Administering View Cloud Pod Architecture

VMware Horizon 6 6.1

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Contents

Administering View Cloud Pod Architecture

Administering View Cloud Pod Architecture describes how to configure and administer a Cloud Pod Architecture environment in VMware Horizon® 6, including how to plan a Cloud Pod Architecture topology and set up, monitor, and maintain a Cloud Pod Architecture configuration.

Intended Audience

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

VMware Technical Publications Glossary

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

Introduction to Cloud Pod Architecture

<div style="text-align: right; font-size: 3em;">1</div>

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

This chapter includes the following topics:

■ "Understanding Cloud Pod Architecture," on page 7

■ "Configuring and Managing a Cloud Pod Architecture Environment," on page 8

■ "Cloud Pod Architecture Limitations," on page 8

Understanding Cloud Pod Architecture

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

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

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

Figure 1-1. Basic Cloud Pod Architecture Topology
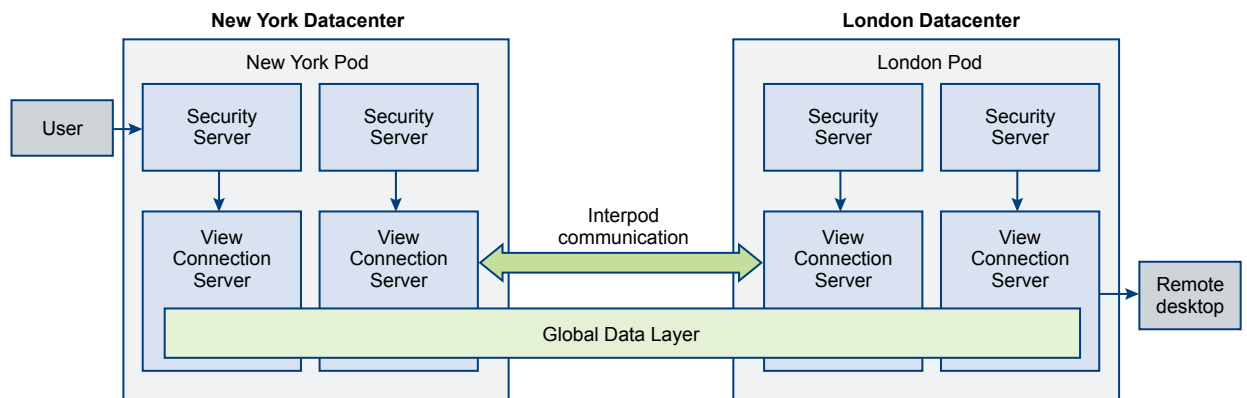
In the example topology, two previously standalone View pods in different datacenters are joined together to form a single pod federation. An end user in this environment can connect to a View Connection Server instance in the New York datacenter and receive a session on a desktop in the London data center.

Sharing Key Data in the Global Data Layer

View 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 View 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.

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

Sending Messages Between Pods

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

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

Configuring and Managing a Cloud Pod Architecture Environment

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

NOTE You cannot use View Administrator to create and manage Cloud Pod Architecture home sites. You must use the `lmvutil` command to perform these tasks.

Cloud Pod Architecture Limitations

The Cloud Pod Architecture feature has certain limitations.

- It does not support using the HTML Access feature. With HTML Access, end users can use a Web browser to connect to remote desktops and are not required to install any client software on their local systems.

- It does not support using remote Windows-based applications hosted on a Microsoft RDS host.

- It is not supported in an IPv6 environment.

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 View implementation. If you are joining existing View 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," on page 9
- "Entitling Users and Groups in the Pod Federation," on page 10
- "Finding and Allocating Desktops in the Pod Federation," on page 10
- "Global Entitlement Example," on page 12
- "Cloud Pod Architecture Topology Limits," on page 12
- "Cloud Pod Architecture Port Requirements," on page 13
- "Security Considerations for Cloud Pod Architecture Topologies," on page 13

Creating Cloud Pod Architecture Sites

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

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

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

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

See "Create and Configure a Site," on page 19.

Entitling Users and Groups in the Pod Federation

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

In a Cloud Pod Architecture environment, you create global entitlements to entitle users or groups to multiple desktops 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.

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

NOTE   As a best practice, you should not configure local and global entitlements for the same desktop pool. If you use both types of entitlements for the same desktop pool, the same desktop might appear as a local and a global entitlement in the list of desktops that Horizon Client shows to an end user.

Each global 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.

A global entitlement's scope policy specifies where View looks for desktops when it allocates desktops to users in the global entitlement. It also determines whether View looks for desktops 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.

Finding and Allocating Desktops in the Pod Federation

View 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 across the pod federation.

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

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

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

Configuring Scope Policy to Control Desktop Search

When you create a global entitlement, you must specify its scope policy. The scope policy determines the scope of the search when the Cloud Pod Architecture feature looks for desktops to satisfy a desktop request from the global entitlement.

You can set the scope policy so that the Cloud Pod Architecture feature searches for desktops 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 entitlements that contain dedicated desktop pools, the scope policy affects where the Cloud Pod Architecture feature looks for desktops only the first time a user requests a dedicated desktop. After the Cloud Pod Architecture feature allocates a dedicated desktop, it returns the user directly to the same desktop.

For information about configuring the scope policy for a global entitlement, see "Create and Configure a Global Entitlement," on page 17.

Configuring Home Sites to Control Desktop Placement

A home site is a relationship between a user or group and a Cloud Pod Architecture site. With home sites, you can ensure that a user always receives desktops from a specific site rather than receiving desktops based on the user's current location. The Cloud Pod Architecture feature includes the following types of home site assignments.

Global home site	You can assign home sites to users and groups. 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. For example, if a user has a home site in New York but is visiting London, the Cloud Pod Architecture feature looks 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	When you use the `lmvutil` command to create a home site for a user or group, you can use the `--entitlementName` option to specify a global entitlement. Per-global-entitlement home sites override global home site assignments.
	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, the Cloud Pod Architecture feature looks in the London site to satisfy the user's desktop request rather than allocating a desktop from the New York site.

When you use the `lmvutil` command with the `--createGroupHomeSite` option to create a per-global-entitlement home site, you must explicitly entitle all Active Directory user groups that contain the home site users. If you have nested user groups, it is not sufficient to entitle only the parent group. In this case, the parent group is explicitly entitled to the global entitlement, but the subgroups are not, and the `--createGroupHomeSite` option fails.

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

For information about creating home sites, see "Assign a Home Site to a User or Group," on page 20. For information about creating global entitlements, see "Create and Configure a Global Entitlement," on page 17.

Global Entitlement Example

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

Figure 2-1. Global Entitlement Example
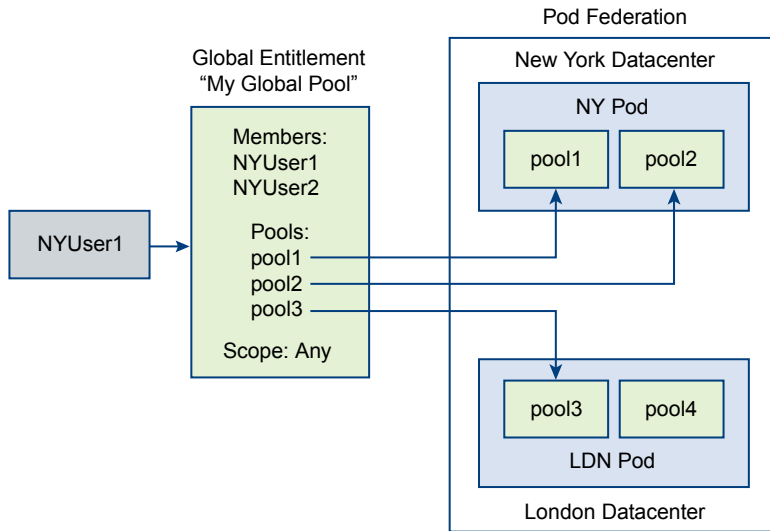
Because My Global Pool has a scope policy of ANY, the Cloud Pod Architecture feature looks for desktops across both NY Pod and LDN Pod when NYUser1 requests a desktop. The Cloud Pod Architecture feature does not try to allocate a desktop from pool4 because pool4 is not part of My Global Pool.

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

For information about creating global entitlements, see "Create and Configure a Global Entitlement," on page 17.

Cloud Pod Architecture Topology Limits

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

Table 2-1. Pod Federation Limits

Component	Limit
Desktops	20,000
Pods	4
Sites	2
View Connection Server instances	20

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 View 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 2-2. Ports Opened During View Connection Server Installation

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

Security Considerations for Cloud Pod Architecture Topologies

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

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

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

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

Setting Up a Cloud Pod Architecture Environment

3

Setting up a Cloud Pod Architecture environment involves initializing the Cloud Pod Architecture feature, joining pods to the pod federation, and creating global entitlements. You can optionally create sites and assign home sites.

This chapter includes the following topics:

Initialize the Cloud Pod Architecture Feature

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

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

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

This procedure shows how to use View Administrator to initialize the Cloud Pod Architecture feature. To use the `lmvutil` command to initialize the Cloud Pod Architecture feature, see "Initializing the Cloud Pod Architecture Feature," on page 40.

Procedure

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

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

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

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

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

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

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

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

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

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

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

What to do next

To add more pods to the pod federation, see "Join a Pod to the Pod Federation," on page 16.

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 View Administrator to join additional pods to the pod federation. Joining additional pods is optional.

You can also use the `lmvutil` command to join a pod to the pod federation. See "Joining a Pod to the Pod Federation," on page 41.

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

Prerequisites

■   Make sure the View Connection Server instances that you want to join have different host names. You cannot join servers that have the same name, even if they are in different domains.

■   Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 15.

Procedure

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

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

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

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

       Use the format *domain\username*.

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

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

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

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

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

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

After the pod is joined to the pod federation, it begins to share health data. You can view this health data on the dashboard in View Administrator. See "View Pod Federation Health in View Administrator," on page 29.

NOTE   A short delay might occur before health data is available in View Administrator.

What to do next

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

Create and Configure a Global Entitlement

You use global entitlements to entitle users and groups to desktops in a Cloud Pod Architecture environment. A global entitlement provides the link between users and their desktops, regardless of where those desktops reside in the pod federation. You must create and configure at least one global entitlement to use the Cloud Pod Architecture feature.

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

Prerequisites

■   Decide which type of global entitlement to create, the users, groups, and pools to include in the global entitlement, and the scope of the global entitlement. See "Entitling Users and Groups in the Pod Federation," on page 10.

■   Decide whether the global entitlement should use home sites. See "Configuring Home Sites to Control Desktop Placement," on page 11.

■   Create the desktop pools to include in the global entitlement. For information about creating desktop pools in View, see the *Setting Up Desktop and Application Pools in View* document.

■   Create the users and groups to include in the global entitlement.

■   Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 15.

Procedure

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

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

3 Define the global entitlement.

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

  The name can contain between 1 and 64 characters. The global entitlement name appears in the list of available entitlements for the user in Horizon Client.

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

  The description can contain between 1 and 1024 characters. The global entitlement name appears in the list of available entitlements for the user in Horizon Client.

 c Select a user assignment policy for the global entitlement.

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

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

 d Select a scope policy for the global entitlement.

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

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

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

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

 f (Optional) If you are creating a floating entitlement, use the **Automatically clean up redundant sessions** option to specify whether to automatically clean up redundant sessions.

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

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

 h Select whether to allow users to reset desktops in the global entitlement.

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

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

    b   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.

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

    The global entitlement appears on the Global Entitlements page.

6   Select the desktop pools that can provide desktops for the users in the global entitlement you created.

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

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

    c   Double-click the global entitlement.

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

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

        NOTE Desktop 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.

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

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

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.

You can also use the lmvutil command to create and configure a site. See "Managing Sites," on page 43.

Prerequisites

■   Decide whether your Cloud Pod Architecture topology should include sites. See "Creating Cloud Pod Architecture Sites," on page 9.

■   Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 15.

Procedure

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

2   Create the site.

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

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

        The site name can contain between 1 and 64 characters.

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

        The site name can contain between 1 and 1024 characters.

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

3   Add a pod to the site.

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

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

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

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

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

Assign a Home Site to a User or Group

A home site is the relationship between a user or group and a Cloud Pod Architecture site. Home sites ensure that users always receive desktops from a particular datacenter, even when they are traveling. Creating home sites is optional.

Prerequisites

■   Decide whether to assign home sites to users or groups in your Cloud Pod Architecture environment. See "Configuring Home Sites to Control Desktop Placement," on page 11.

■   Group the pods in your pod federation into sites. See "Create and Configure a Site," on page 19.

■   Global entitlements do not use home sites by default. When creating a global entitlement, you must select the **Use home site** option to cause View to use a user's home site when allocating desktops from that global entitlement. See "Create and Configure a Global Entitlement," on page 17.

■   Initialize the Cloud Pod Architecture feature. See "Initialize the Cloud Pod Architecture Feature," on page 15.

■   Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See "lmvutil Command Authentication," on page 38.

Procedure

■ To create a home site for a user, run the `lmvutil` command with the `−−createUserHomeSite` option.

You can run the command on any View Connection Server instance in the pod federation.

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

Option	Description
--userName	Name of the user. Use the format *domain\username*.
--siteName	Name of the site to associate with the user as the home site.
--entitlementName	(Optional) Name of a global 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 home site.

For example:

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

■ To create a home site for a group, run the `lmvutil` command with the `−−createGroupHomeSite` option.

You can run the command on any View Connection Server instance in the pod federation.

`lmvutil −−createGroupHomeSite −−userName` *domain\username* `−−siteName` *name* `[−−entitlementName` *name*`]`

Option	Description
--groupName	Name of the group. Use the format *domain\groupname*.
--siteName	Name of the site to associate with the group as the home site.
--entitlementName	(Optional) Name of a global 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 group home site.

For example:

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

Test a Cloud Pod Architecture Configuration

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

Prerequisites

■ Install the latest version of Horizon Client on a supported computer or mobile device.

■ Verify that you have credentials for a user in one of your newly created global entitlements.

Procedure

1 Start Horizon Client.

2 Connect to any View 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 View Connection Server instance, the global entitlement name appears in the list of available desktop pools.

3   Select the global entitlement and connect to a desktop.

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

What to do next

If the global entitlement does not appear when you connect to the View Connection Server instance, use View Administrator to verify that the entitlement is configured correctly. If the global entitlement appears but the desktop does not start, all desktop 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 View floating desktops. Access to customer data is kept secure in the health insurance company's datacenters.

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

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

1   Designing the Example Topology on page 23

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

2   Initializing the Example Configuration on page 23

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

3   Joining Pods in the Example Configuration on page 24

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

4   Creating Sites in the Example Configuration on page 24

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

5   Creating Global Entitlements in the Example Configuration on page 24

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

6

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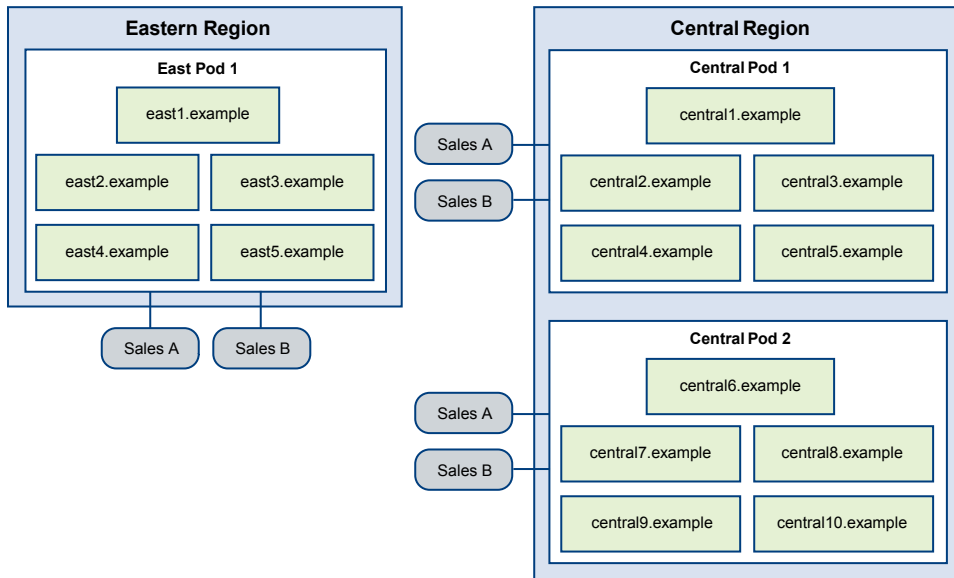
In this topology, the Eastern region site contains a single pod, East Pod 1, that consists of five View Connection Server instances called east1.example through east5.example.

The Central region site contains two pods, Central Pod 1 and Central Pod 2. Each pod contains five View Connection Server instances. The View Connection Servers in the first pod are called central1.example through central5.example. The View 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 View administrator logs in to the View Administrator user interface for a View Connection Server instance in East Pod 1, selects **View Configuration > Cloud Pod Architecture**, and clicks **Initialize the Cloud Pod Architecture feature**.

Because the View administrator uses the View Administrator user interface for a View 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 View administrator uses View Administrator to join Central Pod 1 and Central Pod 2 to the pod federation.

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

    Central Pod 1 is now joined to the pod federation.

2   To join Central Pod 2, the View administrator logs in to the View Administrator user interface for a View Connection Server instance in Central Pod 2, selects **View Configuration > Cloud Pod Architecture**, clicks **Join the pod federation**, and provides the host name or IP address of a View 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 View Connection Server instances across both pods in the Central region are part of the pod federation.

Creating Sites in the Example Configuration

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

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

2   To create a site for the Eastern datacenter, the View administrator selects **View Configuration > Sites** and clicks **Add**.

3   To create a site for the Central datacenter, the View administrator selects **View Configuration > Sites** and clicks **Add**.

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

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

6   To move Central Pod 2 to the site for the Central datacenter, the View administrator selects **View Configuration > Sites**, selects the site that currently contains Central Pod 2, selects Central Pod 2, clicks **Edit**, and selects the Central datacenter site from the **Site** drop-down menu.

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

Creating Global Entitlements in the Example Configuration

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

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

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

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

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

Creating a View URL for the Example Configuration

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

Managing a Cloud Pod Architecture Environment

4

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

This chapter includes the following topics:

View a Cloud Pod Architecture Configuration

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

This procedure shows how to use View Administrator to view information about global entitlements, pods, and sites. To use the `lmvutil` command to view this information, see Chapter 5, "lmvutil Command Reference," on page 37.

Prerequisites

Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See "lmvutil Command Authentication," on page 38.

Procedure

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

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

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

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

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

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

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

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

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

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

■ To list the home sites for a user, run the lmvutil command with the ‑‑showUserHomeSites option.

lmvutil ‑‑showUserHomeSites ‑‑userName *domain\username* [‑‑entitlementName *name*]

Option	Description
‑‑userName	Name of the user for whom to list home sites. Use the format *domain\username*.
‑‑entitlementName	(Optional) Name of a global entitlement. Use this option to list the home sites for a user and global entitlement combination.

For example:

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

■ To list the home sites for a group, run the lmvutil command with the ‑‑showGroupHomeSites option.

lmvutil ‑‑showGroupHomeSites ‑‑groupName *domain\groupname* [‑‑entitlementName *name*]

Option	Description
‑‑groupName	Name of the group for which to list home sites. Use the format *domain\groupname*.
‑‑entitlementName	(Optional) Name of a global entitlement. Use this option to list the home sites for a group and global entitlement combination.

For example:

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

View Pod Federation Health in View Administrator

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

You can also view the health of a pod federation from the command line by using the vdmadmin command with the –H option. For information about vdmadmin syntax, see the *Setting Up Desktop and Application Pools in View* document.

IMPORTANT View event databases are not shared across pods in a pod federation.

Procedure

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

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

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

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

View Desktop Sessions in the Pod Federation

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

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

Procedure

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

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

3   Select search criteria and begin the search.

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

The search results include the names of the user, machine, pool, pod, brokering pod ID, site, and global entitlements associated with each session. The session start time, duration, and state also appear in the search results.

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

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. Home sites associated with global entitlements can override home sites associated with users and groups. For these reasons, it can be difficult to determine the effective home site for a particular user. You can use the `lmvutil` command to list a user's effective home site.

Prerequisites

Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See

Procedure

◆ On any View Connection Server instance in the pod federation, run the `lmvutil` command with the `--resolveUserHomeSite` option.

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

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*.

For example:

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

Add a Pod to a Site

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

You can also use the `lmvutil` command to add a pod to an existing site. See

Procedure

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

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

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

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

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

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

Modifying Global Entitlements

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

Add a Desktop Pool to a Global Entitlement

You can use View Administrator to add a desktop pool to an existing global entitlement. You can add a particular desktop pool to only one global entitlement.

You can also use the `lmvutil` command to add a desktop pool to a global entitlement. See "Adding a Desktop Pool to a Global Entitlement," on page 49.

Prerequisites

Create the desktop pool to add to the global entitlement. See the *Setting Up Desktop and Application Pools in View* document.

Procedure

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

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

3   Double-click the global entitlement.

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

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

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

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

Remove a Desktop Pool From a Global Entitlement

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

You can also use the `lmvutil` command to remove a desktop pool from a global entitlement. See "Removing a Desktop Pool From a Global Entitlement," on page 50.

Procedure

1   Log in to the View Administrator user interface for any View Connection Server instance in the pod that contains the desktop pool to remove.

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

3   On the **Local Pools** tab, select the desktop pool to remove from the global entitlement and click **Delete**.

Add a User or Group to a Global Entitlement

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

You can also use the `lmvutil` command to add a user or group to a global entitlement. See "Adding a User or Group to a Global Entitlement," on page 51.

Prerequisites

Create the user or group to add to the global entitlement.

Procedure

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

2   In View Administrator, select **Catalog > Global Entitlements** and double-click the global entitlement.

3   On the **Users and Groups** tab, click **Add**.

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

5   Select the Active Directory user or group to add to the global entitlement and click **OK**.

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

Remove a User or Group From a Global Entitlement

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

You can also use the `lmvutil` command to remove a user or group from a global entitlement. See "Removing a User or Group From a Global Entitlement," on page 51.

Procedure

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

2   In View Administrator, select **Catalog > Global Entitlements** and double-click the global entitlement.

3   On the Users and Groups tab, select the user or group to delete and click **Delete**.

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

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

Modify Attributes or Policies for a Global Entitlement

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

You can also use the `lmvutil` command to modify global entitlement attributes and polices. See "Modifying a Global Entitlement," on page 48.

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

Procedure

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

2   In View Administrator, select **Catalog > Global Entitlements**

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

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

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

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

Policy	Description
Scope	Specifies where to look for desktops that satisfy a desktop request from the global entitlement. You can select only one scope policy. ■ **All sites** - View looks for desktops on any pod in the pod federation. ■ **Within site** - View looks for desktops only on pods in the same site as the pod to which the user is connected. ■ **Within pod** - View looks for desktops only in the pod to which the user is connected.
Use home site	Causes View to look for desktops in the user's home site. If the user does not have a home site and the **Entitled user must have home site** option is not selected, the site to which the user is currently connected is assumed to be the home site.
Entitled user must have home site	Causes the global entitlement to be available only if the user has a home site. This option is available only when the **Use home site** option is selected.
Automatically clean up redundant sessions	Logs off extra user sessions for the same entitlement.. This option is available only for floating entitlements. Multiple floating desktop 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 in the global entitlement.

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

Delete a Global Entitlement

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

You can also use the `lmvutil` command to delete a global entitlement. See "Deleting a Global Entitlement,"

Procedure

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

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

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

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

Remove a Home Site Association

You can use the `lmvutil` command to remove the association between a user or group and a home site. You can also remove the association between a home site and a global entitlement for a specified user or group.

Prerequisites

Become familiar with the `lmvutil` command authentication options and requirements and verify that you have sufficient privileges to run the `lmvutil` command. See "lmvutil Command Authentication," on page 38.

Procedure

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

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

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

Option	Description
--userName	Name of the user. Use the format *domain\username*.
--entitlementName	(Optional) Name of a global entitlement. Use this option to remove the association between the home site and a global entitlement for the specified user.

  For example:

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

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

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

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

Option	Description
--groupName	Name of the group. Use the format *domain\groupname*.
--entitlementName	(Optional) Name of a global entitlement. Use this option to remove the association between the home site and a global entitlement for the specified group.

  For example:

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

Remove a Pod From the Pod Federation

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

To remove the last pod in the pod federation, you unitialize the Cloud Pod Architecture feature. See "Uninitialize the Cloud Pod Architecture Feature," on page 35.

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

You can also use the `lmvutil` command to remove a pod from the pod federation. See "Removing a Pod From a Pod Federation," on page 42.

Procedure

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

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

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

    View Administrator shows the progress of the unjoin operation.

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

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

Uninitialize the Cloud Pod Architecture Feature

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

You can also use the `lmvutil` command to uninitialize the Cloud Pod Architecture feature. See "Disabling the Cloud Pod Architecture Feature," on page 41.

Prerequisites

You need to uninitialize the Cloud Pod Architecture feature on only one pod in the pod federation. If the pod federation contains multiple pods, you must unjoin the other pods before you begin the uninitialization process. See "Remove a Pod From the Pod Federation," on page 34.

Procedure

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

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

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

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

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

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

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

lmvutil Command Reference 5

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

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

This chapter includes the following topics:

lmvutil Command Use

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

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

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

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

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

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

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

lmvutil Command Authentication

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

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

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

Table 5-1. lmvutil Command Authentication Options

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

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

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

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

lmvutil Command Output

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

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

The `lmvutil` command produces only US English output.

lmvutil Command Options

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

For `lmvutil` command authentication options, see "lmvutil Command Authentication," on page 38.

Table 5-2. lmvutil Command Options

Option	Description
−−activatePendingCertificate	Activates a pending SSL certificate. See "Activating a Pending Certificate," on page 59.
−−addGroupEntitlement	Associates a user group with a global entitlement. See "Adding a User or Group to a Global Entitlement," on page 51.

Table 5-2. lmvutil Command Options (Continued)

Option	Description
--addPoolAssociation	Associates a desktop pool with a global entitlement. See "Adding a Desktop Pool to a Global Entitlement," on page 49.
--addUserEntitlement	Associates a user with a global entitlement. See "Adding a User or Group to a Global Entitlement," on page 51
--assignPodToSite	Assigns a pod to a site. See "Assigning a Pod to a Site," on page 44.
--createGlobalEntitlement	Creates a global entitlement. See "Creating a Global Entitlement," on page 46.
--createSite	Creates a site. See "Creating a Site," on page 44.
--createGroupHomeSite	Associates a user group with a home site. See "Configuring a Home Site," on page 52.
--createPendingCertificate	Creates a pending SSL certificate. See "Creating a Pending Certificate," on page 58.
--createUserHomeSite	Associates a user with a home site. See "Configuring a Home Site," on page 52.
--deleteGlobalEntitlement	Deletes a global entitlement. See "Deleting a Global Entitlement," on page 49.
--deleteSite	Deletes a site. See "Deleting a Site," on page 45.
--deleteGroupHomeSite	Removes the association between a user group and a home site. See "Deleting a Home Site," on page 53.
--deleteUserHomeSite	Removes the association between a user and a home site. See "Deleting a Home Site," on page 53.
--editSite	Modifies the name or description of a site. See "Changing a Site Name or Description," on page 45.
--ejectPod	Removes an unavailable pod from a pod federation. See "Removing a Pod From a Pod Federation," on page 42.
--help	Lists the lmvutil command options.
--initialize	Initializes the Cloud Pod Architecture feature. See "Initializing the Cloud Pod Architecture Feature," on page 40.
--join	Joins a pod to a pod federation. See "Joining a Pod to the Pod Federation," on page 41.
--listAssociatedPools	Lists the desktop pools that are associated with a global entitlement. See "Listing the Desktop Pools in a Global Entitlement," on page 55.
--listEntitlements	Lists associations between users or user groups and global entitlements. "Listing the Users or Groups in a Global Entitlement," on page 55.
--listGlobalEntitlements	Lists all global entitlements. See "Listing Global Entitlements," on page 54.
--listPods	Lists the pods in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 58.
--listSites	Lists the sites in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 58.

Table 5-2. lmvutil Command Options (Continued)

Option	Description
--listUserAssignments	Lists the dedicated desktop pod assignments for a user and global entitlement combination. See "Listing User Assignments," on page 57.
--removePoolAssociation	Removes the association between a desktop pool and a global entitlement. See "Removing a Desktop Pool From a Global Entitlement," on page 50.
--resolveUserHomeSite	Shows the effective home site for a user. See "Listing the Effective Home Site for a User," on page 56.
--removeGroupEntitlement	Removes a user group from a global entitlement. See "Removing a User or Group From a Global Entitlement," on page 51.
--removeUserEntitlement	Removes a user from a global entitlement. See "Removing a User or Group From a Global Entitlement," on page 51.
--showGroupHomeSites	Shows all of the home sites for a group. See "Listing the Home Sites for a User or Group," on page 56.
--showUserHomeSites	Shows all of the home sites for a user. See "Listing the Home Sites for a User or Group," on page 56.
--uninitialize	Disables the Cloud Pod Architecture feature. See "Disabling the Cloud Pod Architecture Feature," on page 41.
--unjoin	Removes an available pod from a pod federation. See "Removing a Pod From a Pod Federation," on page 42.
--updateGlobalEntitlement	Modifies a global entitlement. See "Modifying a Global Entitlement," on page 48.
--updatePod	Modifies the name or description of a pod. See "Changing a Pod Name or Description," on page 43.
--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

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

Syntax

```
lmvutil --initialize
```

Usage Notes

You run this command only once, on one View Connection Server instance in the pod. You can run the command on any View 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

You can use the `lmvutil` command with the `--uninitialize` option to disable the Cloud Pod Architecture feature.

Syntax

```
lmvutil --uninitialize
```

Usage Notes

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

You run this command on only one View Connection Server instance in a pod. You can run the command on any View Connection Server instance in the pod. In a pod federation topology, you run this command for only one pod.

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

Example

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

Managing Pod Federations

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

- Joining a Pod to the Pod Federation on page 41

  You can use the `lmvutil` command with the `--join` option to join a pod to the pod federation.

- Removing a Pod From a Pod Federation on page 42

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

- Changing a Pod Name or Description on page 43

  You can 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

You can 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 View Connection Server instance in a pod.

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

Options

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

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

Option	Description
––joinServer	DNS name or IP address of any View Connection Server instance in any pod that has been initialized or is already part of the pod federation.
––userName	Name of a View 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

You can 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

You use the lmvutil command with the ––unjoin option to remove a pod from a pod federation. You can run the command on any View Connection Server instance in the pod.

You typically use the lmvutil command with the ––ejectPod option only to remove a pod that is not available. 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 lmvutil command with 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

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

Syntax

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

Usage Notes

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

Options

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

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

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

Example

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

Managing Sites

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

■ Creating a Site on page 44

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

■ Assigning a Pod to a Site on page 44

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

■ Changing a Site Name or Description on page 45

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

■ Deleting a Site on page 45

You can use the `lmvutil` command with the `--deleteSite` option to delete a site.

Creating a Site

You can 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

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

Options

You can specify these options when you create a site.

Table 5-5. Options for Creating a Site

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

Example

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

Assigning a Pod to a Site

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

Syntax

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

Usage Notes

Before you can assign a pod to a site, you must create the site. See "Creating a Site," on page 44.

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

Options

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

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

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

You can use the `lmvutil` command with the `--listPods` option to list the names of the pods in a Cloud Pod Architecture topology. See "Listing the Pods or Sites in a Cloud Pod Architecture Topology," on page 58.

Example

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

Changing a Site Name or Description

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

Syntax

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

Usage Notes

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

Options

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

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

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

Example

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

Deleting a Site

You can use the `lmvutil` command with the `--deleteSite` option to delete a site.

Syntax

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

Usage Notes

The `lmvutil` 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 entitlements in a Cloud Pod Architecture environment. Global entitlements link users to desktops, regardless of where the desktops are located in the pod federation. They also determine how the Cloud Pod Architecture feature allocates desktops to those users.

■ Creating a Global Entitlement on page 46

You can use the `lmvutil` command with the `--createGlobalEntitlement` to create a global entitlement. A global entitlement links together users and desktops, regardless of where the desktops are located in the pod federation. Global entitlements also include policies that determine how the Cloud Pod Architecture feature allocates desktops to those users.

■ Modifying a Global Entitlement on page 48

You can use the `lmvutil` command with the `--updateGlobalEntitlement` option to modify the scope, description, and other attributes of a global entitlement.

■ Deleting a Global Entitlement on page 49

You can use the `lmvutil` command with the `--deleteGlobalEntitlement` option to delete a global entitlement.

■ Adding a Desktop Pool to a Global Entitlement on page 49

You can use the `lmvutil` command with the `--addPoolAssociation` option to add a desktop pool to a global entitlement.

■ Removing a Desktop Pool From a Global Entitlement on page 50

You can use the `lmvutil` command with the `--removePoolAssociation` option to remove a desktop pool from a global entitlement.

■ Adding a User or Group to a Global Entitlement on page 51

You can use the `lmvutil` command with the `--addUserEntitlement` or `--addGroupEntitlement` option to add a user or group to a global entitlement.

■ Removing a User or Group From a Global Entitlement on page 51

You can use the `lmvutil` command with the `--removeUserEntitlement` or `--removeGroupEntitlement` option to remove a user or group from a global entitlement.

Creating a Global Entitlement

You can use the `lmvutil` command with the `--createGlobalEntitlement` to create a global entitlement. A global entitlement links together users and desktops, regardless of where the desktops are located in the pod federation. Global entitlements also include policies that determine how the Cloud Pod Architecture feature allocates desktops to those users.

Syntax

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

Usage Notes

You can use the `lmvutil` command on any View Connection Server instance in a pod federation. View stores new data in the Global Data Layer and replicates that data in all pods in the pod federation.

This command returns an error message if the global entitlement already exists, the scope is invalid, the Cloud Pod Architecture feature is not initialized, or the command cannot create the global entitlement.

Options

You can specify these options when you create a global entitlement.

Table 5-8. Options for Creating Global Entitlements

Option	Description
−−entitlementName	Name of the global entitlement. The name can contain between 1 and 64 characters. The global entitlement name appears in the list of available entitlements for the user in Horizon Client.
−−scope	Scope of the global entitlement. Valid values are as follows: ■ ANY. View looks for desktops on any pod in the pod federation. ■ SITE. View looks for desktops only on pods in the same site as the pod to which the user is connected. ■ LOCAL. View looks for desktops only in the pod to which the user is connected.
−−isDedicated	Creates a dedicated entitlement. A dedicated entitlement can contain only dedicated desktop pools. To create a floating entitlement, use the −−isFloating option. An entitlement can be either dedicated or floating. You cannot specify the −−isDedicated option with the −−multipleSessionAutoClean option.
−−isFloating	Creates a floating entitlement. A floating entitlement can contain only floating desktop pools. To create a dedicated entitlement, specify the −−isDedicated option. An entitlement can be either floating or dedicated.
−−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 View to look for desktops on the user's home site. If the user does not have a home site, View begins searching for desktops on the site to which the user is currently connected.
−−multipleSessionAutoClean	(Optional) Logs off extra user sessions for the same entitlement. Multiple floating desktop sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When multiple sessions occur, Horizon Client prompts the user to select a session. This option determines what happens to sessions that the user does not select. If you do not specify this option, users must manually end their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.
−−requireHomeSite	(Optional) Causes the global entitlement to be available only if the user has a home site. This option is applicable only when the −−fromHome option is also specified.
−−defaultProtocol	(Optional) Default display protocol for desktops in the global entitlement. Valid values are RDP and PCOIP.

Example

```
lmvutil −−authAs adminEast −−authDomain domainEast −−authPassword "*" −−createGlobalEntitlement
−−entitlementName "Agent Sales" −−scope LOCAL
−−isDedicated
```

Modifying a Global Entitlement

You can use the `lmvutil` command with the `--updateGlobalEntitlement` option to modify the scope, description, and other attributes of a global entitlement.

Syntax

```
lmvutil --updateGlobalEntitlement --entitlementName name
[--scope scope] [--description text] [--disabled] [--enabled]
[--fromHome] [--disableFromHome] [--multipleSessionAutoClean] [--disableMultipleSessionAutoClean]
[--requireHomeSite] [--disableRequireHomeSite] [--defaultProtocol value]
```

Usage Notes

You can use the `lmvutil` command on any View Connection Server instance in a pod federation. View stores new data in the Global Data Layer and replicates that data among all pods in the pod federation.

This command returns an error message if the global entitlement does not exist, the scope is invalid, the Cloud Pod Architecture feature is not initialized, or the command cannot update the global entitlement.

Options

You can specify these options when you modify a global entitlement.

Table 5-9. Options for Modifying Global Entitlements

Option	Description
--entitlementName	Name of the global entitlement to modify.
--scope	Scope of the global entitlement. Valid values are as follows: ■ ANY. View looks for desktops on any pod in the pod federation. ■ SITE. View looks for desktops only on pods in the same site as the pod to which the user is connected. ■ LOCAL. View looks for desktops 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 View to look for desktops on the user's home site. If the user does not have a home site, View begins searching for desktops on the site to which the user is currently connected.
--disableFromHome	(Optional) Disables the `--fromHome` option function if the `--fromHome` option was previously specified for the global entitlement.
--multipleSessionAutoClean	(Optional) Logs off extra user sessions for the same entitlement. Multiple floating desktop 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.

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

Option	Description
--disableMultipleSessionAutoClean	(Optional) Disables the --multipleSessionAutoClean option function if the --multipleSessionAutoClean option was previously specified for the global entitlement.
--requireHomeSite	(Optional) Causes the global entitlement to be available only if the user has a home site. This option is applicable only when the --fromHome option is also specified.
--disableRequireHomeSite	(Optional) Disables the --requireHomeSite option function if the --requireHomeSite option was previously specified for the global entitlement.
--defaultProtocol	(Optional) Default display protocol for desktops in the global entitlement. Valid values are RDP and PCOIP.

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalEntitlement
--entitlementName "Agent Sales" --scope ANY --isDedicated
```

Deleting a Global Entitlement

You can use the lmvutil command with the --deleteGlobalEntitlement option to delete a global entitlement.

Syntax

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

Command Usage

The lmvutil command returns an error message if the specified global entitlement does not exist, the Cloud Pod Architecture feature is not initialized, or the command cannot delete the global entitlement.

Options

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

Example

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

Adding a Desktop Pool to a Global Entitlement

You can use the lmvutil command with the --addPoolAssociation option to add a desktop pool to a global entitlement.

Syntax

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

Usage Notes

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

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

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

Options

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

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

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

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --addPoolAssociation --
entitlementName "Agent Sales" --poolId "Sales B"
```

Removing a Desktop Pool From a Global Entitlement

You can use the `lmvutil` command with the `‑‑removePoolAssociation` option to remove a desktop pool from a global entitlement.

Syntax

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

Usage Notes

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

Options

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

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

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

Example

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removePoolAssociation --entitlementName "Agent Sales" --poolID "Sales B"
```

Adding a User or Group to a Global Entitlement

You can use the `lmvutil` command with the `--addUserEntitlement` or `--addGroupEntitlement` option to add a user or group to a global entitlement.

Syntax

```
lmvutil --addUserEntitlement --userName domain\username --entitlementName name
lmvutil --addGroupEntitlement --groupName domain\groupname --entitlementName name
```

Usage Notes

Repeat the `lmvutil` command for each user or group to add to the global entitlement.

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

Options

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

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

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

Example

```
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

You can use the `lmvutil` command with the `--removeUserEntitlement` or `--removeGroupEntitlement` option to remove a user or group from a global entitlement.

Syntax

```
lmvutil --removeUserEntitlement --userName domain\username --entitlementName name
lmvutil --removeGroupEntitlement --groupName domain\groupname --entitlementName name
```

Usage Notes

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

Options

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

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

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

Example

```
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. You can associate a user or group with a home site to restrict desktop choice to a particular site.

■ Configuring a Home Site on page 52

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

■ Deleting a Home Site on page 53

You can use the `lmvutil` command with the `--deleteUserHomeSite` or `--deleteGroupHomeSite` option to remove the association between a user or group and a home site.

Configuring a Home Site

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

Syntax

```
lmvutil --createUserHomeSite --userName domain\username --siteName name [--entitlementName name]
lmvutil --createGroupHomeSite --groupName domain\groupname --siteName name [--entitlementName name]
```

Usage Notes

You must create a site before you can configure it as a home site. See "Creating a Site," on page 44.

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 command cannot create the home site.

Options

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

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

Option	Description
--userName	Name of a user to associate with the home site. Use the format *domain\username*.
--groupName	Name of a group to associate with the home site. Use the format *domain\groupname*.
--siteName	Name of the site to associate with the user or group as the home site.
--entitlementName	(Optional) Name of a global 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.

Example

```
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

You can use the `lmvutil` command with the `--deleteUserHomeSite` or `--deleteGroupHomeSite` option to remove the association between a user or group and a home site.

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 entitlement does not exist, or if the command cannot delete the home site setting.

Options

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

Table 5-15. Options for Deleting a Home Site

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

Example

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

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

Viewing a Cloud Pod Architecture Configuration

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

- Listing Global Entitlements on page 54

  You can use the `lmvutil` command with the `--listGlobalEntitlements` option to list all global entitlements.

- Listing the Desktop Pools in a Global Entitlement on page 55

  You can use the `lmvutil` command with the `--listAssociatedPools` option to list the desktop pools that are associated with a specific global entitlement.

- Listing the Users or Groups in a Global Entitlement on page 55

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

- Listing the Home Sites for a User or Group on page 56

  You can use the `lmvutil` command with the `--showUserHomeSites` or `--showGroupHomeSites` option to list all the configured home sites for a specific user or group.

- Listing the Effective Home Site for a User on page 56

  Because you can assign home sites to users and groups and to global entitlements, you can configure more than one home site for a specific user. You can use the `lmvutil` command with the `--resolveUserHomeSite` option to determine the effective home site for a specific user.

- Listing User Assignments on page 57

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

- Listing the Pods or Sites in a Cloud Pod Architecture Topology on page 58

  You can use the `lmvutil` command with the `--listPods` or `--listSites` option to view the pods or sites in your Cloud Pod Architecture topology.

Listing Global Entitlements

You can use the `lmvutil` command with the `--listGlobalEntitlements` option to list all global entitlements.

Syntax

```
lmvutil --listGlobalEntitlements
```

Usage Notes

This`lmvutil` command returns an error message if the Cloud Pod Architecture feature is not initialized or if the command cannot list the global entitlements.

Example

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

Listing the Desktop Pools in a Global Entitlement

You can use the `lmvutil` command with the `--listAssociatedPools` option to list the desktop pools that are associated with a specific global entitlement.

Syntax

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

Usage Notes

The `lmvutil` 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 pools.

Example

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

Listing the Users or Groups in a Global Entitlement

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

Syntax

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

Usage Notes

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

Options

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

Table 5-16. Options for Listing Global Entitlement Associations

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

Example

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

Listing the Home Sites for a User or Group

You can use the `lmvutil` command with the `--showUserHomeSites` or `--showGroupHomeSites` option to list all the configured home sites for a specific user or group.

Syntax

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

Usage Notes

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

Options

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

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

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

Example

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

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

Listing the Effective Home Site for a User

Because you can assign home sites to users and groups and to global entitlements, you can configure more than one home site for a specific user. You can use the `lmvutil` command with the `--resolveUserHomeSite` option to determine the effective home site for a specific user.

Syntax

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

Usage Notes

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

Options

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

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

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

Example

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

Listing User Assignments

You can use the `lmvutil` command with the `−−listUserAssignments` option 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 the `lmvutil` command is managed internally by the Cloud Pod Architecture brokering software.

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

Options

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

Table 5-19. Options for Listing User Assignments

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

You can use the `lmvutil` command with the `--listPods` or `--listSites` option to view the pods or sites in your Cloud Pod Architecture topology.

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

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

- Creating a Pending Certificate on page 58

  You can use the `lmvutil` command with the `--createPendingCertificate` option to create a pending SSL certificate.

- Activating a Pending Certificate on page 59

  You can use the `lmvutil` command with the `--activatePendingCertificate` option to activate a pending certificate.

Creating a Pending Certificate

You can use the `lmvutil` command with the `--createPendingCertificate` option to create a pending SSL certificate.

Syntax

```
LMVUtil --createPendingCertificate
```

Usage Notes

The `lmvutil` 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

You can 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 the `lmvutil` command. Wait for the Global Data Layer replication process to distribute the certificate to all View 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 View Connection Server instances.

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

Example

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

Index

U

uninitializing **35**
unitializing **41**

V

View URL **25**
VIPA communication channel **8**