Cloud Pod Architecture in Horizon

VMware Horizon 2209

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

https://docs.vmware.com/

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

Contents

Cloud Pod Architecture in Horizon

Cloud Pod Architecture in Horizon describes how to configure and manage a Cloud Pod Architecture environment in VMware Horizon®.

Intended Audience

This document is written for experienced Windows and Linux system administrators who are familiar with virtual machine technology and data center operations.

Introduction to Cloud Pod Architecture

1

The Cloud Pod Architecture feature uses standard VMware Horizon components to provide cross-data center 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

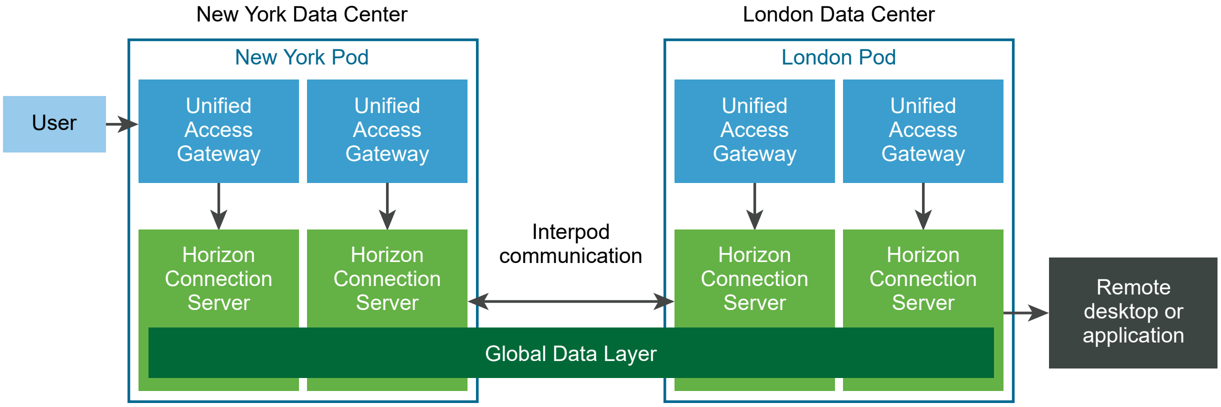
With the Cloud Pod Architecture feature, you can link together multiple pods to provide a single large desktop and application brokering and management environment.

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 8 implementation, you manage each pod independently. With the Cloud Pod Architecture feature, you can join together multiple pods to form a single Horizon 8 implementation called a pod federation.

A pod federation can span multiple sites and data centers and simultaneously simplify the administration effort required to manage a large-scale Horizon 8 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 data centers are joined together to form a single pod federation. An end user in this environment can connect to the New York pod and receive a desktop or application in either pod.

When using Cloud Pod Architecture with Unified Access Gateway appliances, each appliance must be associated with a single pod.

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.

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. VMware Horizon 8 configures the VIPA communication channel when you initialize the Cloud Pod Architecture feature.

Configuring and Managing a Cloud Pod Architecture Environment

You use Horizon Console or the `lmvutil` command-line interface to set up and manage a Cloud Pod Architecture environment. `lmvutil` is installed as part of the VMware Horizon 8 installation. You can also use Horizon Console to view pod health and session information.

Cloud Pod Architecture Domain Requirements

The Cloud Pod Architecture feature has certain domain requirements.

- If pods span multiple Active Directory domains, you must configure a two-way trust between the domains.
- Untrusted domains need to be configured separately for each pod.

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 VMware Horizon 8 implementation. If you are joining existing HorizonHorizon 8 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 data center. 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 data centers to different sites and entitle users and groups to pools that span those sites. If a data center 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 VMware Horizon 8 environment, you use Horizon Console 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 8 looks for desktops or applications when it allocates desktops or applications to users in the global entitlement. It also determines whether Horizon 8 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, VMware Horizon 8 searches for an available desktop or application in the pools that are associated with that global entitlement. By default, Horizon 8 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 8 uses the default search behavior only the first time a user requests a desktop. After Horizon 8 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 VMware Horizon 8 looks for desktops or applications to satisfy a request from the global entitlement.

You can set the scope policy so that Horizon 8 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 8 looks for desktops the first time a user requests a dedicated desktop. After Horizon 8 allocates a dedicated desktop, it returns the user directly to the same desktop.

Understanding the Multiple Sessions Per User Policy for Global Desktop Entitlements

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 desktop 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 desktop entitlement, all of the desktop pools associated with the global desktop 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, VMware Horizon 8 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 8 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 8 looks for desktops the first time a user requests a dedicated desktop. After Horizon 8 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 8 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 8 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 8 searches for and allocates desktops and applications as described in Finding and Allocating Desktops and Applications in the Pod Federation.

Considerations for Unauthenticated Users

A VMware 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 Console.
- 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 Console 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.

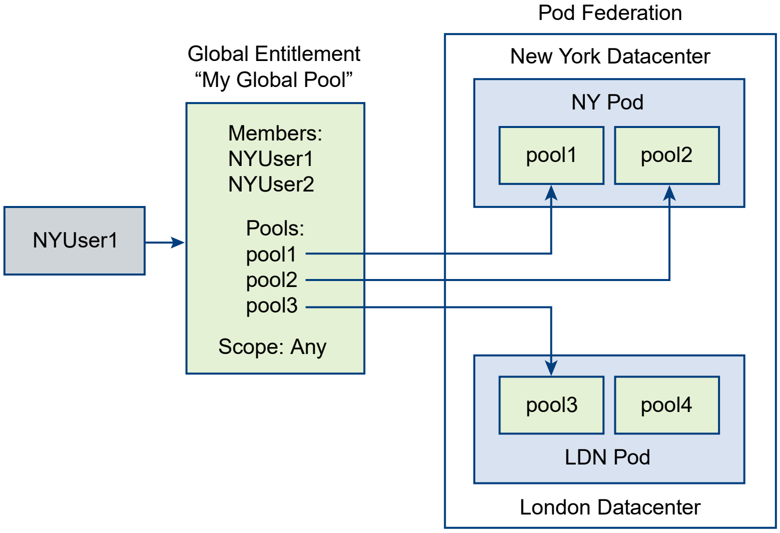
- Unauthenticated access users are not entitled to global application entitlements that have applications published from a desktop pool.

For information about setting up unauthenticated users, see the *Horizon 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 data center and pool3 and pool4 are in a pod called LDN Pod in the London data center.

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 Connection Server Restrictions Example.

Implementing Connection Server Restrictions for Global Entitlements

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

With the Connection Server restrictions feature, 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 Connection Server restrictions 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. Tag Matching Rules 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 Connection Server restrictions feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular Connection Server instance.

Requirements and Limitations for Connection Server Restrictions

Before implementing Connection Server restrictions for global entitlements, you must be aware of certain requirements 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 Unified Access Gateway appliance, you must configure restrictions on the Connection Server instance with which the Unified Access Gateway appliance is paired. You cannot configure restrictions on a Unified Access Gateway appliance.

- Connection Server restrictions 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 Workspace ONE Access and you configure Connection Server restrictions, the VMware Workspace ONE Access app might display global entitlements to users when the global entitlements are actually restricted. When a VMware Workspace ONE Access 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.

Connection Server Restrictions 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 Unified Access Gateway appliance and supports external users.

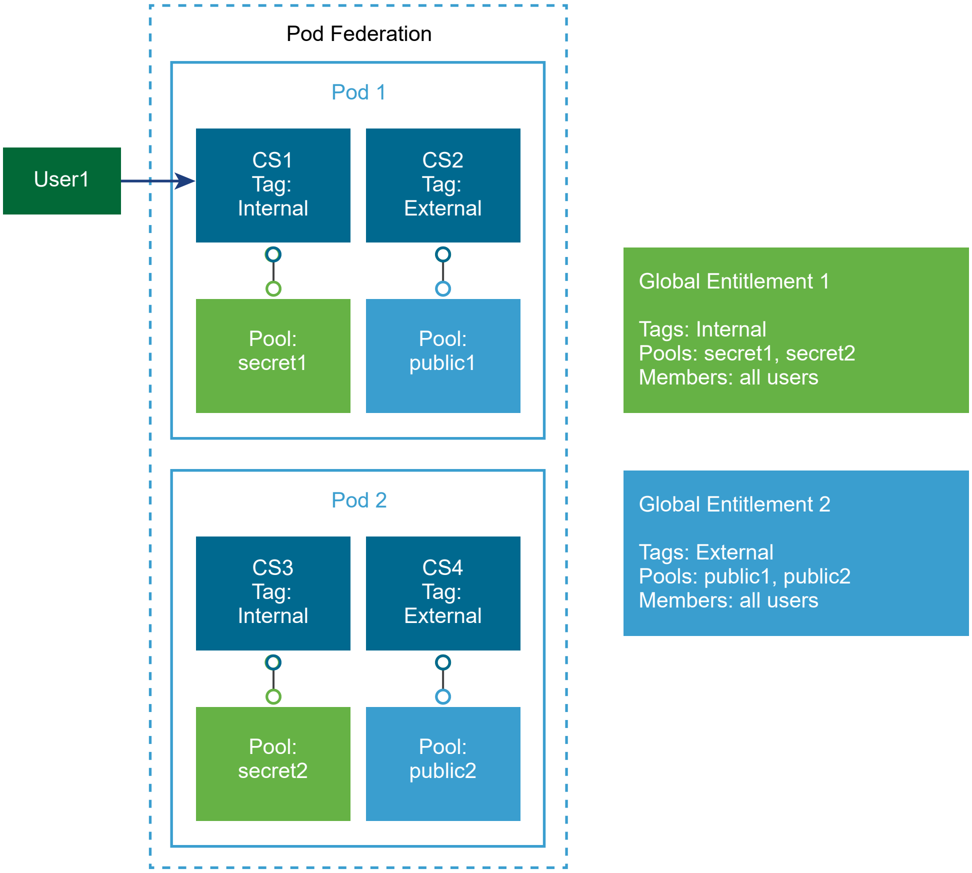
To prevent external users from accessing certain desktop and application pools, you could assign tags as follows:

- 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. Connection Server Restrictions Example



Implementing Client Restrictions for Global Entitlements

You can restrict access to global entitlements to specific client computers. To restrict access, you add the names of the client computers that are allowed to access a global entitlement in an Active Directory security group and then add this group to the global entitlement's users and groups.

The client restrictions features has certain requirements and limitations.

- You must enable the client restrictions policy when you create or modify the global entitlement. By default, the client restrictions policy is disabled. You can enable this policy only for floating desktop entitlements and global application entitlements.
- The global entitlement client restrictions policy setting overrides the pool-level client restrictions policy setting. As a best practice, if you enable the client restrictions policy on a global entitlement, do not enable the client restrictions policy on the pools that the global entitlement contains.
- You must add the Active Directory security group that contains the names of the client computers that are allowed to access the global entitlement when you create or modify the global entitlement.

- The client restrictions feature allows only specific client computers to access global entitlements. It does not give users access to global entitlements. For example, if a user is not included in a global entitlement (either as a user or as a member of a user group), the user cannot access the global entitlement, even if the user's client computer is allowed to access the global entitlement.
- The client restrictions feature is supported only with Windows client computers in this release.
- When the client restrictions policy is enabled for a global entitlement, non-Windows clients and HTML Access clients cannot launch the global entitlement.

Implementing the Session Pre-Launch Feature for Global Application Entitlements

With the session pre-launch feature, a Horizon administrator can configure a published application so that the session starts before a user opens the application in Horizon Client. The session pre-launch feature enables faster start times for frequently used published applications.

You can enable the session pre-launch feature for a global application entitlement by enabling the pre-launch policy when you create or modify the global application entitlement. All the application pools in the global application entitlement must support the session pre-launch feature, and the pre-launch session timeout must be the same for all farms.

For information about configuring application pools and farms to use the session pre-launch feature, see the *Windows Desktops and Applications in Horizon* document.

The session pre-launch feature is not supported for remote desktops.

Enabling Multi-Session Mode for Global Application Entitlements

When you create a global application entitlement, you can specify whether users can start multiple sessions of the same published application on different client devices. This feature is called multi-session mode.

For example, if a user opens a published application in multi-session mode on client A, and then opens the same published application on client B, the published application remains open on client A and a new session of the published application opens on client B. By comparison, if the user opens the published application on client A in single-session mode, the session on client A is disconnected and reconnected on client B.

When you enable multi-session mode, you can specify whether it is on by default, off by default, or enforced.

- When multi-session mode is on or off by default, users that have Horizon Client can disable or enable multi-session mode by modifying the **Multi-Launch** setting on the client. Users that have earlier versions of Horizon Client cannot change the default setting.

- When multi-session mode is enforced, it is always on and users cannot disable it in Horizon Client.

For more information about using the **Multi-Launch** setting, see the Horizon Client documentation.

The multi-session mode feature has the following requirements and limitations for global application entitlements.

- The multi-session mode setting that you configure for the global application entitlement must match the setting that is configured for the application pools associated with the global application entitlement. For information about enabling multi-session mode for application pools, see the *Windows Desktops and Applications in Horizon* document.
- You cannot enable the session pre-launch feature for the global application entitlement, or the application pools associated with the global application entitlement, when multi-session mode is enabled. The session pre-launch feature is not supported when multi-session mode is enabled.

Enabling Session Collaboration for Global Desktop Entitlements

With the Session Collaboration feature, end users can invite other users to join an existing remote desktop session.

To enable remote desktop users to collaborate, a Horizon administrator must enable the Session Collaboration feature for the desktop pool that provides the remote desktop. For RDS desktop pools, a Horizon administrator must enable the Session Collaboration feature for the farm on which the RDS desktop pool is based.

To enable invited users to join sessions from pods other than the session owner's pod, you must enable the Session Collaboration policy for the global desktop entitlement that contains the desktop pool when you create or modify the global desktop entitlement.

For complete Session Collaboration feature requirements and limitations, including licensing requirements, see "Configuring Session Collaboration" in the *Horizon Remote Desktop Features and GPOs* document.

Session Collaboration is not supported for published applications.

Implementing Backup Global Entitlements

When you edit a global desktop entitlement or global application entitlement, you can select a backup global entitlement. A backup global entitlement delivers remote desktops or published applications when the primary global entitlement fails to start a session because of problems such as insufficient pool capacity or unavailable pods. A backup global entitlement can contain pools from any pod in the pod federation.

The following backup global entitlement settings must match the corresponding primary global entitlement settings.

- User assignment type
- Default display protocol (only if users are not allowed to select the display protocol)
- Supported display protocols
- Allow users to restart machines
- Allow users to initiate separate sessions from different client devices
- Allow Session Collaboration

Backup global entitlement have the following restrictions and limitations.

- For global desktop entitlements, you can configure a backup global entitlement only if the user assignment policy is set to Floating.
- After you configure a backup global entitlement, the edit functionality, user entitlements, and home site override setting for the backup global entitlement are disabled.
- You cannot select an existing primary or backup global entitlement when you select a backup global entitlement.
- A backup global entitlement cannot be cloud managed.
- A backup global entitlement cannot be associated with any user or group entitlements.

For information about editing a global entitlement, see Modify Attributes or Policies for a Global Entitlement.

Considerations for Mixed-Version Environments

Mixed-version Cloud Pod Architecture environments are supported beginning with Horizon 7 version 7.4.

New features do not work in a mixed-version environment. For example, a new feature that is visible in Horizon Console for a VMware Horizon 2006 Connection Server instance is not visible in Horizon Console for a Horizon 7 version 7.5 Connection Server instance. VMware recommends that you upgrade all pods to the same VMware Horizon version.

Considerations for Workspace ONE Mode

If a Horizon administrator enables Workspace ONE mode for a Connection Server instance, Horizon Client users can be redirected to a Workspace ONE server to launch their entitlements.

During Workspace ONE mode configuration, a Horizon administrator specifies the host name of the Workspace ONE server. In a Cloud Pod Architecture environment, every pod in the pod federation must be configured to point to the same Workspace ONE server.

For information about configuring Workspace ONE mode, see the *Horizon Administration* document.

Considerations for VMware Cloud on AWS

You can deploy VMware Horizon in a hybrid cloud environment when you use Cloud Pod Architecture to interconnect VMware Horizon on-premises and VMware Horizon pods on VMware Cloud on AWS. You can entitle users to virtual desktops and published applications on-premises and on VMware Cloud on AWS.

For more information, see "Architecting Horizon Cloud Pod Architecture (CPA) for VMware Cloud on AWS " in the *Horizon 7 on VMware Cloud on AWS Deployment Guide* document at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf.

Considerations for RDS Per-Device Client Access Licensing

When a Windows client device connects to a published desktop or application on an RDS host, it receives an RDS Per-Device Client Access License (CAL), if the Per-Device licensing mode is configured on the RDS host. By default, the CAL is stored only on the client device.

If the client device has a license, it always presents that license. If the client device does not present a license, the most up-to-date license that can be found on any pod involved in the published desktop or application launch is used. If a license cannot be found on any pod involved in the launch, the client device's ID is presented to the license server and a license is issued.

Important VMware recommends that you upgrade to the latest Windows client and server software for the best handling of RDS licensing.

For more information, see "Understanding RDS Per-Device Client Access Licensing in Horizon" in the *Windows Desktops and Applications in Horizon* document.

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.

The following table shows the total number of sessions that are supported in this release.

Table 2-2. Pod Federation Limits

Object	Limit
Total sessions	250,000
Pods	50
Sessions per pod	12,000
Sites	15

Table 2-2. Pod Federation Limits (continued)

Object	Limit
Connection Server instances per pod	7
Total Connection Server instances	350

The limits for pods, sites, and total Connection Server instances indicate the maximum supported number for each component in the pod federation. As long as the configuration remains within the specified limits, you can design a suitable topology to achieve the total number of sessions.

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.

Note Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Server instances. These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication. For more information about the dynamic range of ports, see the Microsoft Windows Server documentation.

Security Considerations for Cloud Pod Architecture

To use Horizon Console or `lmvutil` commands to configure and manage a Cloud Pod Architecture environment, you must have certain roles or privileges.

To access the following pages and tabs in Horizon Console, you must have the Administrators (Read only) role on the root access group, or, at a minimum, the **Manage Cloud Pod Architecture** privilege:

- **Cloud Pod Architecture** and **Sites** pages in **Settings**

- **Global Entitlements** page in **Inventory**
- **Home Site Assignment** and **Home Site Resolution** tabs on the **Users and Groups** page

To perform operations on the following pages and tabs in Horizon Console, you must have the Administrators role on the root access group, or, at a minimum, the **Manage Cloud Pod Architecture** privilege:

- **Cloud Pod Architecture** and **Sites** pages in **Settings**
- **Global Entitlements** page in **Inventory**
- **Home Site Assignment** tab on the **Users and Groups** page

If you can access the **Home Site Resolution** tab, you can also look up the home site resolution for a user. No additional privileges are required.

To join an active pod federation on pod Y from pod X, you must have the credentials of the administrator that installed Connection Server Y. The credentials of an administrator with only the **Manage Cloud Pod Architecture** privilege on pod Y are not sufficient to perform this action.

For complete information about permissions, privileges, and roles, see the *Horizon Administration* document.

Setting Up Cloud Pod Architecture in Horizon Console 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 shows how to set up a Cloud Pod Architecture environment in Horizon Console. For information about using the `lmvutil` command-line interface, see Chapter 6 Administering Cloud Pod Architecture with lmvutil.

This chapter includes the following topics:

- Initialize the Cloud Pod Architecture Feature
- Join a Pod to the Pod Federation
- Assign a Tag to a Connection Server Instance
- Configuring Shortcuts for Global Entitlements
- Worksheet for Configuring a Global Entitlement
- Create and Configure a Global Entitlement
- Add a Pool to a Global Entitlement
- Create and Configure a Site
- Assign a Home Site to a User or Group
- Create a Home Site Override
- Test a Cloud Pod Architecture Configuration in Horizon Client
- Example: Setting Up a Basic Cloud Pod Architecture Configuration

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, VMware Horizon 8 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.

Connection Server creates federation access group permissions on the root federation access group for all authorized administrators automatically.

Procedure

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

2 Select **Settings > Cloud Pod Architecture**, click **Initialize the Cloud Pod Architecture feature**, and click **OK** to start the initialization process.

   Horizon Console shows the progress of the initialization process. 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.

3 (Optional) To change the default name of the pod federation, click **Edit**, type the new name in the **Name** text box, and click **OK**.

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

5 (Optional) To change the default name of the site, select **Settings > 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.

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 Console to join additional pods to the pod federation. Joining additional pods is optional.

Global entitlements, global sessions, and federation access groups are replicated from the pods in the pod federation. Connection Server creates federation access group permissions on the root federation access group for all authorized administrators automatically.

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.

Procedure

1 Log in to the Horizon Console user interface for any Connection Server in the pod that you are joining to the pod federation.

2 Select **Settings > Cloud Pod Architecture** and click **Join the pod federation**.

3 In the **Connection Server (host name or IP address)** 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 (domain/username)** 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 To join the pod to the pod federation, click **OK**.

   Horizon Console 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.

Results

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 Console. See Review Pod Federation Health.

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

What to do next

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

Assign a Tag to a Connection Server Instance

If you plan to restrict access to a global entitlement based on the Connection Server instance that users initially connect to when they select the global entitlement, you must first assign one or more tags to the Connection Server instance.

Prerequisites

Become familiar with the Connection Server restrictions feature. See Implementing Client Restrictions for Global Entitlements.

Procedure

1 Log in to the Horizon Console user interface for the Connection Server instance.

2 Select **Settings > Servers**.

3 Click the **Connection Servers** tab, select the Connection Server instance, and click **Edit**.

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

Separate multiple tags with a comma or semicolon.

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

6 Repeat these steps for each Connection Server instance to which you want to assign tags.

What to do next

When you create or edit a global entitlement, select the tags that are associated with the Connection Server instances that you want to access the global entitlement. See Create and Configure a Global Entitlement or Modify Attributes or Policies for a Global Entitlement.

Configuring Shortcuts for Global Entitlements

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

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

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

On Mac clients, if Horizon Client for Mac is configured to run published applications from the `Applications` folder and allow automatic shortcuts from the server, category folders for global application entitlements appear in the `Applications` folder on the Mac client.

After you create a shortcut, a check mark appears in the App Shortcut column for the global entitlement on the Global Entitlements page in Horizon Console.

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

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

Worksheet for Configuring a Global Entitlement

When you create a global entitlement in Horizon Console, the user interface prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the global entitlement.

You can print this worksheet and write down the values to specify when you add a global entitlement.

Table 3-1. Worksheet: Options for Configuring a Global Entitlement

Option	Description	Fill In Your Value Here
Name	Unique name that identifies the global entitlement in Horizon Console. The name can contain between 1 and 64 characters.	
Display Name	(Optional) Display name of the global entitlement. The display name appears to users in the list of available desktops and applications in Horizon Client. The display name does not need to be unique. Multiple global entitlements can have the same display name. If you do not specify a display name, the unique name appears to users in Horizon Client. The display name can contain between 1 and 64 characters.	
Federation Access Group	Associates the global entitlement and its sessions with a federation access group. Federation access groups enable you to delegate the administration of specific global entitlements and global sessions to different administrators. The default setting is the root federation access group. For more information, see Chapter 4 Setting Up Federation Access Groups in Horizon Console.	
Description	(Optional) Description of the global entitlement. The description can contain between 1 and 1024 characters.	
Connection Server Restrictions	(Optional) Associates Connection Server tags with the global entitlement to restrict access to the global entitlement from specific Connection Server instances. **Note** You can select only tags that are assigned to Connection Server instances in the local pod. To select tags assigned to Connection Server instances in another pod, you must log in to a Connection Server instance in the other pod and modify the global entitlement. For more information, see Implementing Connection Server Restrictions for Global Entitlements.	

Table 3-1. Worksheet: Options for Configuring a Global Entitlement (continued)

Option	Description	Fill In Your Value Here
Category Folder	(Optional) Creates a shortcut for the global entitlement. You can select an existing category folder, or create a category folder. You can configure up to four subfolders. You can configure a Windows Start menu shortcut, a desktop shortcut, or both. A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords. For more information, see Configuring Shortcuts for Global Entitlements.	
Backup Global Entitlement	(Only available when you edit a global entitlement) A backup global entitlement delivers remote desktops or published applications when the primary global entitlement cannot start a session. For requirements and restrictions, see Implementing Backup Global Entitlements.	
User Assignment	(Global desktop entitlement only) Specifies the type of desktop pool that the global entitlement can contain. You can configure one of the following user assignment policies: ■ **Floating** - the global entitlement contains only floating desktop pools. ■ **Dedicated** - the global entitlement contains only dedicated desktop pools.	
Scope	Specifies where to look for desktops or applications to satisfy a request from the global entitlement. You can configure one of the following scope policies: ■ **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. For more information, see Understanding the Scope Policy.	

Table 3-1. Worksheet: Options for Configuring a Global Entitlement (continued)

Option	Description	Fill In Your Value Here
Use Home Site and **Entitled user must have Home Site**	(Optional) If users have home sites, configures a home site policy for the global entitlement. You can configure the following home site policies: ■ **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 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. For more information, see Using Home Sites.	
Automatically Clean Up Redundant Sessions	(Optional) Specifies whether to clean up redundant sessions. 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. You can configure **PCoIP** or **VMware Blast**.	
Allow Users to Choose Protocol	When you enable this policy, users can override the default display protocol.	
Allow Users to Restart Machines	(Global desktop entitlement only) When you enable this policy, users can reset and restart desktops in the global desktop entitlement.	
Pre-launch	(Global application entitlement only) When you enable this policy, users can start the global application entitlement more quickly. **Note** If you enable this policy, all the application pools in the global application entitlement must also support the session pre-launch feature, and the pre-launch session timeout must be the same for all farms.	

Table 3-1. Worksheet: Options for Configuring a Global Entitlement (continued)

Option	Description	Fill In Your Value Here
Allow Session Collaboration	When you enable this policy, users can invite other users to join their remote desktop sessions. **Note** If you enable this policy, all the desktop pools in the global desktop entitlement must also support the Session Collaboration feature. For RDS desktop pools, the Session Collaboration feature is enabled at the farm level. For more information, see Enabling Session Collaboration for Global Desktop Entitlements.	
Allow user to initiate separate sessions from different client devices	(Global desktop entitlement only) When you enable this 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. You can enable this policy only for floating desktop entitlements. **Note** If you enable this policy, all the desktop pools in the global entitlement must also support multiple sessions per user. For more information, see Understanding the Multiple Sessions Per User Policy for Global Desktop Entitlements.	
Client Restrictions	When you enable this policy, access to the global entitlement is restricted to specific client computers. You can enable this policy only for floating desktop entitlements and global application entitlements. You must add the names of the computers that are allowed to access the global entitlement in an Active Directory security group. You can select this security group when you add users or groups to the global entitlement. For more information, see Implementing Client Restrictions for Global Entitlements.	

Table 3-1. Worksheet: Options for Configuring a Global Entitlement (continued)

Option	Description	Fill In Your Value Here
Multi-Session Mode	(Global application entitlement only) Use this policy to configure the multi-session mode feature for a global application entitlement. Valid values are as follows. ■ **Disabled** - Multi-session mode is not supported. ■ **Enabled (Default Off)** - Multi-session mode is supported, but it is disabled by default. To use multi-session mode, users must enable the **Multi-Launch** setting in Horizon Client 4.10 or later. For users that have an earlier version of Horizon Client, the application is always started in single-session mode. ■ **Enabled (Default On)** - Multi-session mode is supported, and it is enabled by default. Users can disable multi-session mode by disabling the **Multi-Launch** setting in Horizon Client 4.10 or later. For users that have an earlier version of Horizon Client, the application is always started in single-session mode. ■ **Enabled (Enforced)** - Multi-session mode is supported, and the application is always started in multi-session mode. Users cannot disable multi-session mode by disabling the **Multi-Launch** setting in Horizon Client 4.10 or later. Users that have an earlier version of Horizon Client receive an error message that states that the requested start mode is not supported. For more information, see Enabling Multi-Session Mode for Global Application Entitlements.	
Show Assigned Machine Name	(Global desktop entitlement only) Displays the host name of the assigned machine instead of the global entitlement name in Horizon Client. If no machine is assigned to the user, "Entitlement name (No Machine Assigned)" appears for the global entitlement in Horizon Client. **Note** If the pod that contains the machine is unavailable or does not reply in time, Connection Server cannot get the assigned machine name. In such cases, "Entitlement name (Unable to get machine name)" appears instead of the global entitlement name in Horizon Client. This option is available only if you select **Dedicated** in **User assignment**.	
Show Machine Alias Name	(Global desktop entitlement only) Displays the alias name of the assigned machine instead of the global entitlement name in Horizon Client. If no machine alias name is set, the host name of the assigned machine appears in Horizon Client. This option is available only if you select **Dedicated** in **User assignment**.	

Create and Configure a Global Entitlement

You can use Horizon Console to create and configure global entitlements. Global entitlements 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 set of policies, and a list of the pools that can provide desktops or applications for entitled users. You can add both users and groups, only users, or only groups, to a global entitlement.

Prerequisites

- Initialize the Cloud Pod Architecture feature. See Initialize the Cloud Pod Architecture Feature.
- Decide which type of global desktop entitlement to create and the users and groups to include in the global entitlement. See Entitling Users and Groups in the Pod Federation.
- Decide which options to configure for the global entitlement. See Worksheet for Configuring a Global Entitlement.

Procedure

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

2 Select **Inventory > Global Entitlements** and click **Add**.

3 Select the type of global entitlement to add.

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

4 Click **Next** and follow the prompts to configure the global entitlement.

Use the configuration information that you gathered in the global entitlement configuration worksheet.

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

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

   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.

      To restrict access to the global entitlement to specific client computers, select the Active Directory security group that contains the names of the computers that are allowed to access the global entitlement.

      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.

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

   The global entitlement appears on the Global Entitlements page.

Results

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.

What to do next

Select the pools that can provide desktops or applications for the users in the global entitlement that you created. See Add a Pool to a Global Entitlement

Add a Pool to a Global Entitlement

You can use Horizon Console 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 multiple pools to a global entitlement, but you can add a particular pool to only one global entitlement.

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.

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.

For global desktop entitlements, the user interface lets you add a local desktop pool only if the following properties match.

- User assignment
- Support for desktop sessions
- Session collaboration (desktop pool should have session collaboration enabled when global desktop entitlement has it enabled)
- Allow user to initiate separate sessions from different client devices for desktop pools with floating user assignment
- If Allow users to choose protocol is set to no, the display protocols match
- A desktop pool that disallows user to restart or reset machines cannot be associated with a global desktop entitlement that allows users to restart or reset machines

For global application entitlements, the user interface lets you add a local application pool only if the following properties match.

- Multi-session mode
- If Allow users to choose protocol is set to no, the display protocols match

Even if the local pool configuration matches the global entitlement configuration, you can add a local pool only if the logged in administrator has privileges to view the local pool.

Prerequisites

- Create and configure the global entitlement. See Create and Configure a Global Entitlement.
- Create the desktop or application pool to add to the global entitlement. See the *Windows Desktops and Applications in Horizon* document.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod that contains the pool to add to the global entitlement.
2. Select **Inventory > Global Entitlements**.
3. Click the global entitlement name.
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.
5. Repeat these steps on a Connection Server instance in each pod that contains a pool to add to the global entitlement.

Results

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.

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.
- Initialize the Cloud Pod Architecture feature. See Initialize the Cloud Pod Architecture Feature.

Procedure

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

2 Create the site.

  a In Horizon Console, select **Settings > 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 To create the site, click **OK**.

3 Add a pod to the site.

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

  a In Horizon Console, select **Settings > Sites**.

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

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

  d 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, VMware Horizon 8 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.

Prerequisites

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

Procedure

1. Log in to the user interface for any Connection Server instance in the pod federation.
2. Select **Users and Groups**, click the **Home Site Assignment** tab, and click **Add**.
3. To filter the users or groups based on your search criteria, select one or more search criteria and click **Find**.

   You can select the **Unauthenticated Users** check box to find unauthenticated access users in the pod federation.
4. Select a user or group and click **Next**.
5. Select the home site to assign to the user or group from the **Home Site** drop-down menu and click **Submit**.

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, VMware Horizon 8 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.

- 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.

Procedure

1. Log in to the user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**.
3. Select the name of the global entitlement to associate with a home site and click the **Home Site Override** tab.
4. Click **Add**.

   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 and click **Next**.

   The user or group must already be included in the global entitlement that you selected.
7. Select the home site to associate with the global entitlement from the **Home Site Override** drop-down menu and click **Submit**.

Test a Cloud Pod Architecture Configuration in Horizon Client

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 remote desktop or published application.

Results

The remote desktop or published application starts successfully. Which remote desktop or published 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 remote desktop or published 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 Console to verify that the entitlement is configured correctly. If the global entitlement appears, but a remote desktop or published 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 data centers.

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 data center 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.

Procedure

1 Designing the Example Topology

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

2 Initializing the Example Configuration

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

3 Joining Pods in the Example Configuration

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

4 Creating Sites in the Example Configuration

The Horizon administrator uses Horizon Console to create a site for the Eastern and Central data centers and adds pods to those sites.

5 Creating Global Desktop Entitlements in the Example Configuration

The Horizon administrator uses Horizon Console 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.

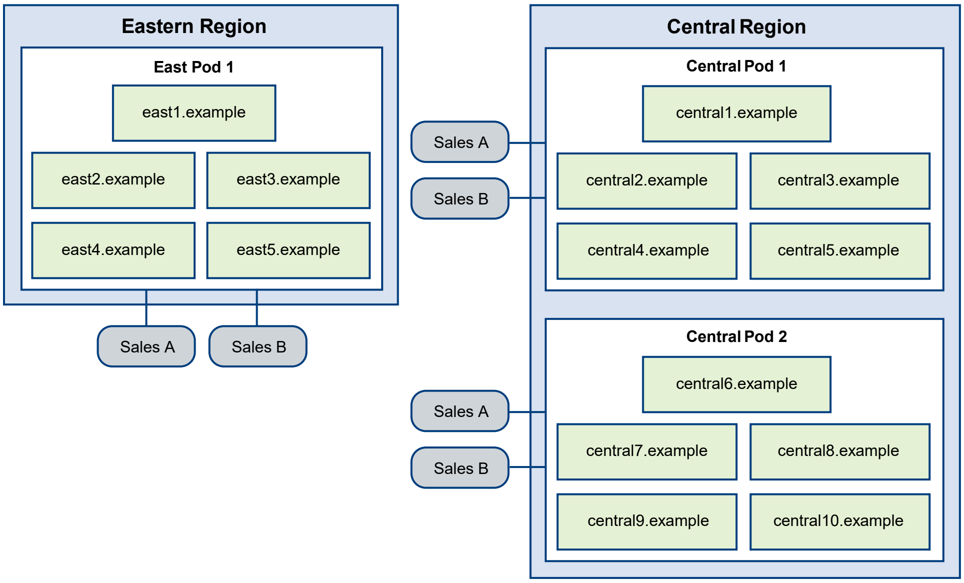
6 Creating a URL for the Example Configuration

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 Console user interface for a Connection Server instance in East Pod 1, selects **Settings > Cloud Pod Architecture**, and clicks **Initialize the Cloud Pod Architecture feature**.

Because the Horizon administrator uses the Horizon Console 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 Console 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 Console user interface for a Connection Server instance in Central Pod 1, selects **Settings > 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 Console user interface for a Connection Server instance in Central Pod 2, selects **Settings > 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 Console to create a site for the Eastern and Central data centers and adds pods to those sites.

1 The Horizon administrator logs in to the Horizon Console user interface for any Connection Server instance in the pod federation.

2 To create a site for the Eastern data center, the Horizon administrator selects **Settings > Sites** and clicks **Add**.

3 To create a site for the Central data center, the Horizon administrator selects **Settings > Sites** and clicks **Add**.

4 To move East Pod 1 to the site for the Eastern data center, the Horizon administrator selects **Settings > Sites**, selects the site that currently contains East Pod 1, selects East Pod 1, clicks **Edit**, and selects the Eastern data center site from the **Site** drop-down menu.

5 To move Central Pod 1 to the site for the Central data center, the Horizon administrator selects **Settings > Sites**, selects the site that currently contains Central Pod 1, selects Central Pod 1, clicks **Edit**, and selects the Central data center site from the **Site** drop-down menu.

6 To move Central Pod 2 to the site for the Central data center, the Horizon administrator selects **Settings > Sites**, selects the site that currently contains Central Pod 2, selects Central Pod 2, clicks **Edit**, and selects the Central data center 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 Console 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 add users to the global desktop entitlement, the Horizon administrator logs in to the Horizon Console user interface for a Connection Server in the pod federation, selects **Inventory > Global Entitlements**, clicks the **Users and Groups** tab, and clicks **Add Entitlements**.

   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 Console user interface for a Connection Server instance in East Pod 1, selects **Inventory > Global Entitlements**, clicks the global desktop entitlement name, 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 Console user interface for a Connection Server instance in Central Pod 1, selects **Inventory > Global Entitlements**, clicks the global desktop entitlement name, 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 Console user interface for a Connection Server instance in Central Pod 2, selects **Inventory > Global Entitlements**, clicks the global desktop entitlement name, 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.

Setting Up Federation Access Groups in Horizon Console

4

With federation access groups, you can segregate sensitive global entitlements and delegate the administration of those global entitlements to a limited set of users. Setting up federation access groups is optional.

Federation access groups are available only in a Cloud Pod Architecture environment.

This chapter includes the following topics:

Understanding Federation Access Groups

By default, global entitlements are created in the root federation access group, which appears as / or Root(/) in Horizon Console. You can create federation access groups under the root federation access group to delegate the administration of specific global entitlements to different administrators.

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

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

To apply to a federation access group, a role must contain at least one object-specific privilege that is applicable to federation access groups. You cannot apply roles that contain only global privileges or access group-specific privileges to federation access groups. For complete information about privileges, privilege scope, and roles in HorizonVMware Horizon 8, see "Configuring Role-Based Delegate Administration" in the *Horizon Administration* document.

You can use Horizon Console to configure and manage federation access groups. When you create a global entitlement, you can accept the default root federation access group or select a different federation access group.

Different Administrators for Different Federation Access Groups

You can create a different administrator to manage the global entitlements and global sessions in each federation access group in your Cloud Pod Architecture configuration.

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

In the following example, the administrator called Admin1 has the Administrators role on the federation access group called CorporateGlobalEntitlements, and the administrator called Admin2 has the Administrators role on the federation access group called DeveloperGlobalEntitlements.

Administrator	Role	Federation Access Group
view-domain.com\Admin1	Administrators	/CorporateGlobalEntitlements
view-domain.com\Admin2	Administrators	/DeveloperGlobalEntitlements

Different Administrators for the Same Federation Access Group

You can create different administrators to manage the same global entitlements and global sessions in a federation access group.

For example, if your corporate global entitlements are in a single federation access group, you can create one administrator that can view and modify the global entitlements in that federation access group and another administrator that can only view the global entitlements in that federation access group.

In the following example, the administrator called Admin1 has the Administrators role on the federation access group called CorporateGlobalEntitlements, and the administrator called Admin2 has the Administrators (Read only) role on the same federation access group.

Administrator	Role	Federation Access Group
view-domain\Admin1	Administrators	/CorporateGlobalEntitlements
view-domain\Admin2	Administrators (Read only)	/CorporateGlobalEntitlements

Understanding Permissions for Federation Access Groups

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

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

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

Table 4-1. Permissions on the Administrators and Groups Tab

Role	Federation Access Group
Help Desk Administrators	`Federation_Group_1`
Administrators (Read only)	`Root(/)`

The first permission shows that Admin 1 has the Help Desk Administrators role on the federation access group called `Federation_Group_1`. The second permission shows that Admin 1 has the Administrators (Read only) role on the root federation access group.

The following table shows how the same permissions appear in Horizon Console when you select `Federation_Group_1` on the **Federation Access Groups** tab.

Table 4-2. Permissions on the Federation Access Groups Tab

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

The first permission is the same as the first permission shown in the first table. The second permission is inherited from the second permission shown in the first table. Because federation access groups inherit permissions from the root federation access group, Admin1 has the Administrators (Read only) role on `Federation_Group_1`. When a permission is inherited, a check mark appears in the **Inherited** column.

The following table shows how the permissions in the first table appear in Horizon Console when you select the Help Desk Administrators role on the **Role Permissions** tab.

Table 4-3. Permissions on the Role Permissions Tab

Administrator	Federation Access Group
horizon-domain.com\Admin1	`/Federation_Group_1`
horizon-domain.com\Admin1	`Root(/)`

Configuring Federation Access Groups

You can use Horizon Console to add federation access groups, move global entitlements to federation access groups, create custom roles to manage federation access groups, create administrators to manage federation access groups, and add permissions to federation access groups.

For information about using the `lmvutil` command-line interface to move a global entitlement to a federation access group, see Creating a Global Entitlement and Modifying a Global Entitlement.

Add a Federation Access Group

You can delegate the administration of specific global entitlements to different administrators by creating federation access groups. By default, federation access groups reside in the root federation access group.

This procedure describes how to add a federation access group from the **Global Administrators View** page in Horizon Console. Alternatively, you can add a federation access group from the **Global Entitlements** page. For more information, see Move a Global Entitlement to a Federation Access Group.

Prerequisites

- Initialize the Cloud Pod Architecture feature. See Initialize the Cloud Pod Architecture Feature.
- Determine how to use the federation access group feature in your Cloud Pod Architecture environment. See Understanding Federation Access Groups.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Settings > Administrators**.
3. On the **Federation Access Groups** tab, click **Add Federation Group**.
4. Type a name and description for the federation access group and click **OK**.

   The description is optional.

What to do next

Move one or more global entitlements to the federation access group. See Move a Global Entitlement to a Federation Access Group.

Move a Global Entitlement to a Federation Access Group

You can move one or more global entitlements to a federation access group.

Prerequisites

- Create a global entitlement. See Create and Configure a Global Entitlement.
- Create a federation access group. See Add a Federation Access Group. Alternatively, you can create the federation access group when you move the global entitlement.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**
3. Select the global entitlement.
4. Select an option from the **Federation Group** drop-down menu.

Option	Description
New Federation Access Group	If the federation access group does not yet exist, select this option to create it. You are prompted to enter a name and description for the federation access group. The description is optional.
Change Federation Access Group	To move the global entitlement to an existing federation access group, select this option. You select the federation access group from a drop-down menu.

   Alternatively, you can click **Edit** and select a federation access group from the **Federation Access Group** drop-down menu on the **Edit Global Entitlement** page.
5. To move the global entitlement to the federation access group, click **OK**.

What to do next

Add a permission to the federation access group.

Manage Global Entitlements and Global Sessions in Federation Access Groups

You can combine specific privileges to create your own custom role to manage global entitlements and global sessions in federation access groups in Horizon Console.

The role must contain at least one object-specific privilege that is applicable to federation access groups. Roles that contain only global privileges or access group-specific privileges cannot be applied to federation access groups.

Note If a role includes privileges that have Global and Federation group scope, even though the permission can be created on federation access groups for the role, internally the privileges that have Global scope are granted for assigned administrators on the root access group.

Prerequisites

- Create a federation access group. See Add a Federation Access Group.
- Become familiar with privileges, privilege scope, and roles in VMware Horizon 8. For complete information, see "Configuring Role-Based Delegated Administration" in the *Horizon Administration* document.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Settings > Administrators**.
3. On the **Role Privileges** tab, click **Add Role**.
4. Enter a name and description for the role, select one or more privileges, and click **OK**.

   The new role appears in the left pane.

Custom Role Updates in a Cloud Pod Architecture Environment

In a Cloud Pod Architecture environment, when a pod is part of a pod federation, permissions might be added or deleted automatically when a role is updated. Permissions are not created or deleted automatically when the Connection Server instance is not part of a pod federation.

The following table describes the actions that cause permissions to be added or deleted automatically.

For complete information about privileges, including privilege scopes, see "Predefined Roles and Privileges" in the *Horizon Administration* document.

Role Privilege Scope Before Update	Action	Role Privilege Scope After Update	Affect on Permissions
Federation group, All, and any other scope.	Deselect privileges that have Federation group and All scope.	Another scope, such as Access Group or Global.	Administrator permissions for the updated role on all federation access groups are removed automatically. Only permissions on access groups remain for the updated role.
Federation group and any other scope.	Deselect privileges that have Federation group scope.	Another scope, such as Access Group or Global.	Administrator permissions for the updated role on all federation groups are removed automatically. Only permissions on access groups remain for the updated role.
All and any other scope.	Deselect privileges that have All scope.	Another scope, such as Access Group or Global.	Administrator permissions for the updated role on all federation access groups are removed automatically. Only permissions on access groups remain for the updated role.
Federation group and any other scope.	Deselect privileges that have Access group, All, or Global scope.	Federation group only.	Administrator permissions for the updated role on all access groups are removed automatically. Permissions remain only on federation access groups for the updated role.
Access group and Global.	Select privileges that have All scope.	Privilege scope set now includes All.	For the administrator users or groups that have permissions on the updated role, permissions are created on the root federation access group automatically. Permissions on the access groups are not affected for the updated role.
Access group and Global.	Select privileges that have Federation group scope.	Privilege scope set now includes even Federation group.	For the administrator users or groups that have permissions on the updated role, permissions are created on the root federation access group automatically. Permissions on the access groups are not affected for the updated role.

Role Privilege Scope Before Update	Action	Role Privilege Scope After Update	Affect on Permissions
Access group and Global.	Select privileges that have All and Federation group scope.	Privilege scope set now includes All and Federation Group.	For the administrator users and groups that have permissions on the updated role, permissions are created on the root access group automatically. Permissions on the federation access groups are not affected for the updated role.
Federation group	Select privileges that have Global scope.	Privilege scope set now includes Global.	Permissions are not created on the access groups, but are internally granted to administrators that have permissions on the role. Permissions on the federation access groups are not affected for the updated role.
Federation group	Select privileges that have Access group scope.	Privilege scope set now includes Access group.	For the administrator users and groups that have permissions on the updated role, permissions are created on the root access group automatically. Permissions on the federation access group are not affected for the updated role.
Federation group	Select privileges that have All scope.	Privilege scope set now includes All.	For the administrator users and groups that have permissions on the updated role, permissions are created on the root access group automatically. Permissions on the federation access group are not affected for the updated role.

Create an Administrator to Manage a Federation Access Group

To create an administrator that can manage a federation access group, you select a user or group from your Active Directory users and groups and assign a role that is applicable to federation access groups in Horizon Console.

To apply to a federation access group, a role must contain at least one object-specific privilege that is applicable to federation access groups. Roles that contain only global privileges or access group-specific privileges do not apply to federation access groups.

Prerequisites

Create a federation access group. See Add a Federation Access Group.

Procedure

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

2 Select **Settings > Administrators**.

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

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

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

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

6 Click **Next** and select a role.

The **Federation Access Group** column indicates whether a role applies to federation access groups.

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

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

Results

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

Managing Federation Access Groups

You can use Horizon Console to add permissions for federation access groups, review the permissions for federation access groups, review the global entitlements in federation access groups, remove permissions from federation access groups, and remove federation access groups.

Add a Permission to a Federation Access Group

You add a permission to a federation access group to define the actions that can be performed on the global entitlements and global sessions in the federation access group and the administrator users or groups that can perform the actions.

When you add a permission, Horizon Console prompts you to select a role to define the actions that can be performed and a user or group that can perform the actions.

The role that you select must contain at least one object-specific privilege that is applicable to federation access groups. Roles that contain only global privileges or access-group specific privileges cannot be applied to federation access groups. For information about creating custom roles for federation access groups, see Manage Global Entitlements and Global Sessions in Federation Access Groups.

Prerequisites

- Create a federation access group. See Add a Federation Access Group.
- Become familiar with permissions. See Understanding Permissions for Federation Access Groups.

Procedure

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

2 Select **Settings > Administrators**.

3 To create a permission that includes a specific federation access group, perform these steps.

   a Select the **Federation Access Groups** tab.

   b Select the federation access group and click **Add Permissions**.

   c Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria.

   d Select an administrator user or group to include in the permission and click **OK**.

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

   e Click **Next**, select a role, and click **Finish**.

   Only roles that are applicable to federation access groups are available for selection.

4 To create a permission that includes a specific administrator user or group, perform these steps.

   a On the **Administrators and Groups** tab, select the administrator or group and click **Add Permission**.

   b Select a role that applies to federation access groups, click **Next**, select the federation access group, and click **Finish**.

   If a role is applicable to both access groups and federation access groups, you must select an access group in addition to the federation access group.

5 To create a permission that includes a specific role, perform these steps.

   a On the **Role Permissions** tab, select the role, and click **Add Permissions**.

   b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria.

   c Select an administrator user or group to include in the permission and click **OK**.

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

   d Select a role that applies to federation access groups and click **Finish**.

   If a role is applicable to both access groups and federation access groups, you must select an access group in addition to the federation access group.

Review the Permissions for a Federation Access Group

You can review the permissions for a federation access group in Horizon Console.

Procedure

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

2 Select **Settings > Administrators**.

3 To review the permissions that include a specific federation access group, perform these steps.

   a On the **Federation Access Groups** tab, select the federation access group.

   The permissions for the selected federation access group appear in the right pane.

4 To review the permissions that include a specific administrator or group, perform these steps.

   a On the **Administrators and Groups** tab, select the administrator or group.

   The permissions for the selected administrator or group appear in the right pane.

5 To review the permissions that include a specific role, perform these steps.

   a On the **Role Permissions** tab, select the role.

   The permissions for the selected role appear in the right pane.

Review the Global Entitlements in a Federation Access Group

You can view the global entitlements in a particular federation access group in Horizon Console.

Procedure

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

2 Select **Inventory > Global Entitlements**.

3 From the **Access Group** drop-down menu, select the federation access group.

Only the global entitlements in the selected federation access group are displayed.

Remove a Permission From a Federation Access Group

You can remove a permission from a federation access group in Horizon Console.

If a role that is applicable only to federation access groups comes to have administrator permissions on access groups, before you can remove the administrator permissions on the federation access groups, you must remove the corresponding permissions for the assigned administrators on the access groups.

Procedure

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

2 Select **Settings > Administrators**.

3 To delete a permission that applies to a specific federation access group, perform these steps.

a On the **Federation Access Groups** tab, select the federation access group, select the permission, and click **Remove Permissions**.

b Click **Remove**.

4 To delete a permission that applies to a specific administrator or group, perform these steps.

a On the **Administrators and Groups** tab, select the user or group, select the permission, and click **Remove Permissions**.

b Click **Remove**.

5 To delete a permission that applies to a specific role, perform these steps.

a On the **Role Permissions** tab, select the role, select the permission, and click **Remove Permissions**.

b Click **Remove**.

Remove a Federation Access Group

You can remove a federation access group in Horizon Console.

Prerequisites

- If the federation access group contains global entitlements, move the global entitlements to another federation access group or to the root federation access group. See Move a Global Entitlement to a Federation Access Group.
- If the federation access group contains permissions in any of the pods in the pod federation, remove the permissions. See Remove a Permission From a Federation Access Group.

You cannot remove the root federation access group.

Procedure

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

2 Select **Settings > Administrators**.

3 **On the Federation Access Groups** tab, select the federation access group and click **Remove Federation Group**.

4 To remove the federation access group, click **OK**.

Managing a Cloud Pod Architecture Environment in Horizon Console

5

You can use Horizon Console to view, modify, and maintin your Cloud Pod Architecture environment.

For general information about using Horizon Console, see the *Horizon Administration* document. For information about using the `lmvutil` command-line interface, see Chapter 6 Administering Cloud Pod Architecture with lmvutil.

This chapter includes the following topics:

Review a Cloud Pod Architecture Configuration

You can use Horizon Console to review information about global entitlements, pods, sites, and home sites.

Procedure

◆ To list all of the global entitlements in your configuration, select **Inventory > Global Entitlements**.

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

- To list the desktop or application pools in a global entitlement, select **Inventory > Global Entitlements**, 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 Console user interface for a Connection Server instance in the remote pod to see those pools.

- To see the global desktop entitlement that contains a specific desktop pool, select **Inventory > Desktops**.

  The name of the global desktop entitlement that contains the desktop pool appears in the Global Entitlement column for that desktop pool on the Desktop Pools page. You can also click a desktop pool name on the Desktop Pools page and view the name of the global desktop entitlement on the **Summary** tab.

- To list the users or groups associated with a global entitlement, select **Inventory > Global Entitlements**, click the global entitlement name, and click the **Users and Groups** tab.

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

- To quickly identify the pod that you are logged in to in Horizon Console, look for the pod name in the header at the top of the Horizon Console window.

  This feature is particularly useful when you are logged in to multiple pods.

- To list the pods in the pod federation, select **Settings > Cloud Pod Architecture**.

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

- To list the sites in the pod federation, including the pods in a site, select **Settings > Sites**.

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

- To list the home site assignments for users and groups, select **Users and Groups** and click the **Home Site Assignment** tab.

- To list the home sites for a user or group by global entitlement, perform these steps.

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

  b Click **Find User**.

  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**.

  The global entitlement name appears in the Entitlements 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 that are associated with a global entitlement, select **Inventory > Global Entitlements**, click the global entitlement name, and click the **Summary** tab.

  The tags that are associated with the global entitlement appear in the Connection Server restrictions field.

Review Pod Federation Health

HorizonHorizon 8 constantly monitors the health of the pod federation by checking the health of each pod and Connection Server instances in those pods. You can review the health of a pod federation in Horizon Console.

You can also review 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 *Horizon Administration* document.

Important Horizon 8 event databases are not shared across pods in a pod federation.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. In Horizon Console, select **Monitor > Dashboard**.
3. In the **System Health** pane, click **View** and then click **Remote Pods**.

Results

The Remote Pods page 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.

Review Desktop and Application Sessions

You can use Horizon Console to review desktop and application sessions across the pod federation.

Procedure

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

2 To search for sessions, perform the following steps.

  a In Horizon Console, select **Search Sessions**.

  b Select search criteria and begin the search.

  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.

Option	Action
Search by user	1 Select **User** from the drop-down menu and click **Find User**. 2 Select search criteria in the Find User dialog box and click **Find**.
Search by pod	1 Select **Pod** from the drop-down menu. 2 Select a pod from the list of pods and click **Search**.
Search by brokering pod	1 Select **Brokering Pod** from the drop-down menu. 2 Select a pod from the list of pods and click **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. From the search results page, you might be able to disconnect or log off a session, restart a desktop, reset a virtual machine, or send a message to a desktop user.

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

3 To view information about all Cloud Pod Architecture sessions, perform these steps.

  a Select **Monitor > Dashboard**.

  b In the **Cloud Pod Architecture Sessions** pane, select a pod from the drop-down menu.

  The doughnut chart shows the total hosted and brokered sessions for the pod that you selected.

  c To view more session information, click **View**.

  A table shows the total number of brokered and hosted sessions for each pod and the pod status. If the pod status is red, the pod is either down or is not running VMware Horizon 7 version 7.12 or later. Sessions on pods that are running earlier versions of VMware Horizon are not counted.

Managing Sites

You can use Horizon Console to create, modify, and delete Cloud Pod Architecture sites. A site is a grouping of pods.

Add a Pod to a Site

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Settings > Sites**.
3. Select the site that currently contains the pod to add to the site.
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**.

Delete a Site

You can use Horizon Console to delete a site from the pod federation.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Settings > Sites**.
3. Select the site to delete, click **Delete**, and click **OK**.

Change a Site Name or Description

You can use Horizon Console to edit a site name or description.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Settings > Sites**.
3. Select the site to edit, click **Edit**, make your changes, and click **OK**.

Managing Global Entitlements

You can use Horizon Console to add and remove pools, users, and groups from global entitlements. You can also delete global entitlements and modify global entitlement attributes and policies.

Remove a Pool From a Global Entitlement

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod that contains the pool to remove.
2. Select **Inventory > Global Entitlements**.
3. Click the name of the global entitlement.
4. On the **Local Pools** tab, click the row that contains the pool, click **Delete**, and click **OK**.

Add a User or Group to a Global Entitlement

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements** and click the name of the global entitlement.
3. On the **Users and Groups** tab, click **Add Entitlements**.
4. To find Active Directory users or groups, click **Add**, select one or more search criteria, and click **Find**.

   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.
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.

   To restrict access to the global entitlement to specific client computers, select the Active Directory security group that contains the names of the computers that are allowed to access the global entitlement.
6. To save your changes, click **OK**.

Remove a User or Group from a Global Entitlement

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements** and click the name for the global entitlement.
3. On the Users and Groups tab, select the check box for the user or group to delete and click **Remove Entitlements**.
4. Click **OK** in the confirmation dialog box.

Modify Attributes or Policies for a Global Entitlement

You can use Horizon Console to modify global entitlement attributes and policies.

You can modify the global entitlement name, display name, and description, the Connection Server tags associated with the global entitlement, and the category folder for a Windows Start menu shortcut. You can change the scope, home site, redundant session, default display protocol, pre-launch, Session Collaboration, and client restriction policies. You can also add a backup global entitlement.

For a global application entitlement, you can modify the application path, version, and publisher after the first application pool is added. If you add an application pool to a global application entitlement that already contains an application pool, the previous values of application path, version, and publisher are retained.

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

Prerequisites

Use the global entitlement configuration worksheet to record the attributes and policies to modify. See Worksheet for Configuring a Global Entitlement.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**.
3. Select the row for the global entitlement and click **Edit**.
4. Modify the global entitlement attributes and policies.

   Use the configuration information that you gathered in the global entitlement configuration worksheet.
5. To save your changes, click **Submit**.

Delete a Global Entitlement

You can use Horizon Console 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 Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**.
3. Click the row for the global entitlement to delete and click **Delete**.
4. Click **OK** in the confirmation dialog box.

Managing Home Sites

You can use Horizon Console to create, modify, delete, and list home sites.

Modify a Home Site Assignment

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Users and Groups** and click the **Home Site Assignment** tab.
3. Select the row for the user or group and click **Edit**.
4. Select a different home site from the **Home Site** drop-down menu and click **OK**.

Remove a Home Site Assignment

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

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

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Users and Groups** and click the **Home Site Assignment** tab.
3. Select the row for the user or group and click **Delete**.
4. To remove the home site assignment, click **OK**.

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 Console to determine a user's effective home site.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Users and Groups** and click the **Home Site Resolution** tab.
3. Click **Find User**.
4. To find Active Directory users, select one or more search criteria, and click **Find**.
5. Select the Active Directory user whose effective home site you want to display and click **OK**.

Results

Horizon Console 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 Entitlements column. You can expand this folder to list the home site assignments that are not in effect for the global entitlement. Horizon Console uses strikethrough text to indicate a home site is not in effect.

Horizon Console 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 Console 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 Console displays **(Default)**. If the home site originated from the global entitlement (a home site override), Horizon Console displays **(Direct)**.

If a user does not have a home site, Horizon Console 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 site for a specific user or group in Horizon Console.

Procedure

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**.
3. Select the name of the global entitlement and click the **Home Site Override** tab.
4. Select the home site override to modify and click **Edit**.
5. Select a different home site from the **Home Site Override** drop-down menu and click **OK**.

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 Console user interface for any Connection Server instance in the pod federation.
2. Select **Inventory > Global Entitlements**.
3. Select the name of the global entitlement and click the **Home Site Override** tab.
4. Select the home site override and click **Remove**.

5 To remove the home site override, click **OK**.

Remove a Pod From the Pod Federation

You can use Horizon Console 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.

Removing a pod from the pod federation permanently deletes all global entitlements, federation access groups, and federation access group permissions for the pod. Global entitlements, federation access groups, and permissions remain on the other pods in the pod federation.

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.

Prerequisites

To remove the last pod in the pod federation, you must uninitialize the Cloud Pod Architecture feature. See Uninitialize the Cloud Pod Architecture Feature.

Procedure

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

2 Select **Settings > Cloud Pod Architecture**, select the pod to unjoin, and click **Unjoin**.

3 To begin the unjoin operation ,click **OK**.

Horizon Console shows the progress of the unjoin operation.

Uninitialize the Cloud Pod Architecture Feature

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

Uninitializing a pod permanently deletes all global entitlements, federation access groups, and federation access group permissions, and returns the pod to a standalone state. This action cannot be undone.

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 remove the other pods before you begin the uninitialization process. See Remove a Pod From the Pod Federation.

Procedure

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

2 Select **Settings > Cloud Pod Architecture** and click **Uninitialize**.

3 To begin the uninitialization process, click **OK**.

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

Administering Cloud Pod Architecture with lmvutil

6

You can use the `lmvutil` command-line interface to set up 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

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

The **Manage Cloud Pod Architecture** privilege, at a minimum, is required to manage a Cloud Pod Architecture environment. For more information, see Security Considerations for Cloud Pod Architecture.

Table 6-1. 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.

Table 6-2. lmvutil Command Options

Option	Description
`--activatePendingCertificate`	Activates a pending SSL certificate. See Activating a Pending Certificate.
`--addGroupEntitlement`	Associates a user group with a global entitlement. See Adding a User or Group to a Global Entitlement.
`--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.
`--addUserEntitlement`	Associates a user with a global entitlement. See Adding a User or Group to a Global Entitlement
`--assignPodToSite`	Assigns a pod to a site. See Assigning a Pod to a Site.
`--createGlobalApplicationEntitlement`	Creates a global application entitlement. See Creating a Global Entitlement.
`--createGlobalEntitlement`	Creates a global desktop entitlement. See Creating a Global Entitlement.
`--createSite`	Creates a site. See Creating a Site.
`--createGroupHomeSite`	Associates a user group with a home site. See Configuring a Home Site.
`--createPendingCertificate`	Creates a pending SSL certificate. See Creating a Pending Certificate.
`--createUserHomeSite`	Associates a user with a home site. See Configuring a Home Site.
`--deleteGlobalApplicationEntitlement`	Deletes a global application entitlement. See Deleting a Global Entitlement.
`--deleteGlobalEntitlement`	Deletes a global deskop entitlement. See Deleting a Global Entitlement.
`--deleteSite`	Deletes a site. See Deleting a Site.
`--deleteGroupHomeSite`	Removes the association between a user group and a home site. See Deleting a Home Site.
`--deleteUserHomeSite`	Removes the association between a user and a home site. See Deleting a Home Site.
`--editSite`	Modifies the name or description of a site. See Changing a Site Name or Description.
`--ejectPod`	Removes an unavailable pod from a pod federation. See Removing a Pod from a Pod Federation.
`--help`	Lists the `lmvutil` command options.
`--initialize`	Initializes the Cloud Pod Architecture feature. See Initializing the Cloud Pod Architecture Feature.
`--join`	Joins a pod to a pod federation. See Joining a Pod to the Pod Federation.

Table 6-2. lmvutil Command Options (continued)

Option	Description
`--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.
`--listEntitlements`	Lists associations between users or user groups and global entitlements. Listing the Users or Groups in a Global Entitlement.
`--listGlobalApplicationEntitlements`	Lists all global application entitlements. See Listing Global Entitlements.
`--listGlobalEntitlements`	Lists all global desktop entitlements. See Listing Global Entitlements.
`--listPods`	Lists the pods in a Cloud Pod Architecture topology. See Listing the Pods or Sites in a Cloud Pod Architecture Topology.
`--listSites`	Lists the sites in a Cloud Pod Architecture topology. See Listing the Pods or Sites in a Cloud Pod Architecture Topology.
`--listUserAssignments`	Lists the dedicated desktop pod assignments for a user and global entitlement combination. See Listing Dedicated Desktop Pool Assignments.
`--removePoolAssociation`	Removes the association between a desktop pool and a global entitlement. See Removing a Pool from a Global Entitlement.
`--resolveUserHomeSite`	Shows the effective home site for a user. See Listing the Effective Home Site for a User.
`--removeGroupEntitlement`	Removes a user group from a global entitlement. See Removing a User or Group from a Global Entitlement.
`--removeUserEntitlement`	Removes a user from a global entitlement. See Removing a User or Group from a Global Entitlement.
`--showGroupHomeSites`	Shows all of the home sites for a group. See Listing the Home Sites for a User or Group.
`--showUserHomeSites`	Shows all of the home sites for a user. See Listing the Home Sites for a User or Group.
`--uninitialize`	Disables the Cloud Pod Architecture feature. See Disabling the Cloud Pod Architecture Feature.
`--unjoin`	Removes an available pod from a pod federation. See Removing a Pod from a Pod Federation.
`--updateGlobalApplicationEntitlement`	Modifes a global application entitlement. See Modifying a Global Entitlement.
`--updateGlobalEntitlement`	Modifies a global desktop entitlement. See Modifying a Global Entitlement.

Table 6-2. lmvutil Command Options (continued)

Option	Description
`--updatePod`	Modifies the name or description of a pod. See Changing a Pod Name or Description.
`--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, VMware Horizon 8 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 a Pod Federation

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

- Joining a Pod to the Pod Federation

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

- 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.

- 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.

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 6-3. 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 6-4. 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

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

- Assigning a Pod to a Site

  Use the `lmvutil` command with the `--assignPodToSite` option to assign a pod to a site.
- Changing a Site Name or Description

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

  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 6-5. 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.

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 6-6. 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.

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 6-7. 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

  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

  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

  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

  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

  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

  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

  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 [--aliasName name | --
disableAliasName]
--scope scope {--isDedicated | --isFloating} [--description text] [--disabled]
[--fromHome] [--multipleSessionAutoClean] [--requireHomeSite] [--defaultProtocol value]
[--preventProtocolOverride] [--allowReset] [--multipleSessionsPerUser] [--tags tags]
[--categoryFolder foldername] [--clientRestrictions] [--collaboration]
```

```
[--shortcutLocations {desktop | launcher | desktop,launcher}] [--displayAssignedHostName] [--
displayMachineAlias]
[--federationAccessGroup name]
```

```
lmvutil --createGlobalApplicationEntitlement --entitlementName name [--aliasName name | --
disableAliasName]
--scope scope [--description text] [--disabled] [--fromHome] [--multipleSessionAutoClean]
[--requireHomeSite] [--defaultProtocol value] [--preventProtocolOverride] [--preLaunch] [--
tags tags]
[--categoryFolder foldername] [--clientRestrictions] [--shortcutLocations {desktop | launcher
| desktop,launcher}]
[--multiSessionMode value] [--federationAccessGroup name]
```

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 6-8. Options for Creating Global Entitlements

Option	Description
`--entitlementName`	Unique name that identifies the global entitlement in Horizon Console. The name can contain between 1 and 64 characters.
`--aliasName`	(Optional) Display name of the global entitlement. The display name appears to users in the list of available desktops and applications in Horizon Client. The display name does not need to be unique. Multiple global entitlements can have the same display name. If you do not specify a display name, the unique name appears to users in Horizon Client. The display name can contain between 1 and 64 characters.
`--disableAliasName`	(Optional) Sets the display name of the global entitlement (`--aliasName` option) to the default value. The unique name of the global entitlement (`--entitlementName` option) appears to users in Horizon Client by default. You can specify either `--aliasName` or `--disableAliasName`, but not both.
`--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.

Table 6-8. Options for Creating Global Entitlements (continued)

Option	Description
`--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.
`--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) Specifies the 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.

Table 6-8. Options for Creating Global Entitlements (continued)

Option	Description
`--multipleSessionsPerUser`	(Optional) Enables the multiple sessions per user policy, which allows users to initiate separate desktop sessions from different client devices. Users that connect to the global desktop 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. Applies only to floating desktop entitlements.
`--preLaunch`	(Optional) Enables the pre-launch policy, which launches the application session before a user opens the global application entitlement in Horizon Client. When you enable the pre-launch policy, users can launch the global application entitlement more quickly. All the application pools in the global application entitlement must support the session pre-launch feature, and the pre-launch session timeout must be the same for all farms.
`--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. For more information, see Implementing Connection Server Restrictions for Global Entitlements.
`--categoryFolder`	(Optional) Specifies the name of the category folder that contains a shortcut for the global entitlement on client devices. You can configure up to four folder levels. A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords. You must also specify the `--shortcutLocations` option to indicate the location of the shortcut on a Windows client device. For more information, see Configuring Shortcuts for Global Entitlements.
`--clientRestrictions`	(Optional) Enables the client restrictions policy, which restricts access to the global entitlement to specific client computers. For more information, see Implementing Client Restrictions for Global Entitlements.
`--collaboration`	(Optional) Enables the Session Collaboration policy, which allows users of remote desktop sessions to invite other users to join their sessions. All the desktop pools in the global desktop entitlement must support the Session Collaboration feature. Applies only to global desktop entitlements.
`--shortcutLocations`	(Optional) Use this option with the `--categoryFolder` option to specify the location of the shortcut on the client device. Valid values are `desktop`, which creates the shortcut on the Windows desktop, and `launcher`, which creates the shortcut in the Windows Start menu. You can also specify both `desktop` and `launcher`, separated by a comma, to create both Windows desktop and Windows Start menu shortcuts.

Table 6-8. Options for Creating Global Entitlements (continued)

Option	Description
`--multiSessionMode`	(Optional) Configures the multi-session mode feature for the global application entitlement. Specify one of the following values: `DISABLED`, `ENABLED_DEFAULT_OFF`, `ENABLED_DEFAULT_ON`, or `ENABLED_ENFORCED`. For more information, see Enabling Multi-Session Mode for Global Application Entitlements.
`--displayAssignedHostName`	(Optional) In Horizon Client, displays the host name of the machine assigned to the user instead of the global entitlement name. Applies only to dedicated desktop entitlements.
`--displayMachineAlias`	(Optional) In Horizon Client, displays the alias name of the machine assigned to the user instead of the global entitlement name. Applies only to dedicated desktop entitlements.
`--federationAccessGroup`	(Optional) Specifies the federation access group that is used to organize global entitlements for delegated administration. For more information, see Chapter 4 Setting Up Federation Access Groups in Horizon Console.

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 [--aliasName name | --
disableAliasName]
[--description text] [--disabled] [--enabled] [--fromHome] [--disableFromHome]
[--multipleSessionAutoClean] [--disableMultipleSessionAutoClean] [--multipleSessionsPerUser]
[--disableMultipleSessionsPerUser] [--requireHomeSite] [--disableRequireHomeSite]
[--defaultProtocol value] [--scope scope] [--tags tags] [--notags] [--categoryFolder
foldername]
[--disableCategoryFolder] [--clientRestrictions] [--disableClientRestrictions] [--
collaboration]
[--disableCollaboration] [--shortcutLocations {desktop | launcher | desktop,launcher}]
[--backupEntitlementName name] [--disableBackupEntitlement] [--displayAssignedHostName ] [--
disableDisplayAssignedHostName]
[--displayMachineAlias] [--disableDisplayMachineAlias] [--federationAccessGroup name]
```

```
lmvutil --updateGlobalApplicationEntitlement --entitlementName name [--aliasName name | --
disableAliasName]
[--description text] [--disabled] [--enabled] [--fromHome] [--disableFromHome] [--
multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--requireHomeSite] [--disableRequireHomeSite] [--
defaultProtocol value] [--scope scope]
[--appVersion value] [--appPublisher value] [--appPath value] [--tags tags] [--notags] [--
preLaunch] [--disablePreLaunch]
[--categoryFolder foldername] [--disableCategoryFolder] [--clientRestrictions] [--
disableClientRestrictions]
[--shortcutLocations {desktop | launcher | desktop,launcher}] [--multiSessionMode value] [--
backupEntitlementName name]
[--disableBackupEntitlement] [--federationAccessGroup name]
```

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 6-9. Options for Modifying Global Entitlements

Option	Description
`--entitlementName`	Unique name of the global entitlement to modify.
`--aliasName`	(Optional) Display name of the global entitlement. The display name appears to users in the list of available desktops and applications in Horizon Client. The display name does not need to be unique. Multiple global entitlements can have the same display name. If you do not specify a display name, the unique name appears to users in Horizon Client. The display name can contain between 1 and 64 characters.
`--disableAliasName`	(Optional) Sets the display name of the global entitlement (`--aliasName` option) to the default value. The unique name of the global entitlement (`--entitlementName` option) appears to users in Horizon Client by default. You can specify either `--aliasName` or `--disableAliasName`, but not both.

Table 6-9. Options for Modifying Global Entitlements (continued)

Option	Description
`--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` function for the global entitlement.
`--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` function for the global entitlement.
`--multipleSessionsPerUser`	(Optional) Enables the multiple sessions per user policy, which allows users to initiate separate desktop sessions from different client devices. Users that connect to the global desktop 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. Applies only to floating desktop entitlements.
`--disableMultipleSessionsPerUser`	(Optional) Disables the multiple sessions per user policy for the global desktop 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` function for the global entitlement.

Table 6-9. Options for Modifying Global Entitlements (continued)

Option	Description
`--defaultProtocol`	(Optional) Specifies the 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.
`--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.
`--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. For more information, see Implementing Connection Server Restrictions for Global Entitlements.
`--notags`	(Optional) Removes tags from the global entitlement.
`--preLaunch`	(Optional) Enables the pre-launch policy, which launches the application session before a user opens the global application entitlement in Horizon Client. When you enable the pre-launch policy, users can launch the global application entitlement more quickly. All the application pools in the global application entitlement must support the session pre-launch feature, and the pre-launch session timeout must be the same for all farms.
`--disablePreLaunch`	(Optional) Disables the pre-launch policy for the global application entitlement.
`--categoryFolder`	(Optional) Specifies the name of the category folder that contains a shortcut for the global entitlement on client devices. You can configure up to four folder levels. A folder name can be up to 64 characters long. To specify a subfolder, enter a backslash (\) character, for example, `dir1\dir2\dir3\dir4`. You can enter up to four folder levels. You cannot begin or end a folder name with a backslash, and you cannot combine two or more backslashes. For example, `\dir1`, `dir1\dir2\`, `dir1\\dir2`, and `dir1\\\dir2` are invalid. You cannot enter Windows reserved keywords. You must also specify the `--shortcutLocations` option to indicate the location of the shortcut on a Windows client device. For more information, see Configuring Shortcuts for Global Entitlements.
`--disableCategoryFolder`	(Optional) Removes the category folder for the global entitlement.
`--clientRestrictions`	(Optional) Enables the client restrictions policy, which restricts access to the global entitlement to specific client computers. For more information, see Implementing Client Restrictions for Global Entitlements.

Table 6-9. Options for Modifying Global Entitlements (continued)

Option	Description
`--disableClientRestrictions`	(Optional) Disables the client restrictions policy for the global entitlement.
`--collaboration`	(Optional) Enables the Session Collaboration policy, which allows users of remote desktop sessions to invite other users to join their sessions. All the desktop pools in the global desktop entitlement must support the Session Collaboration feature. Applies only to global desktop entitlements.
`--disableCollaboration`	(Optional) Disables the Session Collaboration policy for the global desktop entitlement.
`--shortcutLocations`	(Optional) Use this option to modify or create a shortcut on the client device. Valid values are `desktop`, which creates the shortcut on the desktop, and `launcher`, which creates the shortcut in the Windows Start menu. You can also specify both `desktop` and `launcher`, separated by a comma, to create both desktop and Windows Start menu shortcuts. If you are modifying a shortcut (that is, the category folder has already been created), you do not need to specify the `--categoryFolder` option, unless you also want to change the category folder name. If the category folder has not yet been created, you must specify the `--categoryFolder` option together with the `--shortcutLocations` option. **Note** Do not use this option with the `--disableCategoryFolder` option.
`--multiSessionMode`	(Optional) Configures the multi-session mode feature for the global application entitlement. Specify one of the following values: `DISABLED`, `ENABLED_DEFAULT_OFF`, `ENABLED_DEFAULT_ON`, or `ENABLED_ENFORCED`. For more information, see Enabling Multi-Session Mode for Global Application Entitlements.
`--backupEntitlementName`	(Optional) Specifies the name of a backup global entitlement. A backup global entitlement delivers remote desktops or published applications when the primary global entitlement cannot start a session. For global desktop entitlements, the user assignment type must be Floating. For more information, see Implementing Backup Global Entitlements.
`--disableBackupEntitlement`	(Optional) Disables the backup global entitlement.
`--displayAssignedHostName`	(Optional) In Horizon Client, displays the host name of the assigned machine instead of the global entitlement name. Applies only to dedicated desktop entitlements.
`--disableDisplayAssignedHostName`	(Optional) Specifies that the assigned machine host name does not appear in Horizon Client. Applies only to dedicated desktop entitlements.
`--displayMachineAlias`	(Optional) In Horizon Client, displays the alias name of the machine assigned to the user instead of the global entitlement name Applies only to dedicated desktop entitlements.

Table 6-9. Options for Modifying Global Entitlements (continued)

Option	Description
`--disableDisplayMachineAlias`	(Optional) Specifies that the alias name of the machine does not appear in Horizon Client. Applies only to dedicated desktop entitlements.
`--federationAccessGroup`	(Optional) Specifies a federation access group that is used to organize global entitlements for delegated administration. For more information, see Chapter 4 Setting Up Federation Access Groups in Horizon Console.

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 6-10. 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 6-11. 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 6-12. 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 6-13. 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

  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

  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.

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 6-14. 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 6-15. 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

  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

  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

  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

  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

  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

  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

  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 6-16. 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 6-17. 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 6-18. 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 6-19. 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

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

- Activating a Pending Certificate

  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
```