Eastern region site contains a single pod, East Pod 1, that consists of five Connection Server instances called east1.example through east5.example.

The Central region site contains two pods, Central Pod 1 and Central Pod 2. Each pod contains five Connection Server instances. The Connection Servers in the first pod are called central1.example through central5.example. The Connection Server instances in the second pod are called central6.example through central10.example.

Each pod in the topology contains two desktop pools of sales agent desktops, called Sales A and Sales B.

Initializing the Example Configuration

To initialize the Cloud Pod Architecture feature, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in East Pod 1, selects **View Configuration > Cloud Pod Architecture**, and clicks **Initialize the Cloud Pod Architecture feature**.

Because the Horizon administrator uses the Horizon Administrator user interface for a Connection Server instance in East Pod 1, the pod federation initially contains East Pod 1. The pod federation also contains a single site, called Default First Site, which contains East Pod 1.

Joining Pods in the Example Configuration

The Horizon administrator uses Horizon Administrator to join Central Pod 1 and Central Pod 2 to the pod federation.

1. To join Central Pod 1, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in Central Pod 1, selects **View Configuration > Cloud Pod Architecture**, clicks **Join the pod federation**, and provides the host name or IP address of a Connection Server instance in East Pod 1.

   Central Pod 1 is now joined to the pod federation.

2. To join Central Pod 2, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in Central Pod 2, selects **View Configuration > Cloud Pod Architecture**, clicks **Join the pod federation**, and provides the host name or IP address of a Connection Server instance in East Pod 1 or Central Pod 1.

   Central Pod 2 is now joined to the pod federation.

After Central Pod 1 and Central Pod 2 are joined to the pod federation, all 10 Connection Server instances across both pods in the Central region are part of the pod federation.

Creating Sites in the Example Configuration

The Horizon administrator uses Horizon Administrator to create a site for the Eastern and Central datacenters and adds pods to those sites.

1. The Horizon administrator logs in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.
2. To create a site for the Eastern datacenter, the Horizon administrator selects **View Configuration > Sites** and clicks **Add**.
3. To create a site for the Central datacenter, the Horizon administrator selects **View Configuration > Sites** and clicks **Add**.
4. To move East Pod 1 to the site for the Eastern datacenter, the Horizon administrator selects **View Configuration > Sites**, selects the site that currently contains East Pod 1, selects East Pod 1, clicks **Edit**, and selects the Eastern datacenter site from the **Site** drop-down menu.
5. To move Central Pod 1 to the site for the Central datacenter, the Horizon administrator selects **View Configuration > Sites**, selects the site that currently contains Central Pod 1, selects Central Pod 1, clicks **Edit**, and selects the Central datacenter site from the **Site** drop-down menu.
6. To move Central Pod 2 to the site for the Central datacenter, the Horizon administrator selects **View Configuration > Sites**, selects the site that currently contains Central Pod 2, selects Central Pod 2, clicks **Edit**, and selects the Central datacenter site from the **Site** drop-down menu.

The pod federation site topology now reflects the geographic distribution of pods in the insurance company's network.

Creating Global Desktop Entitlements in the Example Configuration

The Horizon administrator uses Horizon Administrator to create a single global desktop entitlement that entitles all sales agents to all desktops in the sales agent desktop pools across all pods in the pod federation.

1 To create and add users to the global desktop entitlement, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server in the pod federation, selects **Catalog > Global Entitlements**, clicks **Add**, and selects **Desktop Entitlement**.

   The Horizon administrator adds the Sales Agents group to the global desktop entitlement. The Sales Agent group is defined in Active Directory and contains all sales agent users. Adding the Sales Agent group to the Agent Sales global desktop entitlement enables sales agents to access the Sales A and Sales B desktop pools on the pods in the Eastern and Central regions.

2 To add the desktop pools in East Pod 1 to the global desktop entitlement, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in East Pod 1, selects **Catalog > Global Entitlements**, double-clicks the global desktop entitlement, clicks **Add** on the **Local Pools** tab, selects the desktop pools to add, and clicks **Add**.

3 To add the desktop pools in Central Pod 1 to the global desktop entitlement, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in Central Pod 1, selects **Catalog > Global Entitlements**, double-clicks the global desktop entitlement, clicks **Add** on the **Local Pools** tab, selects the desktop pools to add, and clicks **Add**.

4 To add the desktop pools in Central Pod 2 to the global desktop entitlement, the Horizon administrator logs in to the Horizon Administrator user interface for a Connection Server instance in Central Pod 2, selects **Catalog > Global Entitlements**, double-clicks the global desktop entitlement, clicks **Add** on the **Local Pools** tab, selects the desktop pools to add, and clicks **Add**.

Creating a URL for the Example Configuration

The insurance company uses a single URL and employs a DNS service to resolve sales.example to the nearest pod in the nearest data center. With this arrangement, sales agents do not need to remember different URLs for each pod and are always directed to the nearest data center, regardless of where they are located.

When a sales agent connects to the URL in Horizon Client, the Agent Sales global entitlement appears on the list of available desktop pools. When a sales agent selects the global desktop entitlement, the Cloud Pod Architecture feature delivers the nearest available desktop in the pod federation. If all of the desktops in the local data center are in use, the Cloud Pod Architecture feature selects a desktop from the other data center. If a sales agent leaves a desktop session logged in, the Cloud Pod Architecture feature returns the sales agent to that desktop, even if the sales agent has since traveled to a different region.

Managing a Cloud Pod Architecture Environment

4

You use Horizon Administrator and the `lmvutil` command to view, modify, and maintain your Cloud Pod Architecture environment. You can also use Horizon Administrator to monitor the health of pods in the pod federation.

This chapter includes the following topics:

View a Cloud Pod Architecture Configuration

You can use Horizon Administrator or the `lmvutil` command to view information about global entitlements, pods, sites, and home sites.

This procedure shows how to use Horizon Administrator to view information about global entitlements, pods, sites, and home sites. To use the `lmvutil` command to view this information, see Chapter 5, "lmvutil Command Reference," on page 43.

This procedure also shows how to use the `lmvutil` command to list the tags associated with a global entitlement. Horizon Administrator does not show the tags associated with a global entitlement.

Procedure

- To list all of the global entitlements in your configuration, in Horizon Administrator, select **Catalog > Global Entitlements**.

  You can use the Horizon Administrator user interface for any Connection Server instance in the pod federation.

- To list the desktop or application pools in a global entitlement, in Horizon Administrator, select **Catalog > Global Entitlements**, double-click the global entitlement name, and click the **Local Pools** tab.

  Only the pools in the local pod appear on the **Local Pools** tab. If a global entitlement includes desktop or application pools in a remote pod, you must log in to the Horizon Administrator user interface for a Connection Server instance in the remote pod to see those pools.

- To list the users or groups associated with a global entitlement, in Horizon Administrator, select **Catalog > Global Entitlements**, double-click the global entitlement, and click the **Users and Groups** tab.

  You can use the Horizon Administrator user interface for any Connection Server instance in the pod federation.

- To list the pods in the pod federation, in Horizon Administrator, select **View Configuration > Cloud Pod Architecture**.

  You can use the Horizon Administrator user interface for any Connection Server instance in the pod federation.

- To list the sites in the pod federation, in Horizon Administrator, select **View Configuration > Sites**.

  You can use the Horizon Administrator user interface for any Connection Server instance in the pod federation.

- To list the home sites for a user by global entitlement, perform these steps in Horizon Administrator.

  a Select **Users and Groups**, click the **Home Site** tab, and select **Resolution**.

  b Click inside the **Click here to find the user** text box.

  c Select one or more search criteria and click **Find** to filter the Active Directory users based on your search criteria.

  d Select the Active Directory user and click **OK**.

  e Click **Look Up** to display the home sites for the user.

  The global entitlement name appears in the Entitlement column and the effective home site for the global entitlement appears in the Home Site Resolution column. The origin of a home site assignment appears in parentheses after the home site name. If a user has multiple home sites, a folder icon appears next to the global entitlement name. You can expand this folder to list the home site assignments that are not in effect for the global entitlement.

- To list the tags associated with a global desktop entitlement, run the `lmvutil` command with the `––listGlobalEntitlements` option.

  You can run this command from any Connection Server instance in the pod federation.

  For example:

  ```
  lmvutil ––authAs adminEast ––authDomain domainEast ––authPassword "*" ––
  listGlobalEntitlements
  ```

  The tags associated with the global entitlement appear after `Restriction Tags` in the command output.

- To list the tags associated with a global application entitlement, run the `lmvutil` command with the `––listGlobalApplicationEntitlements` option.

  You can run this command from any Connection Server instance in the pod federation.

  For example:

  ```
  lmvutil ––authAs adminEast ––authDomain domainEast ––authPassword "*" ––
  listGlobalApplicationEntitlements
  ```

  The tags appear after `Restriction Tags` in the command output.

View Pod Federation Health in Horizon Administrator

Horizon constantly monitors the health of the pod federation by checking the health of each pod and Connection Server instances in those pods. You can view the health of a pod federation in Horizon Administrator.

You can also view the health of a pod federation from the command line by using the `vdmadmin` command with the `–H` option. For information about `vdmadmin` syntax, see the *View Administration* document.

Important Horizon event databases are not shared across pods in a pod federation.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Inventory > Dashboard**.

The Remote Pods section in the System Health pane lists all pods, their member Connection Server instances, and the known health status for each Connection Server instance.

A green health icon indicates that the Connection Server instance is online and available for the Cloud Pod Architecture feature. A red health icon indicates that the Connection Server instance is offline or the Cloud Pod Architecture feature cannot connect to the Connection Server instance to confirm its availability.

View Desktop and Application Sessions in the Pod Federation

You can use Horizon Administrator to search for and view desktop and application sessions across the pod federation.

You can search for desktop and application sessions by user, pod, or brokering pod. The user is the end user who is connected to the desktop or application, the pod is the pod on which the desktop or application is hosted, and the brokering pod is the pod to which the user was connected when the desktop or application was first allocated.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Inventory > Search Sessions**.

3 Select search criteria and begin the search.

Option	Action
Search by user	a Select **User** from the drop-down menu. b Click in the text box. c Select search criteria in the Find User dialog box and click **OK**. d Click **Search** to begin the search.
Search by pod	a Select **Pod** from the drop-down menu and select a pod from the list of pods that appears. b Click **Search** to begin the search.
Search by brokering pod	a Select **Brokering Pod** from the drop-down menu and select a pod from the list of pods that appears. b Click **Search** to begin the search.

The search results include the user, type of session (desktop or application), machine, pool or farm, pod, brokering pod ID, site, and global entitlements associated with each session. The session start time, duration, and state also appear in the search results.

Note The brokering pod ID is not immediately populated for new sessions in the search results. This ID usually appears in Horizon Administrator between two and three minutes after a session begins.

Add a Pod to a Site

You can use Horizon Administrator to add a pod to an existing site.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **View Configuration > Sites**.

3 Select the site that currently contains the pod to add to the site.

The names of the pods in the site appear in the lower pane.

4 Select the pod to add to the site and click **Edit**.

5 Select the site from the **Site** drop-down menu and click **OK**.

Modifying Global Entitlements

You can add and remove desktop pools, users, and groups from global entitlements. You can also delete global entitlements and modify global entitlement attributes and policies.

Add a Pool to a Global Entitlement

You can use Horizon Administrator to add a desktop pool to an existing global desktop entitlement, or add an application pool to an existing global application entitlement. You can add a particular pool to only one global entitlement.

Prerequisites

Create the desktop or application pool to add to the global entitlement. See the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod that contains the pool to add to the global entitlement.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Double-click the global entitlement.

4 On the **Local Pools** tab, click **Add**, select the desktop or application pool to add, and click **Add**.

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

Note Pools that are already associated with a global entitlement or that do not meet the criteria for the global entitlement policies you selected are not displayed.

Note If a Horizon administrator changes the pool-level display protocol or protocol override policy after a desktop pool is associated with a global desktop entitlement, users can receive a desktop launch error when they select the global desktop entitlement. If a Horizon administrator changes the pool-level virtual machine reset policy after a desktop pool is associated with the global desktop entitlement, users can receive an error if they try to reset the desktop.

Remove a Pool from a Global Entitlement

You can use Horizon Administrator to remove a pool from a global entitlement.

Procedure

1. Log in to the Horizon Administrator user interface for any Connection Server instance in the pod that contains the pool to remove.
2. In Horizon Administrator, select **Catalog > Global Entitlements**.
3. On the **Local Pools** tab, select the pool to remove from the global entitlement and click **Delete**.

Add a User or Group to a Global Entitlement

You can use Horizon Administrator to add a user or group to an existing global entitlement.

Procedure

1. Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.
2. In Horizon Administrator, select **Catalog > Global Entitlements** and double-click the global entitlement.
3. On the **Users and Groups** tab, click **Add**.
4. Click **Add**, select one or more search criteria, and click **Find** to filter Active Directory users or groups based on your search criteria.

   You can select the **Unauthenticated Users** check box to find and add unauthenticated access users to global application entitlements. You cannot add unauthenticated access users to global desktop entitlements. If you attempt to add an unauthenticated access user to a global desktop entitlement, Horizon Administrator returns an error message.
5. Select the Active Directory user or group to add to the global entitlement and click **OK**.

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

Remove a User or Group From a Global Entitlement

You can use Horizon Administrator to remove a user or group from a global entitlement.

Procedure

1. Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.
2. In Horizon Administrator, select **Catalog > Global Entitlements** and double-click the global entitlement.
3. On the Users and Groups tab, select the user or group to delete and click **Delete**.

   You can press Ctrl or Shift to select multiple users and groups.
4. Click **OK** in the confirmation dialog box.

Modify Attributes or Policies for a Global Entitlement

You can use Horizon Administrator to modify the name and description attributes and scope and other policies of a global entitlement.

You cannot modify the type of desktop pool that a global desktop entitlement can contain.

You must use the `lmvutil` command to add or remove tags from a global entitlement. For more information, see "Restrict Access to a Global Entitlement," on page 22 and "Remove Tags From a Global Entitlement," on page 37.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Select the global entitlement and click **Edit**.

4 To modify the name or description of the global entitlement, type a new name or description in the **Name** or **Description** text box in the General pane.

The name can contain between 1 and 64 characters. The description can contain between 1 and 1024 characters.

5 To modify a global entitlement policy, select or deselect the policy in the Policy pane.

Policy	Description
Scope	Specifies where to look for desktops or applications that satisfy a desktop or application request from the global entitlement. You can select only one scope policy. ■ **All sites** - look for desktops or applications on any pod in the pod federation. ■ **Within site** - look for desktops or applications only on pods in the same site as the pod to which the user is connected. ■ **Within pod** - look for desktops or applications only in the pod to which the user is connected.
Use home site	Determine whether to begin searching for desktops or applications in the user's home site. If the user does not have a home site and the **Entitled user must have home site** option is not selected, the site to which the user is currently connected is assumed to be the home site.
Entitled user must have home site	Makes the global entitlement available only if the user has a home site. This option is available only when the **Use home site** option is selected.
Automatically clean up redundant sessions	Logs off extra user sessions for the same entitlement.. This option is available only for floating desktop entitlements and application entitlements. Multiple sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When multiple sessions occur, Horizon Client prompts the user to select a session. This option determines what happens to sessions that the user does not select. If you do not select this option, users must manually end their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.
Default display protocol	Specifies the default display protocol for desktops or applications in the global entitlement.

Policy	Description
HTML Access	Determines whether to allow users to use the HTML Access feature to access desktops or applications in the global entitlement. With HTML Access, end users can use a Web browser to connect to remote desktops and are not required to install any client software on their local systems.
Allow user to initiate separate sessions from different client devices	Determines whether to allow users to initiate separate desktop sessions from different client devices (multiple sessions per user policy). If you enable this setting, users that connect to the global entitlement from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not enable this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. You can enable this setting only for floating desktop entitlements. **Note** If you enable this setting, all of the desktop pools in the global entitlement must also support multiple sessions per user.

6 To modify the application path, version, and publisher information for a global application entitlement, type values in the application text boxes.

Note If you add an application pool to the global application entitlement after you modify these values, the values are overwritten with values from the application pool.

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

Remove Tags From a Global Entitlement

You can use the `lmvutil` command to remove tags from a global entitlement.

Note You cannot use Horizon Administrator to remove tags from a global entitlement.

Prerequisites

- Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See "lmvutil Command Use," on page 43.
- Become familiar with the `lmvutil` command options `--updateGlobalEntitlement` and `--updateGlobalApplicationEntitlement`. See "Modifying a Global Entitlement," on page 55.
- Log in to any Connection Server instance in the pod federation.

Procedure

- To remove tags from a global desktop entitlement, run the `lmvutil` command with the `--updateGlobalEntitlement` and `--notags` options.

  The following example removes tags from the global desktop entitlement named Windows 8 Desktop:

  ```
  lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
  --updateGlobalEntitlement --entitlementName "Windows 8 Desktop" --notags
  ```

- To remove tags from a global application entitlement, run the `lmvutil` command with the `--updateGlobalApplicationEntitlement` and `--notags` options.

  The following example removes tags from the global application entitlement named Microsoft Office PowerPoint:

  ```
  lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
  --updateGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint"
  --notags
  ```

Delete a Global Entitlement

You can use Horizon Administrator to permanently delete a global entitlement. When you delete a global entitlement, all of the users who are dependent on that global entitlement for desktops cannot access their desktops. Existing desktop sessions remain connected.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Click the global entitlement to delete and click **Delete**.

4 Click **OK** in the confirmation dialog box.

Managing Home Site Assignments

You can modify and delete home site assignments. You can also display the effective home site for each global entitlement to which a user belongs.

Modify a Home Site Assignment

You can change an existing home site assignment for a specific user or group.

To modify the association between a global entitlement and a home site for a specific user or group, see "Modify a Home Site Override," on page 39.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Users and Groups**, click the **Home Site** tab, and select **Assignment**.

3 Select the home site assignment to modify and click **Edit**.

4 Select a different home site from the **Home Site** drop-down menu.

5 Click **OK** to save the new home site assignment.

Remove a Home Site Assignment

You can remove the association between a user or group and a home site.

To remove the association between a home site and a global entitlement for a specific user or group, see "Remove a Home Site Override," on page 40.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Users and Groups**, click the **Home Site** tab, and select **Assignment**.

3 Select the home site assignment to remove and click **Delete**.

4 Click **OK** to remove the home site assignment.

Determine the Effective Home Site for a User

Because you can assign home sites to both users and groups, a single user can have multiple home sites. In addition, home sites associated with global entitlements can override a user's own home site. You can use Horizon Administrator to determine a user's effective home site.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Users and Groups**, click the **Home Site** tab, and select **Resolution**.

3 Click inside the **Click here to find the user** text box.

4 Select one or more search criteria and click **Find** to filter the Active Directory users based on your search criteria.

5 Select the Active Directory user whose effective home site you want to display and click **OK**.

6 Click **Look Up**.

Horizon Administrator displays the effective home site for each global entitlement to which the user belongs. Only global entitlements that have the **Use home site** policy enabled are displayed.

The home site that is in effect appears in the Home Site Resolution column. If a user has multiple home sites, a folder icon appears next to the global entitlement name in the Entitlement column. You can expand this folder to list the home site assignments that are not in effect for the global entitlement. Horizon Administrator uses strikethrough text to indicate a home site is not in effect.

Horizon Administrator displays the origin of a home site assignment in parentheses after the home site name in the Home Site Resolution column. If the home site originated from a group in which the user belongs, Horizon Administrator displays the name of the group, for example, **(via Domain Users)**. If the home site originated from the user's own home site assignment, Horizon Administrator displays **(Default)**. If the home site originated from the global entitlement (a home site override), Horizon Administrator displays **(Direct)**.

If a user does not have a home site, Horizon Administrator displays **No home site defined** in the Home Site Resolution column.

Modify a Home Site Override

You can change the association between a global entitlement and a home for site for a specific user or group.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Double-click the global entitlement.

4 On the **Home Site Override** tab, select the user or group and click **Edit**.

5 Select a different home site from the **Home Site** drop-down menu.

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

Remove a Home Site Override

You can remove the association between a global entitlement and a home site for a specific user or group.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod federation.

2 In Horizon Administrator, select **Catalog > Global Entitlements**.

3 Double-click the global entitlement.

4 On the **Home Site Overrides** tab, select the user or group and click **Remove**.

5 Click **OK** to remove the home site override.

Remove a Pod From the Pod Federation

You can use Horizon Administrator to remove a pod that was previously joined to the pod federation. You might want to remove a pod from the pod federation if it is being recommissioned for another purpose or if it was wrongly configured.

To remove the last pod in the pod federation, you uninitialize the Cloud Pod Architecture feature. See "Uninitialize the Cloud Pod Architecture Feature," on page 40.

Important Do not stop or start a Connection Server instance while it is being removed from a pod federation. The Connection Server service might not restart correctly.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod that you want to remove from the pod federation.

2 In Horizon Administrator, select **Cloud Pod Architecture** and click **Unjoin** in the Pod Federation pane.

3 Click **OK** to begin the unjoin operation.

Horizon Administrator shows the progress of the unjoin operation.

4 When Horizon Administrator prompts you to reload the client, click **OK**.

After the Horizon Administrator user interface is refreshed, **Global Entitlements** no longer appears under **Catalog** and **Sites** no longer appears under **View Configuration** in the Horizon Administrator Inventory panel.

Uninitialize the Cloud Pod Architecture Feature

You can use Horizon Administrator to uninitialize the Cloud Pod Architecture feature.

Prerequisites

You need to uninitialize the Cloud Pod Architecture feature on only one pod in the pod federation. If the pod federation contains multiple pods, you must unjoin the other pods before you begin the uninitialization process. See "Remove a Pod From the Pod Federation," on page 40.

Procedure

1 Log in to the Horizon Administrator user interface for any Connection Server instance in the pod.

2 In Horizon Administrator, select **View Configuration > Cloud Pod Architecture**.

3 In the Pod Federation pane, click **Uninitialize**.

4 Click **OK** to begin the uninitialization process.

After the uninitialization process is finished, your entire Cloud Pod Architecture configuration, including sites, home sites, and global entitlements, is deleted.

5 When Horizon Administrator prompts you to reload the client, click **OK**.

After the Horizon Administrator user interface is refreshed, **Global Entitlements** no longer appears under **Catalog** and **Sites** no longer appears under **View Configuration** in the Horizon Administrator Inventory panel.

lmvutil Command Reference

5

You use the `lmvutil` command-line interface to configure and manage a Cloud Pod Architecture implementation.

NOTE You can use the `vdmutil` command-line interface to perform the same operations as `lmvutil`.

This chapter includes the following topics:

lmvutil Command Use

The syntax of the `lmvutil` command controls its operation.

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

`lmvutil` *`command_option`* `[`*`additional_option argument`*`] ...`

Alternatively, you can use the `vdmutil` command to perform the same operations as the `lmvutil` command. Use the following form of the `vdmutil` command from a Windows command prompt.

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

The additional options that you can use depend on the command option.

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

lmvutil Command Authentication

To use the `lmvutil` command to configure and manage a Cloud Pod Architecture environment, you must run the command as a user who has the Administrators role.

You can use Horizon Administrator to assign the Administrators role to a user. See the *View Administration* document.

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

Table 5-1. lmvutil Command Authentication Options

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

For example, the following `lmvutil` command logs in the user domainEast\adminEast and initializes the Cloud Pod Architecture feature.

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --initialize
```

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

lmvutil Command Output

The `lmvutil` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails.

The `lmvutil` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `lmvutil` command writes output to standard output.

The `lmvutil` command produces only US English output.

lmvutil Command Options

You use the command options of the `lmvutil` command to specify the operation to perform. All options are preceded by two hyphens (--).

For `lmvutil` command authentication options, see "lmvutil Command Authentication," on page 44.

Table 5-2. lmvutil Command Options

Option	Description
`--activatePendingCertificate`	Activates a pending SSL certificate. See "Activating a Pending Certificate," on page 67.
`--addGroupEntitlement`	Associates a user group with a global entitlement. See "Adding a User or Group to a Global Entitlement," on page 59.

Table 5-2. lmvutil Command Options (Continued)

Option	Description
`--addPoolAssociation`	Associates a desktop pool with a global desktop entitlement or an application pool with a global application entitlement. See "Adding a Pool to a Global Entitlement," on page 57.
`--addUserEntitlement`	Associates a user with a global entitlement. See "Adding a User or Group to a Global Entitlement," on page 59
`--assignPodToSite`	Assigns a pod to a site. See "Assigning a Pod to a Site," on page 50.
`--createGlobalApplicationEntitlement`	Creates a global application entitlement. See "Creating a Global Entitlement," on page 52.
`--createGlobalEntitlement`	Creates a global desktop entitlement. See "Creating a Global Entitlement," on page 52.
`--createSite`	Creates a site. See "Creating a Site," on page 50.
`--createGroupHomeSite`	Associates a user group with a home site. See "Configuring a Home Site," on page 61.
`--createPendingCertificate`	Creates a pending SSL certificate. See "Creating a Pending Certificate," on page 67.
`--createUserHomeSite`	Associates a user with a home site. See "Configuring a Home Site," on page 61.
`--deleteGlobalApplicationEntitlement`	Deletes a global application entitlement. See "Deleting a Global Entitlement," on page 57.
`--deleteGlobalEntitlement`	Deletes a global deskop entitlement. See "Deleting a Global Entitlement," on page 57.
`--deleteSite`	Deletes a site. See "Deleting a Site," on page 51.
`--deleteGroupHomeSite`	Removes the association between a user group and a home site. See "Deleting a Home Site," on page 62.
`--deleteUserHomeSite`	Removes the association between a user and a home site. See "Deleting a Home Site," on page 62.
`--editSite`	Modifies the name or description of a site. See "Changing a Site Name or Description," on page 51.
`--ejectPod`	Removes an unavailable pod from a pod federation. See "Removing a Pod From a Pod Federation," on page 48.
`--help`	Lists the `lmvutil` command options.
`--initialize`	Initializes the Cloud Pod Architecture feature. See "Initializing the Cloud Pod Architecture Feature," on page 46.
`--join`	Joins a pod to a pod federation. See "Joining a Pod to the Pod Federation," on page 48.
`--listAssociatedPools`	Lists the desktop pools that are associated with a global desktop entitlement or the application pools that are associated with a global application entitlement. See "Listing the Pools in a Global Entitlement," on page 63.
`--listEntitlements`	Lists associations between users or user groups and global entitlements. "Listing the Users or Groups in a Global Entitlement," on page 64.
`--listGlobalApplicationEntitlements`	Lists all global application entitlements. See "Listing Global Entitlements," on page 63.
`--listGlobalEntitlements`	Lists all global desktop entitlements. See "Listing Global Entitlements," on page 63.

Table 5-2. lmvutil Command Options (Continued)

Option	Description
`--listPods`	Lists the pods in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 66.
`--listSites`	Lists the sites in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 66.
`--listUserAssignments`	Lists the dedicated desktop pod assignments for a user and global entitlement combination. See "Listing Dedicated Desktop Pool Assignments," on page 66.
`--removePoolAssociation`	Removes the association between a desktop pool and a global entitlement. See "Removing a Pool from a Global Entitlement," on page 58.
`--resolveUserHomeSite`	Shows the effective home site for a user. See "Listing the Effective Home Site for a User," on page 65.
`--removeGroupEntitlement`	Removes a user group from a global entitlement. See "Removing a User or Group From a Global Entitlement," on page 60.
`--removeUserEntitlement`	Removes a user from a global entitlement. See "Removing a User or Group From a Global Entitlement," on page 60.
`--showGroupHomeSites`	Shows all of the home sites for a group. See "Listing the Home Sites for a User or Group," on page 64.
`--showUserHomeSites`	Shows all of the home sites for a user. See "Listing the Home Sites for a User or Group," on page 64.
`--uninitialize`	Disables the Cloud Pod Architecture feature. See "Disabling the Cloud Pod Architecture Feature," on page 47.
`--unjoin`	Removes an available pod from a pod federation. See "Removing a Pod From a Pod Federation," on page 48.
`--updateGlobalApplicationEntitlement`	Modifes a global application entitlement. See "Modifying a Global Entitlement," on page 55.
`--updateGlobalEntitlement`	Modifies a global desktop entitlement. See "Modifying a Global Entitlement," on page 55.
`--updatePod`	Modifies the name or description of a pod. See "Changing a Pod Name or Description," on page 49.
`--verbose`	Enables verbose logging. You can add this option to any other option to obtain detailed command output. The `lmvutil` command writes to standard output.

Initializing the Cloud Pod Architecture Feature

Use the `lmvutil` command with the `--initialize` option to initialize the Cloud Pod Architecture feature. When you initialize the Cloud Pod Architecture feature, Horizon sets up the Global Data Layer on each Connection Server instance in the pod and configures the VIPA communication channel.

Syntax

```
lmvutil --initialize
```

Usage Notes

Run this command only once, on one Connection Server instance in the pod. You can run the command on any Connection Server instance in the pod. You do not need to run this command for additional pods. All other pods join the initialized pod.

This command returns an error message if the Cloud Pod Architecture feature is already initialized or if the command cannot complete the operation.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --initialize
```

Disabling the Cloud Pod Architecture Feature

Use the `lmvutil` command with the `--uninitialize` option to disable the Cloud Pod Architecture feature.

Syntax

```
lmvutil --uninitialize
```

Usage Notes

Before you run this command, use the `lmvutil` command with the `--unjoin` option to remove any other pods in the pod federation.

Run this command on only one Connection Server instance in a pod. You can run the command on any Connection Server instance in the pod. If your pod federation contains multiple pods, you need to run this command for only one pod.

This command returns an error message if the Cloud Pod Architecture feature is not initialized, if the command cannot find the pod, or if the pod federation contains other pods.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --uninitialize
```

Managing Pod Federations

The `lmvutil` command provides options to configure and modify pod federations.

- Joining a Pod to the Pod Federation on page 48

  Use the `lmvutil` command with the `--join` option to join a pod to the pod federation.

- Removing a Pod From a Pod Federation on page 48

  Use the `lmvutil` command with the `--unjoin` or `--ejectPod` option to remove a pod from a pod federation.

- Changing a Pod Name or Description on page 49

  Use the `lmvutil` command with the `--updatePod` option to update or modify the name or description of a pod.

Joining a Pod to the Pod Federation

Use the `lmvutil` command with the `--join` option to join a pod to the pod federation.

Syntax

```
lmvutil --join joinServer serveraddress --userName domain\username --password password
```

Usage Notes

You must run this command on each pod that you want to join to the pod federation. You can run the command on any Connection Server instance in a pod.

This command returns an error message if you provide invalid credentials, the specified Connection Server instance does not exist, a pod federation does not exist on the specified server, or the command cannot complete the operation.

Options

You must specify several options when you join a pod to a pod federation.

Table 5-3. Options for Joining a Pod to a Pod Federation

Option	Description
`--joinServer`	DNS name or IP address of any Connection Server instance in any pod that has been initialized or is already part of the pod federation.
`--userName`	Name of a Horizon administrator user on the already initialized pod. Use the format *domain\username*.
`--password`	Password of the user specified in the `--userName` option.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --join
--joinServer 123.456.789.1 --userName domainCentral\adminCentral --password secret123
```

Removing a Pod From a Pod Federation

Use the `lmvutil` command with the `--unjoin` or `--ejectPod` option to remove a pod from a pod federation.

Syntax

```
lmvutil --unjoin
```

```
lmvutil --ejectPod --pod pod
```

Usage Notes

To remove a pod from a pod federation, use the `--unjoin` option. You can run the command on any Connection Server instance in the pod.

To remove a pod that is not available from a pod federation, use the `--ejectPod` option. For example, a pod might become unavailable if a hardware failure occurs. You can perform this operation on any pod in the pod federation.

Important In most circumstances, you should use the `--unjoin` option to remove a pod from a pod federation.

These commands return an error message if the Cloud Pod Architecture feature is not initialized, the pod is not joined to a pod federation, or if the commands cannot perform specified operations.

Options

When you use the `--ejectPod` option, you use the `--pod` option to identify the pod to remove from the pod federation.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --unjoin
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --ejectPod
--pod "East Pod 1"
```

Changing a Pod Name or Description

Use the `lmvutil` command with the `--updatePod` option to update or modify the name or description of a pod.

Syntax

```
lmvutil --updatePod --podName podname [--newPodName podname] [--description text]
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the command cannot find or update the pod.

Options

You can specify these options when you update a pod name or description.

Table 5-4. Options for Changing a Pod Name or Description

Option	Description
`--podName`	Name of the pod to update.
`--newPodName`	(Optional) New name for the pod. A pod name can contain between 1 and 64 characters.
`--description`	(Optional) Description of the site. The description can contain between 1 and 1024 characters.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--updatePod --podName "East Pod 1" --newPodName "East Pod 2"
```

Managing Sites

You can use `lmvutil` command options to create, modify, and delete Cloud Pod Architecture sites. A site is a grouping of pods.

- Creating a Site on page 50

  Use the `lmvutil` command with the `--createSite` option to create a site in a Cloud Pod Architecture topology.

- Assigning a Pod to a Site on page 50

  Use the `lmvutil` command with the `--assignPodToSite` option to assign a pod to a site.

- Changing a Site Name or Description on page 51

  Use the `lmvutil` command with the `--editSite` option to edit the name or description of a site.

- Deleting a Site on page 51

  Use the `lmvutil` command with the `--deleteSite` option to delete a site.

Creating a Site

Use the `lmvutil` command with the `--createSite` option to create a site in a Cloud Pod Architecture topology.

Syntax

```
lmvutil --createSite --siteName sitename [--description text]
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized, the specified site already exists, or the command cannot create the site.

Options

You can specify these options when you create a site.

Table 5-5. Options for Creating a Site

Option	Description
`--siteName`	Name of the new site. The site name can contain between 1 and 64 characters.
`--description`	(Optional) Description of the site. The description can contain between 1 and 1024 characters.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createSite
--siteName "Eastern Region"
```

Assigning a Pod to a Site

Use the `lmvutil` command with the `--assignPodToSite` option to assign a pod to a site.

Syntax

```
lmvutil --assignPodToSite --podName podname --siteName sitename
```

Usage Notes

Before you can assign a pod to a site, you must create the site. See "Creating a Site," on page 50.

This command returns an error message if the Cloud Pod Architecture feature is not initialized, the command cannot find the specified pod or site, or if the command cannot assign the pod to the site.

Options

You must specify these options when you assign a pod to a site.

Table 5-6. Options for Assigning a Pod to a Site

Option	Description
`--podName`	Name of the pod to assign to the site.
`--siteName`	Name of the site.

You can use the `lmvutil` command with the `--listPods` option to list the names of the pods in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 66.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--assignPodToSite --podName "East Pod 1" --siteName "Eastern Region"
```

Changing a Site Name or Description

Use the `lmvutil` command with the `--editSite` option to edit the name or description of a site.

Syntax

```
lmvutil --editSite --siteName sitename [--newSiteName sitename] [--description text]
```

Usage Notes

This command returns an error message if the specified site does not exist or if the command cannot find or update the site.

Options

You can specify these options when you change a site name or description.

Table 5-7. Options for Changing a Site Name or Description

Option	Description
`--siteName`	Name of the site to edit.
`--newSiteName`	(Optional) New name for the site. The site name can contain between 1 and 64 characters.
`--description`	(Optional) Description of the site. The description can contain between 1 and 1024 characters.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --editSite
--siteName "Eastern Region" --newSiteName "Western Region"
```

Deleting a Site

Use the `lmvutil` command with the `--deleteSite` option to delete a site.

Syntax

```
lmvutil --deleteSite --sitename sitename
```

Usage Notes

This command returns an error message if the specified site does not exist or if the command cannot find or delete the site.

Options

You use the `--sitename` option to specify the name of the site to delete.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteSite --sitename "Eastern Region"
```

Managing Global Entitlements

You can use `lmvutil` command options to create, modify, and list global desktop entitlements and global application entitlements in a Cloud Pod Architecture environment.

- Creating a Global Entitlement on page 52

  To create a global desktop entitlement, use the `lmvutil` command with the `--createGlobalEntitlement` option. To create a global application entitlement, use the `lmvutil` command with the `--createGlobalApplicationEntitlement` option.

- Modifying a Global Entitlement on page 55

  To modify a global desktop entitlement, use the `lmvutil` command with the `--updateGlobalEntitlement` option. To modify a global application entitlement, use the `lmvutil` command with the `--updateGlobalApplicationEntitlement` option.

- Deleting a Global Entitlement on page 57

  To delete a global desktop entitlement, use the `lmvutil` command with the `--deleteGlobalEntitlement` option. To delete a global application entitlement, use the `lmvutil` command with the `--deleteGlobalApplicationEntitlement` option.

- Adding a Pool to a Global Entitlement on page 57

  Use the `lmvutil` command with the `--addPoolAssociation` option to add a desktop pool to a global desktop entitlement or an application pool to a global application entitlement.

- Removing a Pool from a Global Entitlement on page 58

  Use the `lmvutil` command with the `--removePoolAssociation` option to remove a desktop pool from a global desktop entitlement or an application pool from a global application entitlement.

- Adding a User or Group to a Global Entitlement on page 59

  To add a user to a global entitlement, use the `lmvutil` command with the `--addUserEntitlement` option. To add a group to a global entitlement, use the `lmvutil` command with the `--addGroupEntitlement` option.

- Removing a User or Group From a Global Entitlement on page 60

  To remove a user from a global entitlement, use the `lmvutil` command with the `--removeUserEntitlement` option. To remove a group from a global entitlement, use the `lmvutil` command with the `--removeGroupEntitlement` option.

Creating a Global Entitlement

To create a global desktop entitlement, use the `lmvutil` command with the `--createGlobalEntitlement` option. To create a global application entitlement, use the `lmvutil` command with the `--createGlobalApplicationEntitlement` option.

Global entitlements provide the link between users and their desktops and applications, regardless of where those desktops and applications reside in the pod federation. Global entitlements also include policies that determine how the Cloud Pod Architecture feature allocates desktops and applications to entitled users.

Syntax

```
lmvutil --createGlobalEntitlement --entitlementName name --scope scope
{--isDedicated | --isFloating} [--description text] [--disabled]
[--fromHome] [--multipleSessionAutoClean] [--requireHomeSite] [--defaultProtocol value]
[--preventProtocolOverride] [--allowReset] [--htmlAccess] [--multipleSessionsPerUser]
[--tags tags]
```

```
lmvutil --createGlobalApplicationEntitlement --entitlementName name --scope scope
[--description text] [--disabled] [--fromHome] [--multipleSessionAutoClean]
[--requireHomeSite] [--defaultProtocol value] [--preventProtocolOverride] [--htmlAccess]
[--tags tags]
```

Usage Notes

You can use these commands on any Connection Server instance in a pod federation. The Cloud Pod Architecture feature stores new data in the Global Data Layer and replicates that data in all pods in the pod federation.

These commands return an error message if the global entitlement already exists, the scope is invalid, the Cloud Pod Architecture feature is not initialized, or the commands cannot create the global entitlement.

Options

You can specify these options when you create a global entitlement. Some options apply only to global desktop entitlements.

Table 5-8. Options for Creating Global Entitlements

Option	Description
`--entitlementName`	Name of the global entitlement. The name can contain between 1 and 64 characters. The global entitlement name appears in the desktops and applications list in Horizon Client for entitled users.
`--scope`	Scope of the global entitlement. Valid values are as follows: ■ ANY. Horizon looks for resources on any pod in the pod federation. ■ SITE. Horizon looks for resources only on pods in the same site as the pod to which the user is connected. ■ LOCAL. Horizon looks for resources only in the pod to which the user is connected.
`--isDedicated`	Creates a dedicated desktop entitlement. A dedicated desktop entitlement can contain only dedicated desktop pools. To create a floating desktop entitlement, use the `--isFloating` option. A global desktop entitlement can be either dedicated or floating. You cannot specify the `--isDedicated` option with the `--multipleSessionAutoClean` option. Applies only to global desktop entitlements.
`--isFloating`	Creates a floating desktop entitlement. A floating desktop entitlement can contain only floating desktop pools. To create a dedicated desktop entitlement, specify the `--isDedicated` option. A global desktop entitlement can be either floating or dedicated. Applies only to global desktop entitlements.
`--disabled`	(Optional) Creates the global entitlement in the disabled state.
`--description`	(Optional) Description of the global entitlement. The description can contain between 1 and 1024 characters.
`--fromHome`	(Optional) If the user has a home site, causes Horizon to begin searching for resources on the user's home site. If the user does not have a home site, Horizon begins searching for resources on the site to which the user is currently connected.

Table 5-8. Options for Creating Global Entitlements (Continued)

Option	Description
`--multipleSessionAutoClean`	(Optional) Logs off extra user sessions for the same entitlement. Multiple sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When multiple sessions occur, Horizon Client prompts the user to select a session. This option determines what happens to sessions that the user does not select. If you do not specify this option, users must manually end their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.
`--requireHomeSite`	(Optional) Causes the global entitlement to be available only if the user has a home site. This option is applicable only when the `--fromHome` option is also specified.
`--defaultProtocol`	(Optional) Default display protocol for desktops or applications in the global entitlement. Valid values are RDP, PCOIP, and BLAST for global desktop entitlements and PCOIP and BLAST for global application entitlements.
`--preventProtocolOverride`	(Optional) Prevents users from overriding the default display protocol.
`--allowReset`	(Optional) Allows users to reset desktops. Applies only to global desktop entitlements.
`--htmlAccess`	(Optional) When you specify this option, users can use the HTML Access feature to access resources in the global entitlement. With HTML Access, end users can use a Web browser to access remote resources and are not required to install any client software on their local systems.
`--multipleSessionsPerUser`	(Optional) Allows users to initiate separate desktop sessions from different client devices. Users that connect to the global entitlement from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not use this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. Applies only to floating desktop entitlements.
`--tags`	(Optional) Specifies one or more tags that restrict access to the global entitlement from Connection Server instances. To specify multiple tags, type a quoted list of tag names separated by a comma or semicolon.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createGlobalEntitlement
--entitlementName "Windows 8 Desktop" --scope LOCAL --isDedicated
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --
createGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --scope LOCAL
```

Modifying a Global Entitlement

To modify a global desktop entitlement, use the `lmvutil` command with the `--updateGlobalEntitlement` option. To modify a global application entitlement, use the `lmvutil` command with the `--updateGlobalApplicationEntitlement` option.

Syntax

```
lmvutil --updateGlobalEntitlement --entitlementName name [--description text]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--multipleSessionsPerUser] [--
disableMultipleSessionsPerUser]
[--requireHomeSite] [--disableRequireHomeSite] [--defaultProtocol value]
[--scope scope] [--htmlAccess] [--disableHtmlAccess] [--tags tags] [--notags]
```

```
lmvutil --updateGlobalApplicationEntitlement --entitlementName name [--description text]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--requireHomeSite] [--disableRequireHomeSite] [--
defaultProtocol value]
[--scope scope] [--htmlAccess] [--disableHtmlAccess] [--appVersion value] [--appPublisher value]
[--appPath value] [--tags tags] [--notags]
```

Usage Notes

You can use these commands on any Connection Server instance in a pod federation. The Cloud Pod Architecture feature stores new data in the Global Data Layer and replicates that data among all pods in the pod federation.

These commands return an error message if the global entitlement does not exist, the scope is invalid, the Cloud Pod Architecture feature is not initialized, or the commands cannot update the global entitlement.

Options

You can specify these options when you modify a global entitlement. Some options apply only to global desktop entitlements or only to global application entitlements.

Table 5-9. Options for Modifying Global Entitlements

Option	Description
`--entitlementName`	Name of the global entitlement to modify.
`--scope`	Scope of the global entitlement. Valid values are as follows: ■ ANY. Horizon looks for resources on any pod in the pod federation. ■ SITE. Horizon looks for resources only on pods in the same site as the pod to which the user is connected. ■ LOCAL. Horizon looks for resources only in the pod to which the user is connected.
`--description`	(Optional) Description of the global entitlement. The description can contain between 1 and 1024 characters.
`--disabled`	(Optional) Disables a previously enabled global entitlement.
`--enabled`	(Optional) Enables a previously disabled global entitlement.
`--fromHome`	(Optional) If the user has a home site, causes Horizon to begin searching for resources on the user's home site. If the user does not have a home site, Horizon begins searching for resources on the site to which the user is currently connected.
`--disableFromHome`	(Optional) Disables the `--fromHome` option function if the `--fromHome` option was previously specified for the global entitlement.

Table 5-9. Options for Modifying Global Entitlements (Continued)

Option	Description
`--multipleSessionAutoClean`	(Optional) Logs off extra user sessions for the same entitlement. Multiple sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When multiple sessions occur, Horizon Client prompts the user to select a session. This option determines what happens to sessions that the user does not select. If you do not specify this option, users must manually end their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.
`--disableMultipleSessionAutoClean`	(Optional) Disables the `--multipleSessionAutoClean` option function if the `--multipleSessionAutoClean` option was previously specified for the global entitlement.
`--multipleSessionsPerUser`	(Optional) Allows users to initiate separate desktop sessions from different client devices. Users that connect to the global entitlement from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not use this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. Applies only to floating desktop entitlements.
`--disableMultipleSessionsPerUser`	(Optional) Disables the `--multipleSessionsPerUser` option function if the `--multipleSessionsPerUser` option was previously specified for the global entitlement.
`--requireHomeSite`	(Optional) Causes the global entitlement to be available only if the user has a home site. This option is applicable only when the `--fromHome` option is also specified.
`--disableRequireHomeSite`	(Optional) Disables the `--requireHomeSite` option function if the `--requireHomeSite` option was previously specified for the global entitlement.
`--defaultProtocol`	(Optional) Default display protocol for desktops or applications in the global entitlement. Valid values are RDP, PCOIP, and BLAST for global desktop entitlements and PCOIP and BLAST for global application entitlements.
`--htmlAccess`	(Optional) When you specify this option, users can use the HTML Access feature to access resources in the global entitlement. With HTML Access, end users can use a Web browser to access remote resources and are not required to install any client software on their local systems.
`--disableHtmlAccess`	(Optional) Disables the `--htmlAccess` option function if the `--htmlAccess` option was previously specified for the global entitlement.
`--appVersion`	(Optional) Version of the application. Applies only to global application entitlements.
`--appPublisher`	(Optional) Publisher of the application. Applies only to global application entitlements.
`--appPath`	(Optional) Full pathname of the application, for example, `C:\Program Files\app1.exe`. Applies only to global application entitlements.

Table 5-9. Options for Modifying Global Entitlements (Continued)

Option	Description
`--tags`	(Optional) Specifies one or more tags that restrict access to the global entitlement from Connection Server instances. To specify multiple tags, type a quoted list of tag names separated by a comma or semicolon.
`--notags`	(Optional) Removes tags from the global entitlement if the `--tags` option was previously used to add tags to the global entitlement.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalEntitlement
--entitlementName "Windows 8 Desktop" --scope ANY --isDedicated
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--updateGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --scope ANY
```

Deleting a Global Entitlement

To delete a global desktop entitlement, use the `lmvutil` command with the `--deleteGlobalEntitlement` option. To delete a global application entitlement, use the `lmvutil` command with the `--deleteGlobalApplicationEntitlement` option.

Syntax

```
lmvutil --deleteGlobalEntitlement --entitlementName name
```

```
lmvutil --deleteGlobalApplicationEntitlement --entitlementName name
```

Command Usage

These commands return an error message if the specified global entitlement does not exist, the Cloud Pod Architecture feature is not initialized, or the commands cannot delete the global entitlement.

Options

You use the `--entitlementName` option to specify the name of the global entitlement to delete.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGlobalEntitlement --entitlementName "Windows 8 Desktop"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint"
```

Adding a Pool to a Global Entitlement

Use the `lmvutil` command with the `--addPoolAssociation` option to add a desktop pool to a global desktop entitlement or an application pool to a global application entitlement.

Syntax

```
lmvutil --addPoolAssociation --entitlementName name --poolId poolid
```

Usage Notes

You must use this command on a Connection Server instance in the pod that contains the pool. For example, if pod1 contains a desktop pool to associate with a global desktop entitlement, you must run the command on a Connection Server instance that resides in pod1.

Repeat this command for each pool to become part of the global entitlement. You can add a particular pool to only one global entitlement.

Important If you add multiple application pools to a global application entitlement, you must add the same application. For example, do not add Calculator and Microsoft Office PowerPoint to the same global application entitlement. If you add different applications, the results will be unpredictable and entitled users will receive different applications at different times.

This command returns an error message if the Cloud Pod Architecture feature is not initialized, the specified entitlement does not exist, the pool is already associated with the specified entitlement, the pool does not exist, or the command cannot add the pool to the global entitlement.

Options

You can specify these options when you add a pool to a global entitlement.

Table 5-10. Options for Adding a Pool to a Global Entitlement

Option	Description
`--entitlementName`	Name of the global entitlement.
`--poolID`	ID of the pool to add to the global entitlement. The pool ID must match the pool name as it appears on the pod.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --addPoolAssociation
--entitlementName "Windows 8 Desktop" --poolId "Windows 8 Desktop Pool A"
```

Removing a Pool from a Global Entitlement

Use the `lmvutil` command with the `--removePoolAssociation` option to remove a desktop pool from a global desktop entitlement or an application pool from a global application entitlement.

Syntax

```
lmvutil --removePoolAssociation --entitlementName name --poolID poolid
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized, the specified global entitlement or pool does not exist, or if the command cannot remove the pool from the global entitlement.

Options

You can specify these options when you remove a pool from a global entitlement.

Table 5-11. Options for Removing a Pool from a Global Entitlement

Option	Description
`--entitlementName`	Name of the global entitlement.
`--poolID`	ID of the pool to remove from the global entitlement. The pool ID must match the pool name as it appears on the pod.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removePoolAssociation --entitlementName "Windows 8 Desktop" --poolID "Windows 8 Desktop Pool A"
```

Adding a User or Group to a Global Entitlement

To add a user to a global entitlement, use the `lmvutil` command with the `--addUserEntitlement` option. To add a group to a global entitlement, use the `lmvutil` command with the `--addGroupEntitlement` option.

Syntax

```
lmvutil --addUserEntitlement --userName domain\username --entitlementName name
```

```
lmvutil --addGroupEntitlement --groupName domain\groupname --entitlementName name
```

Usage Notes

Repeat these commands for each user or group to add to the global entitlement.

These commands return an error message if the specified entitlement, user, or group does not exist or if the command cannot add the user or group to the entitlement.

Options

You can specify these options when you add a user or group to a global entitlement.

Table 5-12. Options for Adding a User or Group to a Global Entitlement

Option	Description
`--userName`	Name of a user to add to the global entitlement. Use the format *domain\username*.
`--groupName`	Name of a group to add to the global entitlement. Use the format *domain\groupname*.
`--entitlementName`	Name of the global entitlement to which to add the user or group.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --addUserEntitlement
--userName domainCentral\adminCentral --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--addGroupEntitlement --groupName domainCentral\adminCentralGroup --entitlementName "Agent Sales"
```

Removing a User or Group From a Global Entitlement

To remove a user from a global entitlement, use the `lmvutil` command with the `--removeUserEntitlement` option. To remove a group from a global entitlement, use the `lmvutil` command with the `--removeGroupEntitlement` option.

Syntax

```
lmvutil --removeUserEntitlement --userName domain\username --entitlementName name
```

```
lmvutil --removeGroupEntitlement --groupName domain\groupname --entitlementName name
```

Usage Notes

These commands return an error message if the Cloud Pod Architecture feature is not initialized, if the specified user name, group name, or entitlement does not exist, or if the command cannot remove the user or group from the entitlement.

Options

You must specify these options when you remove a user or group from a global entitlement.

Table 5-13. Options for Removing a User or Group From a Global Entitlement

Option	Description
`--userName`	Name of a user to remove from the global entitlement. Use the format *domain\username*.
`--groupName`	Name of a group to remove from the global entitlement. Use the format *domain\groupname*.
`--entitlementName`	Name of the global entitlement from which to remove the user or group.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removeUserEntitlement --userName domainCentral\adminCentral --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removeGroupEntitlement --groupName domainCentral\adminCentralGroup --entitlementName "Agent
Sales"
```

Managing Home Sites

You can use `lmvutil` command options to create, modify, delete, and list home sites.

- Configuring a Home Site on page 61

  To create a home site for a user, use the `lmvutil` command with the `--createUserHomeSite` option. To create a home site for a group, use the `lmvutil` command with the `--createGroupHomeSite` option. You can also use these options to associate a home site with a global desktop entitlement or global application entitlement.

- Deleting a Home Site on page 62

  To remove the association between a user and a home site, use the `lmvutil` command with the `--deleteUserHomeSite` option. To remove the association between a group and a home site, use the `lmvutil` command with the `--deleteGroupHomeSite` option.

Configuring a Home Site

To create a home site for a user, use the `lmvutil` command with the `--createUserHomeSite` option. To create a home site for a group, use the `lmvutil` command with the `--createGroupHomeSite` option. You can also use these options to associate a home site with a global desktop entitlement or global application entitlement.

Syntax

`lmvutil --createUserHomeSite --userName` *`domain\username`* `--siteName` *`name`* `[--entitlementName` *`name`*`]`

`lmvutil --createGroupHomeSite --groupName` *`domain\groupname`* `--siteName` *`name`* `[--entitlementName` *`name`*`]`

Usage Notes

You must create a site before you can configure it as a home site. See "Creating a Site," on page 50.

These commands return an error message if the Cloud Pod Architecture feature is not initialized, the specified user or group does not exist, the specified site does not exist, the specified entitlement does not exist, or the commands cannot create the home site.

Options

You can specify these options when you create a home site for a user or group.

Table 5-14. Options for Creating a Home Site for a User or Group

Option	Description
`--userName`	Name of a user to associate with the home site. Use the format *domain\username*.
`--groupName`	Name of a group to associate with the home site. Use the format *domain\groupname*.
`--siteName`	Name of the site to associate with the user or group as the home site.
`--entitlementName`	(Optional) Name of a global desktop entitlement or global application entitlement to associate with the home site. When a user selects the specified global entitlement, the home site overrides the user's own home site. If you do not specify this option, the command creates a global user or group home site.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createUserHomeSite --
userName domainEast\adminEast --siteName "Eastern Region" --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--createGroupHomeSite --groupName domainEast\adminEastGroup --siteName "Eastern Region"
--entitlementName "Agent Sales"
```

Deleting a Home Site

To remove the association between a user and a home site, use the `lmvutil` command with the `--deleteUserHomeSite` option. To remove the association between a group and a home site, use the `lmvutil` command with the `--deleteGroupHomeSite` option.

Syntax

```
lmvutil --deleteUserHomeSite --userName domain\username [--entitlementName name]
```

```
lmvutil --deleteGroupHomeSite --groupName domain\groupname [--entitlementName name]
```

Usage Notes

These commands return an error message if the specified user or group does not exist, the specified global entitlement does not exist, or if the commands cannot delete the home site setting.

Options

You can specify these options when you remove the association between a user or group and a home site.

Table 5-15. Options for Deleting a Home Site

Option	Description
`--userName`	Name of a user. Use the format *domain\username*.
`--groupName`	Name of a group. Use the format *domain\groupname*.
`--entitlementName`	(Optional) Name of a global desktop entitlement or global application entitlement. You can use this option to remove the association between the home site and a global entitlement for the specified user or group.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --deleteUserHomeSite
--userName domainEast\adminEast
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGroupHomeSite --groupName domainEast\adminEastGroup
```

Viewing a Cloud Pod Architecture Configuration

You can use `lmvutil` command options to list information about a Cloud Pod Architecture configuration.

- Listing Global Entitlements on page 63

  To list information about all global desktop entitlements, including their policies and attributes, use the `lmvutil` command with the `--listGlobalEntitlements` option. To list information about all global application entitlements, including their policies and attributes, use the `lmvutil` command with the `--listGlobalApplicationEntitlements` option.

- Listing the Pools in a Global Entitlement on page 63

  Use the `lmvutil` command with the `--listAssociatedPools` option to list the desktop or application pools that are associated with a specific global entitlement.

- Listing the Users or Groups in a Global Entitlement on page 64

  Use the `lmvutil` command with the `--listEntitlements` option to list all the users or groups associated with a specific global entitlement.

- Listing the Home Sites for a User or Group on page 64

  To list all the configured home sites for a specific user, use the `lmvutil` command with the `--showUserHomeSites` option. To list all the configured home sites for a specific group, use the `lmvutil` command with the `--showGroupHomeSites` option.

- Listing the Effective Home Site for a User on page 65

  Use the `lmvutil` command with the `--resolveUserHomeSite` option to determine the effective home site for a specific user. Because home sites can be assigned to users and groups and to global entitlements, it is possible to configure more than one home site for a user.

- Listing Dedicated Desktop Pool Assignments on page 66

  Use the `lmvutil` command with the `--listUserAssignments` option to to list the dedicated desktop pool assignments for a user and global entitlement combination.

- Listing the Pods or Sites in a Cloud Pod Architecture Topology on page 66

  To view the pods in the pod federation, use the `lmvutil` command with the `--listPods` option. To view the sites in the pod federation, use the `lmvutil` command with the `--listSites` option.

Listing Global Entitlements

To list information about all global desktop entitlements, including their policies and attributes, use the `lmvutil` command with the `--listGlobalEntitlements` option. To list information about all global application entitlements, including their policies and attributes, use the `lmvutil` command with the `--listGlobalApplicationEntitlements` option.

Syntax

```
lmvutil --listGlobalEntitlements
```

```
lmvutil --listGlobalApplicationEntitlements
```

Usage Notes

These commands return an error message if the Cloud Pod Architecture feature is not initialized or if the commands cannot list the global entitlements.

Examples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listGlobalEntitlements
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--listGlobalApplicationEntitlements
```

Listing the Pools in a Global Entitlement

Use the `lmvutil` command with the `--listAssociatedPools` option to list the desktop or application pools that are associated with a specific global entitlement.

Syntax

```
lmvutil --listAssociatedPools --entitlementName name
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the specified global entitlement does not exist.

Options

You use the `--entitlementName` option to specify the name of the global entitlement for which to list the associated desktop or application pools.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listAssociatedPools
--entitlementName "Agent Sales"
```

Listing the Users or Groups in a Global Entitlement

Use the `lmvutil` command with the `--listEntitlements` option to list all the users or groups associated with a specific global entitlement.

Syntax

```
lmvutil --listEntitlements {--userName domain\username | --groupName domain\groupname | --
entitlementName name}
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the specified user, group, or entitlement does not exist.

Options

You can specify these options when you list global entitlement associations.

Table 5-16. Options for Listing Global Entitlement Associations

Option	Description
`--userName`	Name of the user for whom you want to list global entitlements. Use the format *domain\username*. This option lists all global entitlements associated with the specified user.
`--groupName`	Name of the group for which you want to list global entitlements. Use the format *domain\groupname*. This option lists all global entitlements associated with the specified group.
`--entitlementName`	Name of a global entitlement. This option lists all users and groups in the specified global entitlement.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listEntitlements
--userName example\adminEast
```

Listing the Home Sites for a User or Group

To list all the configured home sites for a specific user, use the `lmvutil` command with the `--showUserHomeSites` option. To list all the configured home sites for a specific group, use the `lmvutil` command with the `--showGroupHomeSites` option.

Syntax

```
lmvutil --showUserHomeSites --userName domain\username [--entitlementName name]
```

```
lmvutil --showGroupHomeSites --groupName domain\groupname [--entitlementName name]
```

Usage Notes

These commands return an error message if the Cloud Pod Architecture feature is not initialized or if the specified user, group, or global entitlement does not exist.

Options

You can specify these options when you list the home sites for a user or group.

Table 5-17. Options for Listing the Home Sites for a User or Group

Option	Description
`--userName`	Name of a user. Use the format *domain\username*.
`--groupName`	Name of a group. Use the format *domain\groupname*.
`--entitlementName`	(Optional) Name of a global entitlement. Use this option if you want to show the home sites for a user or group and global entitlement combination.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --showUserHomeSites
--userName example\adminEast
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --showGroupHomeSites
--groupName example\adminEastGroup
```

Listing the Effective Home Site for a User

Use the `lmvutil` command with the `--resolveUserHomeSite` option to determine the effective home site for a specific user. Because home sites can be assigned to users and groups and to global entitlements, it is possible to configure more than one home site for a user.

Syntax

```
lmvutil --resolveUserHomeSite --entitlementName name --userName domain\username
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the specified global entitlement or user does not exist.

Options

You must specify these options when you list the effective home site for a user.

Table 5-18. Options for Listing the Effective Home Site for a User

Option	Description
`--entitlementName`	Name of a global entitlement. This option enables you to determine the effective home site for a user and global entitlement combination, which might be different from the home site that is configured for the user.
`--userName`	Name of the user whose home site you want to list. Use the format *domain\username*.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--resolveUserHomeSite --userName domainEast\adminEast
```

Listing Dedicated Desktop Pool Assignments

Use the `lmvutil` command with the `--listUserAssignments` option to to list the dedicated desktop pool assignments for a user and global entitlement combination.

Syntax

`lmvutil --listUserAssignments {--userName` *`domain\username`* `| --entitlementName` *`name`* `| --podName` *`name`* `| --siteName` *`name`*`}`

Usage Notes

The data produced by this command is managed internally by the Cloud Pod Architecture brokering software.

This command returns an error if the Cloud Pod Architecture feature is not initialized or if the command cannot find the specified user, global entitlement, pod, or site.

Options

You must specify one of the following options when you list user assignments.

Table 5-19. Options for Listing User Assignments

Option	Description
`--userName`	Name of the user for whom you want to list assignments. Use the format *domain\username*. This option lists the global entitlement, pod, and site assignments for the specified user.
`--entitlementName`	Name of a global entitlement. This option lists the users assigned to the specified global entitlement.
`--podName`	Name of a pod. This option lists the users assigned to the specified pod.
`--siteName`	Name of a site. This option lists the users assigned to the specified site.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword
"*" --listUserAssignments --podName "East Pod 1"
```

Listing the Pods or Sites in a Cloud Pod Architecture Topology

To view the pods in the pod federation, use the `lmvutil` command with the `--listPods` option. To view the sites in the pod federation, use the `lmvutil` command with the `--listSites` option.

Syntax

```
lmvutil --listPods
```

```
lmvutil --listSites
```

Usage Notes

These commands return an error message if the Cloud Pod Architecture feature is not initialized or if the commands cannot list the pods or sites.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listPods
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listSites
```

Managing SSL Certificates

You can use `lmvutil` command options to create and activate pending SSL certificates in a Cloud Pod Architecture environment.

The Cloud Pod Architecture feature uses signed certificates for bidirectional SSL to protect and validate the VIPA communication channel. The certificates are distributed in the Global Data Layer. The Cloud Pod Architecture feature replaces these certificates every seven days.

To change a certificate for a specific Connection Server instance, you create a pending certificate, wait for the Global Data Layer replication process to distribute the certificate to all Connection Server instances, and activate the certificate.

The `lmvutil` command certificate options are intended for use only if a certificate becomes compromised and a Horizon administrator wants to update the certificate sooner than seven days. These options affect only the Connection Server instance on which they are run. To change all certificates, you must run the options on every Connection Server instance.

- Creating a Pending Certificate on page 67

  Use the `lmvutil` command with the `--createPendingCertificate` option to create a pending SSL certificate.

- Activating a Pending Certificate on page 67

  Use the `lmvutil` command with the `--activatePendingCertificate` option to activate a pending certificate.

Creating a Pending Certificate

Use the `lmvutil` command with the `--createPendingCertificate` option to create a pending SSL certificate.

Syntax

```
lmvutil --createPendingCertificate
```

Usage Notes

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the command cannot create the certificate.

Example

```
LMVUtil --authAs adminEast --authDomain domainEast --authPassword "*"
--createPendingCertificate
```

Activating a Pending Certificate

Use the `lmvutil` command with the `--activatePendingCertificate` option to activate a pending certificate.

Syntax

```
lmvutil --activatePendingCertificate
```

Usage Notes

You must use the `lmvutil` command with the `––createPendingCertificate` option to create a pending certificate before you can use this command. Wait for the Global Data Layer replication process to distribute the certificate to all Connection Server instances before you activate the pending certificate. VIPA connection failures and resulting brokering problems can occur if you activate a pending certificate before it is fully replicated to all Connection Server instances.

This command returns an error message if the Cloud Pod Architecture feature is not initialized or if the command cannot activate the certificate.

Example

```
lmvutil ––authAs adminEast ––authDomain domainEast ––authPassword "*"
––activatePendingCertificate
```

Index