Administrar la arquitectura Cloud Pod en Horizon 7

Modificado el 26 de julio de 2017
VMware Horizon 7 7.2

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Administrar Arquitectura de Cloud Pod en Horizon 7

Administrar la arquitectura Cloud Pod en Horizon 7 describe cómo configurar y administrar un entorno de Arquitectura de Cloud Pod en VMware Horizon® 7, incluida la forma de planificar una topología de Arquitectura de Cloud Pod y establecer, supervisar y mantener una configuración de Arquitectura de Cloud Pod.

Público al que se dirige

Esta información se dirige a todo aquel que desee configurar y mantener un entorno de Arquitectura de Cloud Pod. La información está escrita para administradores de sistemas Windows o Linux con experiencia que estén familiarizados con la tecnología de máquinas virtuales y operaciones de centros de datos.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario de términos que quizás desconozca. Para ver la definición de los términos que se utilizan en la documentación técnica de VMware, visite http://www.vmware.com/support/pubs.

Introducción a Arquitectura de Cloud Pod 1

La función Arquitectura de Cloud Pod usa componentes estándar de Horizon para proporcionar administración de centros de datos cruzados, asignación de usuarios a escritorios flexibles y globales, escritorios de alta disponibilidad y funcionalidad de recuperación ante desastres.

Este capítulo cubre los siguientes temas:

Comprender Arquitectura de Cloud Pod

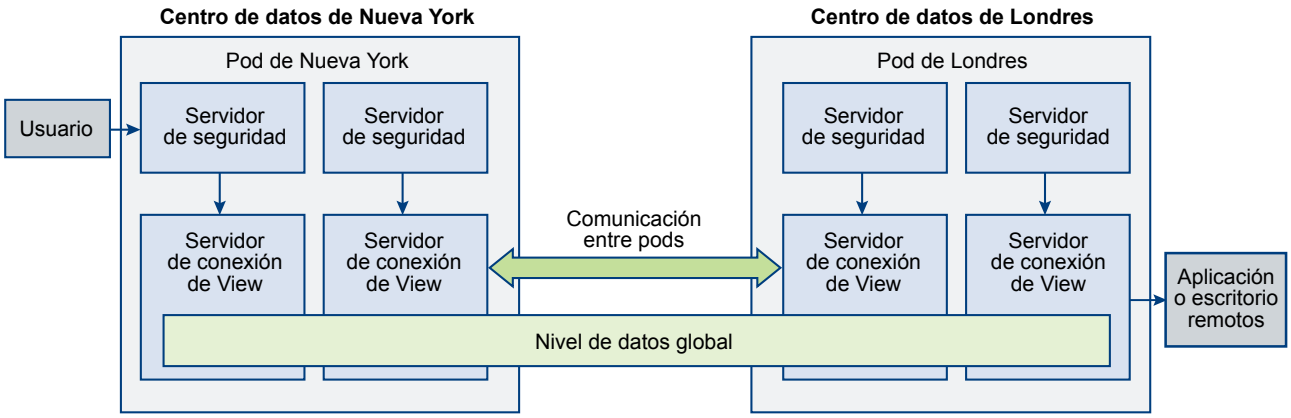
Con la función Arquitectura de Cloud Pod, puede vincular varios pods para ofrecer un único entorno de administración de aplicaciones y escritorios de gran tamaño.

Un pod consta de un grupo de instancias del servidor de conexión, un almacenamiento compartido, un servidor de la base de datos y vSphere, así como de las infraestructuras de red necesarias para alojar grupos de aplicaciones y escritorios. En una implementación de Horizon tradicional, administre cada pod de forma independiente. Con la función Arquitectura de Cloud Pod, puede conectar varios pods para formar una única implementación de Horizon que recibe el nombre de federación de pods.

Una federación de pods puede expandirse a varios sitios y bases de datos y, de forma simultánea, simplificar el esfuerzo de administración necesario para administrar una implementación de Horizon a gran escala.

El diagrama siguiente es un ejemplo de una topología de Arquitectura de Cloud Pod básica.

Figura 1-1. Topología Arquitectura de Cloud Pod básica



En esta topología de ejemplo, se conectan dos pods previamente independientes de centros de datos diferentes para formar una federación de pods única. Un usuario final de este entorno puede conectarse a la instancia del servidor de conexión en el centro de datos de Nueva York y recibir una aplicación o un escritorio en el centro de datos de Londres.

Compartir datos de clave en el Nivel de datos global

Las instancias del servidor de conexión de una federación de pods usan el Nivel de datos global para compartir datos de clave. Los datos compartidos incluyen información sobre la topología de la federación de pods, autorizaciones de grupos y usuarios, directivas, además de otro tipo de información de la configuración de Arquitectura de Cloud Pod.

En un entorno de Arquitectura de Cloud Pod, los datos compartidos se replican en cada instancia del servidor de conexión en una federación de pods. La información de la configuración de la topología y la autorización almacenada en el Nivel de datos global determina dónde y cómo se asignan los escritorios en la federación de pods.

Horizon configura el Nivel de datos global en cada instancia del servidor de conexión de una federación de pods cuando inicializa la función Arquitectura de Cloud Pod.

Enviar mensajes entre pods

Las instancias del servidor de conexión se comunican en un entorno de Arquitectura de Cloud Pod gracias a un protocolo de comunicación entre pods denominado API Interpod de View (VIPA).

Las instancias del servidor de conexión usan el canal de comunicación VIPA para iniciar nuevos escritorios, encontrar escritorios existentes y compartir datos de estado, además de otra información. Horizon configura el canal de comunicación VIPA cuando inicializa la función Arquitectura de Cloud Pod.

Configurar y administrar un entorno de Arquitectura de Cloud Pod

Use Horizon Administrator y la interfaz de la línea de comando de `lmvutil` para configurar y administrar un entorno de Arquitectura de Cloud Pod. `lmvutil` se instala como parte de la instalación de Horizon. También puede usar Horizon Administrator para ver el estado de los pods y obtener información sobre las sesiones.

Limitaciones de Arquitectura de Cloud Pod

La función Arquitectura de Cloud Pod tiene algunas limitaciones.

- La función Arquitectura de Cloud Pod no se admite en un entorno IPv6.
- No se admiten clientes en modo de pantalla completa en una implementación de Arquitectura de Cloud Pod si no implementa una solución alternativa. Para obtener más instrucciones, consulte el artículo 2148888 de la base de conocimientos de VMware.

Diseñar una topología de Arquitectura de Cloud Pod 2

Antes de empezar a configurar la función Arquitectura de Cloud Pod, debe tomar varias decisiones sobre su topología de Arquitectura de Cloud Pod. Las topologías de Arquitectura de Cloud Pod pueden variar en función de los objetivos, de las necesidades de los usuarios y de la implementación de Horizon existente. Si conecta pods de Horizon existentes a una federación de pods, la topología de Arquitectura de Cloud Pod se basa en la topología de la red existente.

Este capítulo cubre los siguientes temas:

Crear sitios de Arquitectura de Cloud Pod

En un entorno de Arquitectura de Cloud Pod, un sitio es una recopilación de pods conectados correctamente en la misma ubicación física, que suele ser un centro de datos único. La función Arquitectura de Cloud Pod trata de igual manera a los pods que están en el mismo sitio.

Cuando inicia la función de Arquitectura de Cloud Pod, esta organiza todos los pods en un sitio predeterminado denominado Primer sitio predeterminado. Si cuenta con una implementación de gran tamaño, es posible que desee crear sitios adicionales y agregar pods a dichos sitios.

La función Arquitectura de Cloud Pod asume que los pods del mismo sitio están en la misma LAN y que los pods de sitios distintos están en distintas LAN. Como los pods conectados a WAN tienen un rendimiento de red más lento, la función Arquitectura de Cloud Pod otorga preferencia a los escritorios y las aplicaciones que están en el sitio o el pod locales cuando asigna los escritorios y las aplicaciones a los usuarios.

Los sitios pueden ser parte útil de una solución de recuperación ante desastres. Por ejemplo, puede asignar pods de distintos centros de datos a sitios distintos y autorizar usuarios y grupos para que usen los grupos que abarcan esos sitios. Si un centro de datos de un sitio no se encuentra disponible, puede usar los escritorios y las aplicaciones del sitio que si lo esté para cumplir las solicitudes del usuario.

Autorizar usuarios y grupos en la federación de pods

En un entorno tradicional de Horizon, debe usar Horizon Administrator para crear autorizaciones locales. Estas autorizaciones locales permiten a los usuarios y a los grupos utilizar un grupo específico de aplicaciones o de escritorios en una instancia del servidor de conexión.

En un entorno de Arquitectura de Cloud Pod, puede crear autorizaciones globales para autorizar a los usuarios y a los grupos a utilizar varios escritorios y aplicaciones a través de varios pods de la federación. Cuando use autorizaciones globales, no es necesario configurar ni administrar autorizaciones locales. Las autorizaciones globales simplifican la administración, incluso en una federación de pods que contiene un único pod.

Las autorizaciones globales se almacenan en el Nivel de datos global. Dado que las autorizaciones globales son datos compartidos, la información relacionada está disponible en todas las instancias del servidor de conexión de la federación de pods.

Puede autorizar a grupos y a usuarios a utilizar los escritorios si crea autorizaciones de escritorios globales. Cada autorización de escritorios global contiene una lista de grupos o usuarios miembros, una lista de grupos de escritorios que pueden proporcionar escritorios a los usuarios autorizados y una directiva de ámbito. Los grupos de escritorios de una autorización global pueden ser grupos dedicados o flotantes. Debe especificar si una autorización global es flotante o dedicada durante su creación.

Puede autorizar a grupos y a usuarios a utilizar las aplicaciones si crea autorizaciones de aplicaciones globales. Cada autorización de aplicaciones global contiene una lista de grupos o usuarios miembros, una lista de grupos de aplicaciones que pueden proporcionar aplicaciones a los usuarios autorizados y una directiva de ámbito.

Una directiva de ámbito de la autorización global especifica dónde debe buscar Horizon aplicaciones y escritorios cuando los asigna a los usuarios en la autorización global. También determina si Horizon busca escritorios o aplicaciones en cualquier pod de la federación, en pods que se encuentran en el mismo sitio o solamente en el pod al que el usuario está conectado.

Como práctica recomendada, no debe configurar las autorizaciones globales y locales del mismo grupo de escritorios. Por ejemplo, si crea autorizaciones globales y locales para el mismo grupo de escritorios, es posible que aparezca el mismo escritorio como una autorización global y local en la lista de escritorios y aplicaciones que Horizon Client muestra a un usuario autorizado. De forma similar, no debe configurar las autorizaciones globales y locales para grupos de aplicaciones creados desde la misma granja.

Buscar y asignar aplicaciones y escritorios en la federación de pods

Las instancias del servidor de conexión en un entorno de Arquitectura de Cloud Pod usan autorizaciones globales compartidas e información de la configuración de la topología desde el Nivel de datos global para determinar dónde buscar y cómo asignar las aplicaciones y los grupos en la federación de pods.

Cuando un usuario solicita un escritorio o una aplicación desde una autorización global, Horizon busca una aplicación o un escritorio disponible en los grupos que están asociados a esa autorización. De forma predeterminada, Horizon otorga preferencia al pod local, al sitio local y a los pods de otros sitios, en ese orden.

Para las autorizaciones de escritorios globales que contienen grupos de escritorios dedicados, Horizon usa el comportamiento de búsqueda predeterminado únicamente la primera vez que un usuario solicita un escritorio. Una vez que Horizon asigna un escritorio dedicado, vuelve a enviar al usuario directamente al mismo escritorio.

Puede modificar el comportamiento de búsqueda y asignación de las autorizaciones globales individuales si establece la directiva de ámbito y configura los sitios principales.

Comprender la directiva de ámbito

Cuando crea una autorización de escritorios global o una autorización de aplicaciones global, debe especificar esta directiva de ámbito. La directiva de ámbito especifica el ámbito de búsqueda cuando Horizon busca escritorios o aplicaciones para satisfacer una solicitud de la autorización global.

Puede configurar la directiva de ámbitos para que Horizon busque solamente en el pod al que el usuario está conectado, en los pods que se encuentran dentro del mismo sitio que el pod del usuario o en todos los pods de la federación.

Para las autorizaciones de escritorio globales que contienen pods dedicados, la directiva de ámbitos afecta al lugar en el que Horizon busca los escritorios la primera vez que un usuario solicita un escritorio dedicado. Una vez que Horizon asigna un escritorio dedicado, vuelve a enviar al usuario directamente al mismo escritorio.

Información sobre la directiva de varias sesiones por usuario

Cuando cree una autorización de escritorio global, puede especificar si los usuarios pueden iniciar sesiones de escritorios independientes desde distintos dispositivos cliente. La directiva de varias sesiones por usuario se aplica solo a las autorizaciones de escritorios globales que incluyen grupos de escritorios flotantes.

Cuando habilite la directiva de varias sesiones por usuario, los usuarios que se conectan a la autorización global desde dispositivos cliente diferentes reciben sesiones de escritorios diferentes. Para volver a conectarse a una sesión de escritorios existente, los usuarios deben usar el mismo dispositivo desde el que se inició la sesión. Si no habilita esta directiva, los usuarios siempre se volverán a conectar a las sesiones de escritorios existentes, independientemente del dispositivo cliente que usen.

Si habilita la directiva de varias sesiones por usuario para una autorización global, todos los grupos de escritorios asociados a la autorización global también deben admitir varios usuarios por sesión.

Usar sitios principales

Un sitio principal supone una relación entre un usuario o un grupo y un sitio de Arquitectura de Cloud Pod. Con los sitios principales, Horizon comienza a buscar los escritorios y las aplicaciones desde un sitio específico en lugar de buscar escritorios y aplicaciones según la ubicación actual del usuario.

Si el sitio principal no está disponible o no tiene recursos que cumplan la solicitud del usuario, Horizon continúa buscando otros sitios según la directiva de ámbito configurada para la autorización global.

Para las autorizaciones de escritorio globales que contienen pods dedicados, el sitio principal afecta al lugar en el que Horizon busca los escritorios la primera vez que un usuario solicita un escritorio dedicado. Una vez que Horizon asigna un escritorio dedicado, vuelve a enviar al usuario directamente al mismo escritorio.

La función Arquitectura de Cloud Pod incluye los siguientes tipos de asignaciones de sitios principales.

Sitio principal global

Un sitio principal que se asigna a un usuario o a un grupo.

Si un usuario que tiene un sitio principal pertenece a un grupo que está asociado a un sitio principal diferente, el asociado al usuario tiene prioridad sobre la asignación de sitio principal del grupo.

Los sitios principales globales son útiles para controlar dónde reciben los usuarios en itinerancia las aplicaciones y los escritorios. Por ejemplo, si un usuario tiene un sitio principal en Nueva York pero está visitando Londres, Horizon comienza a buscar en el sitio de Nueva York para satisfacer la solicitud del escritorio del usuario en lugar de asignar un escritorio más cercano al usuario. Las asignaciones de los sitios principales globales se aplican a todas las autorizaciones globales.

IMPORTANTE: De forma predeterminada, las autorizaciones globales no reconocen sitios principales. Para establecer que una autorización global use sitios principales, debe seleccionar la opción **Utilizar sitio principal** al crear o modificar la autorización global.

Sitio principal por autorización global (sitio principal de reemplazo)

Un sitio principal que está asociado a una autorización global.

Los sitios principales por autorización global reemplazan las asignaciones del sitio principal global. Por esta razón, los sitios principales por autorización global también se conocen como sitio principal de reemplazo.

Por ejemplo, si un usuario que tiene el sitio principal en Nueva York accede a una autorización global que asocia dicho usuario al sitio principal de Londres, Horizon empieza a buscar en el sitio de Londres para cumplir la solicitud de la aplicación del usuario en lugar de asignar una aplicación del sitio de Nueva York.

La configuración de sitios principales es opcional. Si un usuario no tiene un sitio principal, Horizon busca y asigna escritorios y aplicaciones como se describe en "Buscar y asignar aplicaciones y escritorios en la federación de pods," página 10.

Consideraciones para los usuarios sin autenticar

Un administrador de Horizon puede crear usuarios para que accedan sin autenticar a aplicaciones publicadas en una instancia del servidor de conexión. En un entorno de Arquitectura de Cloud Pod, puede autorizar estos usuarios sin autenticar a las aplicaciones de la federación de pods agregándolas a las autorizaciones de aplicaciones globales.

A continuación, se muestran las consideraciones para usuarios sin autenticar de un entorno de Arquitectura de Cloud Pod.

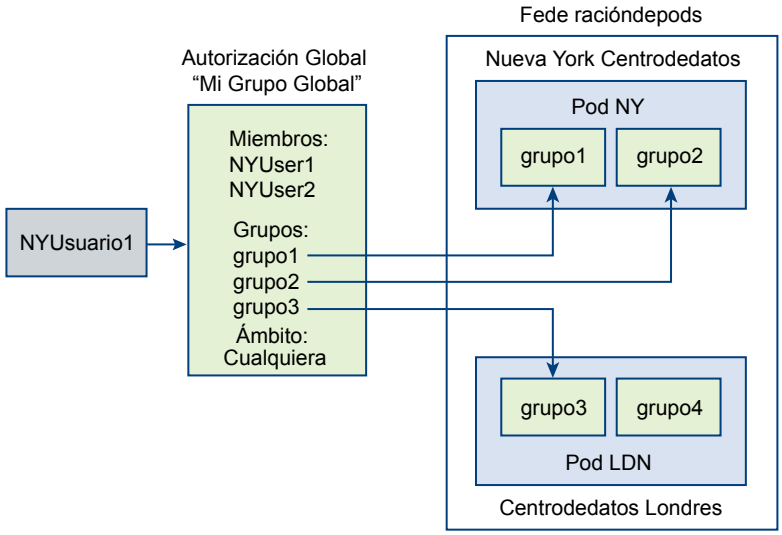
- Los usuarios sin autenticar solo pueden tener autorizaciones de aplicaciones globales. Si un usuario sin autenticar se incluye en una autorización de escritorios global, aparece un icono de advertencia junto al nombre de la pestaña **Usuarios y grupos** de la autorización de escritorios global en Horizon Administrator.
- Cuando conecta un pod a la federación de pods, los datos de los usuarios sin autenticar se envían al Nivel de datos global. Si desconecta o expulsa de la federación un pod que contiene usuarios sin autenticar, los datos de estos usuarios referentes a ese pod se eliminan del Nivel de datos global.
- Solo puede tener un usuario sin autenticar para cada usuario de Active Directory. Si el mismo alias de usuario está asignado a más de un usuario de Active Directory, Horizon Administrator muestra un mensaje de error en la pestaña **Acceso sin autenticar** en el panel Usuarios y grupos.
- Puede asignar sitios principales a usuarios sin autenticar.
- Los usuarios sin autenticar pueden tener varias sesiones.

Para obtener más información sobre cómo configurar los usuarios sin autenticar, consulte el documento *Administración de View*.

Ejemplo de autorización global

En este ejemplo NYUser1 es un miembro de la autorización de escritorios global denominado Mi grupo global. Mi grupo global proporciona una autorización para tres grupos de escritorios flotantes, denominados grupo1, grupo2 y grupo3. grupo1, grupo2 se encuentran en un pod denominado Pod NY en el centro de datos de Nueva York y grupo3 y grupo 4 se encuentran en un pod denominado Pod LDN en el centro de datos de Londres.

Figura 2-1. Ejemplo de autorización global



Dado que Mi grupo global tiene una directiva de ámbito CUALQUIERA, la función Arquitectura de Cloud Pod busca escritorios tanto en Pod NY como en Pod LDN cuando NYUsuario1 solicita un escritorio. La función Arquitectura de Cloud Pod no intenta asignar un escritorio desde grupo4 ya que este grupo no forma parte de Mi grupo global.

Si NYUsuario1 inicia sesión en Pod NY, la función Arquitectura de Cloud Pod asigna un escritorio desde grupo1 o grupo2, si hay algún escritorio disponible. Si no hay ningún escritorio disponible en grupo1 ni en grupo2, la función Arquitectura de Cloud Pod asigna un escritorio desde grupo3.

Para consultar un ejemplo de autorizaciones globales restringidas, consulte “Ejemplo de autorización global restringida,” página 15.

Restringir acceso a las autorizaciones globales

Puede configurar la función de las autorizaciones globales restringidas para limitar el acceso a las autorizaciones globales en función de la instancia del servidor de conexión a la que se conectan los usuarios inicialmente cuando seleccionan dichas autorizaciones.

Con las autorizaciones globales restringidas, asigne una o varias etiquetas a una instancia del servidor de conexión. A continuación, cuando configure una autorización global, especifique las etiquetas de las instancias del servidor de conexión que desea que tengan acceso a la autorización global.

Puede agregar etiquetas a autorizaciones de escritorios globales y a autorizaciones de aplicaciones globales.

Coincidencia de etiquetas

La función de autorizaciones globales restringidas utiliza la coincidencia de etiquetas para determinar si una instancia del servidor de conexión puede acceder a una autorización global determinada.

En el nivel más básico, la coincidencia de etiquetas determina que una instancia del servidor de conexión que tiene una etiqueta específica pueda acceder a una autorización global que cuenta con la misma etiqueta.

La ausencia de asignaciones de etiquetas también puede tener un efecto si los usuarios que se conectan a una instancia del servidor de conexión pueden acceder a una autorización global. Por ejemplo, las instancias del servidor de conexión sin etiquetas solo pueden acceder mediante autorizaciones globales que tampoco tengan ninguna etiqueta.

Tabla 2-1 muestra el modo en que la coincidencia de etiquetas determina cuándo una instancia del servidor de conexión puede acceder a una autorización global.

Tabla 2-1. Reglas de coincidencia de etiquetas

Servidor de conexión	Autorización global	¿Acceso permitido?
Sin etiquetas	Sin etiquetas	Sí
Sin etiquetas	Una o varias etiquetas	No
Una o varias etiquetas	Sin etiquetas	Sí
Una o varias etiquetas	Una o varias etiquetas	Solo cuando coinciden las etiquetas

La función de autorizaciones globales restringidas solo aplican la coincidencia de etiquetas. Debe diseñar su topología de red para forzar a determinados clientes a conectarse a través de una instancia particular del servidor de conexión.

Consideraciones y limitaciones para las autorizaciones globales restringidas

Antes de implementar las autorizaciones globales restringidas, debe tener en cuenta algunas consideraciones y limitaciones.

- Una única instancia del servidor de conexión o una autorización global puede tener varias etiquetas.
- Varias instancias del servidor de conexión y autorizaciones globales pueden tener la misma etiqueta.
- Cualquier instancia del servidor de conexión puede acceder a una autorización global que no tenga ninguna etiqueta.
- Las instancias del servidor de conexión sin etiquetas solo pueden acceder a autorizaciones globales que tampoco tengan etiquetas.
- Si usa un servidor de seguridad, debe configurar autorizaciones restringidas en la instancia del servidor de conexión con la que el servidor de seguridad está emparejado. No puede configurar autorizaciones restringidas en un servidor de seguridad.
- Las autorizaciones globales restringidas tienen preferencia sobre otras autorizaciones o asignaciones. Por ejemplo, aunque un usuario esté asignado a una máquina en particular, el usuario no puede acceder a esa máquina si la etiqueta asignada a la autorización global no coincide con la etiqueta asignada a la instancia del servidor de conexión a la que el usuario está conectado.
- Si pretende proporcionar acceso a las autorizaciones globales mediante VMware Identity Manager y configura las restricciones del servidor de conexión, la aplicación VMware Identity Manager puede mostrar las autorizaciones globales a los usuarios cuando estas autorizaciones están restringidas. Cuando un usuario de VMware Identity Manager intenta conectarse a una autorización global, el escritorio o la aplicación no se inician si la etiqueta asignada a la autorización global no coincide con la etiqueta asignada a la instancia del servidor de conexión a la que el usuario está conectado.

Ejemplo de autorización global restringida

En este ejemplo, se muestra un entorno de Arquitectura de Cloud Pod que incluye dos pods. Ambos pods contienen dos instancias del servidor de conexión. La primera instancia del servidor de conexión admite usuarios internos, mientras que la segunda instancia del servidor de conexión está emparejada con un servidor de seguridad y admite usuarios externos.

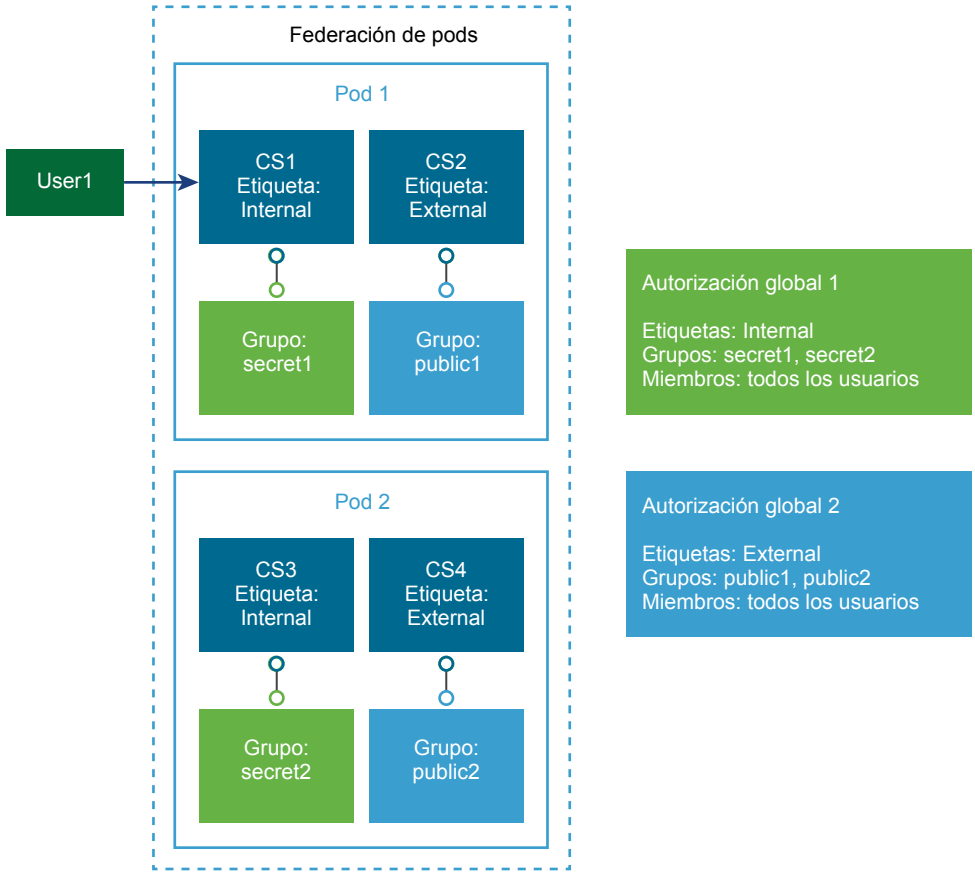
Para evitar que los usuarios externos accedan a determinados grupos de aplicaciones y de escritorios, puede asignar etiquetas como las que se indican a continuación:

- Asigne la etiqueta "Internal" a la instancia del servidor de conexión que admite usuarios internos.
- Asigne la etiqueta "External" a las instancias del servidor de conexión que admite usuarios externos.
- Asigne la etiqueta "Internal" a las autorizaciones globales que deban ser accesibles únicamente para los usuarios internos.
- Asigne la etiqueta "External" a las autorizaciones globales que deban ser accesibles únicamente para los usuarios externos.

Los usuarios externos no pueden ver las autorizaciones globales que están etiquetadas como Internal porque inician sesión a través de instancias del servidor de conexión que están etiquetadas como External. Los usuarios internos no pueden ver las autorizaciones globales que están etiquetadas como External porque inician sesión a través de instancias del servidor de conexión que están etiquetadas como Internal.

En el siguiente diagrama, User1 se conecta a la instancia del servidor de conexión denominada CS1. Dado que CS1 está etiquetada como Internal al igual que la autorización global 1, User1 solo puede ver la autorización global 1. Dado que la autorización global 1 incluye grupos secret1 y secret2, User1 solo puede recibir escritorios y aplicaciones de los grupos secret1 y secret2.

Figura 2-2. Ejemplo de autorización global restringida



Consideraciones para el modo Workspace ONE

Si un administrador de Horizon habilita el modo Workspace ONE para una instancia del servidor de conexión, es posible que los usuarios de Horizon Client se redireccionen a un servidor de Workspace ONE para iniciar sus autorizaciones.

Durante la configuración del modo Workspace ONE, el administrador de Horizon especifica el nombre de host del servidor Workspace ONE. En un entorno de Arquitectura de Cloud Pod, cada pod de una federación debe configurarse para que se dirijan al mismo servidor de Workspace ONE.

Para obtener más información sobre cómo configurar el modo Workspace ONE, consulte cómo configurar las directivas de acceso de Workspace ONE en Horizon Administrator que aparece en el documento *Administración de View*.

Límites de la topología de Arquitectura de Cloud Pod

Una topología típica de Arquitectura de Cloud Pod consta de dos o más pods, que se vinculan en una federación de pods. Las federaciones de pods están sujetas a ciertos límites.

Tabla 2-2. Límites de la federación de pods

Objeto	Límite
Sesiones totales	120.000
Pods	25
Sesiones por pod	10.000

Tabla 2-2. Límites de la federación de pods (Continua)

Objeto	Límite
Sitios	5
Instancias del servidor de conexión	175

Requisitos de puertos de Arquitectura de Cloud Pod

Ciertos puertos de red se deben abrir en el firewall de Windows para que Arquitectura de Cloud Pod funcione. Cuando instale el servidor de conexión, el programa de instalación puede configurar de forma opcional las reglas de firewall que necesita. Estas reglas abren los puertos que se utilizan de forma predeterminada. Si cambia los puertos predeterminados tras la instalación o la red tiene otros firewalls, debe configurar de forma manual el firewall de Windows.

Tabla 2-3. Puertos abiertos durante la instalación del servidor de conexión

Protocolo	Puerto TCP	Descripción
HTTP	22389	Se usa para la replicación LDAP del nivel de datos global. Los datos compartidos se replican en cada instancia del servidor de conexión de una federación de pods. Cada instancia del servidor de conexión de una federación de pods ejecuta una segunda instancia LDAP para almacenar los datos compartidos.
HTTPS	22636	Se usa para la replicación LDAP segura del nivel de datos global.
HTTPS	8472	Se usa para la comunicación API Interpod de View (VIPA). Las instancias del servidor de conexión usan el canal de comunicación VIPA para iniciar nuevos escritorios y nuevas aplicaciones, encontrar escritorios existentes y compartir datos de estado, además de otra información.

Consideraciones de seguridad para topologías de Arquitectura de Cloud Pod

Para usar Horizon Administrator o el comando `lmvutil` para configurar y administrar un entorno de Arquitectura de Cloud Pod, debe tener la función Administradores. Los usuarios que tengan esta función en el grupo de acceso raíz se consideran superusuarios.

Cuando una instancia del servidor de conexión es parte de un grupo replicado de instancias del servidor de conexión, los derechos de los superusuarios se amplían a otras instancias del servidor de conexión del pod. De forma similar, cuando un pod se conecta a una federación, los derechos de los superusuarios se amplían a todas las instancias del servidor de conexión que se encuentran en todos los pods de la federación. Estos derechos son necesarios para modificar las autorizaciones globales y realizar otras operaciones en el Nivel de datos global.

Si no desea que ciertos superusuarios puedan realizar operaciones en el Nivel de datos global, puede eliminar la asignación de la función de administradores y asignar la función de administradores locales en su lugar. Los usuarios que tengan la función de administradores locales tienen derechos de superusuarios únicamente en la instancia del servidor de conexión local y en todas las instancias de un grupo replicado.

Para obtener más información sobre la asignación de funciones en Horizon Administrator, consulte el documento *Administración de View*.

Configurar un entorno de Arquitectura de Cloud Pod 3

La configuración de un entorno de Arquitectura de Cloud Pod incluye la inicialización de la función Arquitectura de Cloud Pod, conectar pods a la federación de pods y crear autorizaciones globales.

Debe crear y configurar al menos una autorización global para usarla en la función Arquitectura de Cloud Pod. De forma opcional, puede crear sitios y asignar sitios principales.

Este capítulo cubre los siguientes temas:

Inicializar la función Arquitectura de Cloud Pod

Antes de configurar un entorno de Arquitectura de Cloud Pod, debe inicializar la función Arquitectura de Cloud Pod.

Solo es necesario que inicialice la función Arquitectura de Cloud Pod una vez, en el primer pod de una federación. Para agregar pods a la federación, conecte los nuevos pods al inicializado.

Durante el proceso de inicialización, Horizon configura el Nivel de datos global en cada instancia del servidor de conexión del pod, configura el canal de comunicación VIPA y establece un acuerdo de replicación entre cada instancia del servidor de conexión.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión del pod.

  Puede inicializar la función Arquitectura de Cloud Pod desde cualquier instancia del servidor de conexión de un pod.

2 En Horizon Administrator, seleccione **Configuración de View > Arquitectura Cloud Pod** y haga clic en **Iniciar la función de arquitectura Cloud Pod**.

3 Cuando aparezca el cuadro de diálogo Iniciar, haga clic en **Aceptar** para iniciar el proceso.

Horizon Administrator muestra el curso del proceso de inicialización. Este proceso puede durar varios minutos.

Tras inicializar la función Arquitectura de Cloud Pod, la federación de pods contiene el pod inicializado y un sitio único. El nombre predeterminado de la federación de pods es Horizon Cloud Pod Federation. El nombre de pod predeterminado se basa en el nombre del host de la instancia del servidor de conexión. Por ejemplo, si el nombre del host es CS1, el nombre del pod es Clúster-CS1. El nombre del sitio predeterminado es Primer sitio predeterminado.

4 Cuando Horizon Administrator le solicite que vuelva a cargar el cliente, haga clic en **Aceptar**.

Después de actualizar la interfaz de Horizon Administrator, **Autorizaciones globales** aparece bajo **Catálogo** y **Sitios** aparece bajo **Configuración de View** en el panel Inventario de Horizon Administrator.

5 (Opcional) Cambie el nombre predeterminado en la federación de pods, seleccione **Configuración de View > Arquitectura Cloud Pod**, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de diálogo **Nombre** y haga clic en **Aceptar**.

6 (Opcional) Cambie el nombre predeterminado del pod, seleccione **Configuración de View > Sitios**, seleccione el pod, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de diálogo **Nombre** y haga clic en **Aceptar**.

7 (Opcional) Cambie el nombre predeterminado del sitio, seleccione **Configuración de View > Sitios**, seleccione el sitio, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de diálogo **Nombre** y haga clic en **Aceptar**.

Qué hacer a continuación

Para agregar más pods a la federación, consulte "Conectar un pod a la federación de pods," página 20.

Conectar un pod a la federación de pods

Durante el proceso de inicialización de Arquitectura de Cloud Pod, la función Arquitectura de Cloud Pod crea una federación de pods que contiene solo uno. Puede usar Horizon Administrator para conectar pods adicionales a la federación. Esta conexión es opcional.

IMPORTANTE: No detenga ni inicie una instancia de servidor de conexión mientras la conecta a una federación de pods. Es posible que el servicio del servidor de conexión no se reinicie correctamente. Puede detener e iniciar el servidor de conexión después de que se conecte a la federación de pods.

Prerequisitos

- Asegúrese de que las instancias del servidor de conexión que desea conectar tengan nombres de host distintos. No puede conectar servidores que tengan el mismo nombre, aunque estén en dominios diferentes.
- Inicie la función Arquitectura de Cloud Pod. Consulte "Inicializar la función Arquitectura de Cloud Pod," página 19.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión en el pod que va a conectar a la federación de pods.

2 En Horizon Administrator, seleccione **Configuración de View > Arquitectura Cloud Pod** y haga clic en **Unirse a la federación de pods**.

3 En el cuadro de texto **Servidor de conexión**, escriba el nombre del host o la dirección IP de cualquier instancia del servidor de conexión de cualquier pod inicializado o que ya esté unido a la federación.

4 En el cuadro de texto **Nombre de usuario**, escriba el nombre de un usuario de Horizon Administrator en el pod ya inicializado.

   Use el formato *dominio\nombredeusuario*.

5 En el cuadro de texto **Contraseña**, escriba la contraseña del usuario de Horizon Administrator.

6 Haga clic en **Aceptar** para conectar el pod a la federación.

   Horizon Administrator muestra el curso del proceso de conexión. El nombre de pod predeterminado se basa en el nombre del host de la instancia del servidor de conexión. Por ejemplo, si el nombre del host es CS1, el nombre del pod es Clúster-CS1.

7 Cuando Horizon Administrator le solicite que vuelva a cargar el cliente, haga clic en **Aceptar**.

   Después de actualizar la interfaz de Horizon Administrator, **Autorizaciones globales** aparece bajo **Catálogo** y **Sitios** aparece bajo **Configuración de View** en el panel Inventario de Horizon Administrator.

8 (Opcional) Cambie el nombre predeterminado del pod, seleccione **Configuración de View > Sitios**, seleccione el pod, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de diálogo **Nombre** y haga clic en **Aceptar**.

Después de conectar el pod a la federación, este comienza a compartir datos de estado. Puede consultar estos datos de estado en el panel de control de Horizon Administrator. Consulte "Ver el estado de la federación de pods en Horizon Administrator," página 37.

NOTA: Es posible que se produzca un pequeño retraso una vez que los datos de estado estén disponibles en Horizon Administrator.

Qué hacer a continuación

Puede repetir estos pasos para conectar pods adicionales a la federación.

Asignar una etiqueta a una instancia del servidor de conexión de Horizon

Si tiene pensado restringir el acceso a una autorización global en función de la instancia del servidor de conexión a la que se conectan inicialmente los usuarios cuando estos seleccionan dicha autorización, primero debe asignar una o varias etiquetas a la instancia del servidor de conexión.

Prerequisitos

Familiarícese con la función de autorizaciones globales restringidas. Consulte "Restringir acceso a las autorizaciones globales," página 13.

Procedimiento

1 Inicie sesión en Horizon Administrator para la instancia del servidor de conexión.

2 Seleccione **Configuración de View > Servidores**.

3 Haga clic en la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión y haga clic en **Editar**.

4 Escriba una o varias etiquetas en el cuadro de texto **Etiquetas**.

   Para separar varias etiquetas, utilice una coma o punto y coma.

5 Haga clic en **Aceptar** para guardar los cambios.

6 Repita estos pasos con cada instancia del servidor de conexión a la que desee asignar etiquetas.

Qué hacer a continuación

Cuando cree o edite una autorización global, seleccione las etiquetas que estén asociadas a las instancias del servidor de conexión a las que quiera que tenga acceso la autorización global. Consulte "Crear y configurar una autorización global," página 22 o "Modificar atributos o directivas de una autorización global," página 39.

Crear y configurar una autorización global

Las autorizaciones globales permiten autorizar a los usuarios y los grupos a utilizar escritorios y aplicaciones en un entorno de Arquitectura de Cloud Pod. Las autorizaciones globales suponen un vínculo entre los usuarios y sus escritorios y aplicaciones, sin tener en cuenta cuál de esos escritorios y esas aplicaciones residen en la federación de pods.

Una autorización global contiene una lista de grupos o de usuarios miembros, un conjunto de directivas y una lista de los grupos que pueden proporcionar escritorios o aplicaciones a los usuarios autorizados. Puede agregar usuarios y grupos, solo usuarios o solo grupos a una autorización global.

Prerequisitos

- Inicie la función Arquitectura de Cloud Pod. Consulte "Inicializar la función Arquitectura de Cloud Pod," página 19.
- Decida el tipo de autorización global de escritorios que desea crear, los usuarios y los grupos que desea incluir en las autorizaciones globales y el ámbito de dicha autorización. Consulte "Autorizar usuarios y grupos en la federación de pods," página 10.
- Decida si quiere restringir el acceso a la autorización global en función de la instancia del servidor de conexión a la que se conectan los usuarios inicialmente cuando seleccionan dicha autorización. Consulte "Restringir acceso a las autorizaciones globales," página 13.
- Si tiene pensado restringir el acceso a la autorización global, asigne una o varias etiquetas a la instancia del servidor de conexión. Consulte "Asignar una etiqueta a una instancia del servidor de conexión de Horizon," página 21.
- Decida si quiere que las autorizaciones globales usen sitios principales. Consulte "Usar sitios principales," página 11.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales** y haga clic en **Agregar**.

3 Seleccione el tipo de autorización global que desea agregar y haga clic en **Siguiente**.

Opción	Descripción
Autorización de escritorios	Agrega una autorización de escritorios global.
Autorización de aplicaciones	Agrega una autorización de aplicaciones global.

4 Configure la autorización global.

a Introduzca un nombre para la autorización global en el cuadro de texto **Nombre**.

El nombre puede tener entre 1 y 64 caracteres. Este nombre aparecerá en la lista de aplicaciones y escritorios disponibles en Horizon Client para cada usuario autorizado.

b (Opcional) Introduzca una descripción para la autorización global en el cuadro de texto **Descripción**.

La descripción puede tener entre 1 y 1024 caracteres.

c (Opcional) Para restringir el acceso a la autorización global, haga clic en **Examinar**, seleccione **Elemento restringido a estas etiquetas**, seleccione las etiquetas que desee asociar a la autorización global y haga clic en **Aceptar**.

Solo las instancias del servidor de conexión que tengan las etiquetas seleccionadas pueden acceder a la autorización global.

NOTA: Solo puede seleccionar las etiquetas asignadas a las instancias del servidor de conexión en el pod local. Para seleccionar las etiquetas asignadas a las instancias del servidor de conexión en otro pod, debe iniciar sesión en el Horizon Administrator que se encuentra en una instancia del servidor de conexión del otro pod y modificar la autorización global.

d Si configura una autorización de escritorios global, seleccione una directiva de asignación de usuarios.

La directiva de asignación de usuarios especifica el tipo de grupo de escritorios que una autorización de escritorios global puede tener. Solo puede seleccionar una directiva de asignación de usuarios.

Opción	Descripción
Flotante	Crea una autorización de escritorio flotante. Una autorización de escritorio flotante solo puede tener grupos de escritorios flotantes.
Dedicado	Crea una autorización de escritorios dedicados. Una autorización de escritorios dedicados solo puede contener grupos de escritorios dedicados.

e Seleccione una directiva de ámbito para la autorización global.

La directiva de ámbito especifica dónde buscar escritorios o aplicaciones para satisfacer una solicitud de la autorización global. Solo puede seleccionar una directiva de ámbito.

Opción	Descripción
Todos los sitios	Busca escritorios o aplicaciones en los pods de la federación.
Dentro del sitio	Busca escritorios o aplicaciones únicamente en los pods del mismo sitio en el que se encuentra el pod al que el usuario está conectado.
Dentro del pod	Busca escritorios o aplicaciones únicamente en el pod al que el usuario está conectado.

f (Opcional) Si los usuarios tienen sitios principales, configure una directiva del sitio principal para la autorización global.

Opción	Descripción
Utilizar sitio principal	Empieza a buscar escritorios o aplicaciones en el sitio principal del usuario. Si el usuario no tiene un sitio principal y la opción **El usuario autorizado debe tener sitio principal** no está seleccionada, se asume que el sitio al que el usuario está conectado es el principal.
El usuario autorizado debe tener sitio principal	Hace que la autorización global esté disponible únicamente si el usuario tiene un sitio principal. La opción está disponible solo cuando la opción **Utilizar sitio principal** está seleccionada.

g (Opcional) La opción **Limpiar automáticamente las sesiones redundantes** permite especificar si desea borrar las sesiones redundantes.

NOTA: Esta opción está disponible únicamente para autorizaciones de escritorios flotantes y autorizaciones de aplicaciones globales.

Pueden aparecer varias sesiones cuando un pod que contiene una sesión se desconecta, el usuario inicia otra sesión y el pod con el problema vuelve a conectarse con la sesión original. Cuando aparecen varias sesiones, Horizon Client solicita que el usuario seleccione una de ellas. Esta opción determina qué sucede con las sesiones que el usuario no selecciona. Si no selecciona esta opción, los usuarios deben cerrar las sesiones adicionales de forma manual. Para hacerlo, pueden cerrar sesión en Horizon Client, o bien iniciar las sesiones y cerrarlas.

h Seleccione el protocolo de visualización predeterminado para escritorios o aplicaciones en la autorización global y especifique si desea permitir a los usuarios sobrescribir el protocolo de visualización predeterminado.

i (Solo para la autorización de escritorio global) Seleccione si desea permitir que los usuarios restablezcan los escritorios en la autorización de escritorios global.

j Seleccione si desea permitir que los usuarios utilicen la función de HTML Access para acceder a escritorios o aplicaciones en la autorización global.

Cuando habilite la directiva HTML Access, los usuarios finales pueden usar un navegador web para conectarse a aplicaciones y escritorios remotos y no es necesario instalar ningún software cliente en los sistemas locales.

k (Solo para la autorización de escritorios global) Seleccione si desea permitir que los usuarios inicien sesiones de escritorios independientes desde dispositivos cliente diferentes.

Cuando habilite la directiva de varias sesiones por usuario, los usuarios que se conectan a la autorización global desde dispositivos cliente diferentes reciben sesiones de escritorios diferentes. Para volver a conectarse a una sesión de escritorios existente, los usuarios deben usar el mismo dispositivo desde el que se inició la sesión. Si no habilita esta directiva, los usuarios siempre se volverán a conectar a las sesiones de escritorios existentes, independientemente del dispositivo cliente que usen. Solo puede habilitar esta directiva para las autorizaciones de escritorios flotantes.

NOTA: Si habilita esta directiva, todos los grupos de escritorios de la autorización global también deben admitir varias sesiones por usuario.

l (Solo para la autorización de escritorio global) Seleccione si desea iniciar la sesión de aplicación antes de que un usuario abra la autorización de aplicaciones global en Horizon Client.

Cuando habilite la directiva de preinicio, los usuarios pueden iniciar la autorización global de aplicaciones con mayor rapidez.

NOTA: Si habilita esta directiva, todos los grupos de aplicaciones de la autorización de aplicaciones global también deben ser compatibles con la función de preinicio de sesiones y, a su vez, el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.

5 Haga clic en **Siguiente** y agregue usuarios o grupos a la autorización global.

a Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos o los usuarios según sus criterios de búsqueda.

Puede seleccionar la casilla de verificación **Usuarios sin autenticar** para buscar y agregar usuarios con acceso sin autenticar a las autorizaciones de aplicaciones globales. No puede agregar usuarios con acceso sin autenticar a las autorizaciones de escritorios globales. Si intenta agregar un usuario con acceso sin autenticar a una autorización de escritorios global, Horizon Administrator devuelve un mensaje de error.

b Seleccione el grupo o el usuario que desea agregar a la autorización global y haga clic en **Aceptar**.

Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.

6 Haga clic en **Siguiente**, revise la configuración de la autorización global y haga clic en **Finalizar** para crear la autorización global.

La autorización global aparecerá en la página Autorizaciones globales.

La función Arquitectura de Cloud Pod almacena la autorización global en Nivel de datos global, que replica la autorización global en cada pod de la federación de pods.

Qué hacer a continuación

Seleccione los grupos que pueden proporcionar escritorios y aplicaciones para los usuarios en la autorización global que creó. Consulte "Agregar un grupo a una autorización global," página 25.

Agregar un grupo a una autorización global

Horizon Administrator permite agregar un grupo de escritorios a una autorización de escritorios global, o bien agregar un grupo de aplicaciones a una autorización de aplicaciones global.

Puede agregar tanto varios grupos como un grupo determinado a una autorización global.

Si agrega varios grupos de aplicaciones a una autorización de aplicaciones global, debe agregar la misma aplicación. Por ejemplo, no agregue Calculadora y Microsoft Office PowerPoint a la misma autorización de aplicaciones global. Si agrega distintas aplicaciones a la misma autorización de aplicaciones global, los usuarios autorizados pueden recibir diferentes aplicaciones en distintos momentos.

NOTA: Si un administrador de Horizon cambia el protocolo de visualización a nivel de grupo o la directiva para sobrescribir un protocolo después de que se asocie un grupo de escritorios con una autorización de escritorios global, los usuarios pueden recibir un error de inicio de escritorio cuando seleccionan la autorización del escritorio global. Si un administrador de Horizon cambia la directiva de restablecimiento de la máquina virtual a nivel de grupo después de que un grupo de escritorios se asocie con la autorización de escritorios global, los usuarios pueden recibir un error si intentan restablecer el escritorio.

Prerequisitos

- Crear y configurar una autorización global. Consulte "Crear y configurar una autorización global," página 22.
- Cree el grupo de aplicaciones o de escritorios que desee agregar a la autorización global. Consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

1. Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión del pod que contiene el grupo que desea agregar a la autorización global.
2. En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.
3. Haga doble clic en la autorización global.
4. En la pestaña **Grupos locales**, haga clic en **Agregar**, seleccione el grupo de aplicaciones o de escritorios y haga clic en **Agregar**.

   Puede pulsar las teclas Ctrl y Mayús para seleccionar varios grupos.

   NOTA: No se muestran los grupos que ya están asociados a una autorización global o que no cumplen los criterios de las directivas de la autorización global que seleccionó. Por ejemplo, si habilitó la directiva HTML Access, no puede seleccionar grupos que no permitan HTML Access.
5. Repita estos pasos en la instancia del servidor de conexión en cada pod que contenga un grupo que desee agregar a la autorización global.

Cuando un usuario autorizado use Horizon Client para conectarse a una instancia del servidor de conexión en la federación de pods, el nombre de la autorización global aparece en la lista de aplicaciones y escritorios disponibles.

Crear y configurar un sitio

Si la topología de Arquitectura de Cloud Pod contiene varios pods, es posible que quiera agruparlos en sitios distintos. La función Arquitectura de Cloud Pod trata de igual manera a los pods que están en el mismo sitio.

Prerequisitos

- Decida si la topología de Arquitectura de Cloud Pod debe incluir estos sitios. Consulte "Crear sitios de Arquitectura de Cloud Pod," página 9.
- Inicie la función Arquitectura de Cloud Pod. Consulte "Inicializar la función Arquitectura de Cloud Pod," página 19.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 Cree el sitio.

a En Horizon Administrator, seleccione **Configuración de View > Sitios** y haga clic en **Agregar**.

b Introduzca un nombre para el sitio en el cuadro de texto **Nombre**.

Un nombre de sitio puede tener entre 1 y 64 caracteres.

c (Opcional) Introduzca una descripción del sitio en el cuadro de texto **Descripción**.

Un nombre de sitio puede tener entre 1 y 1024 caracteres.

d Haga clic en **Aceptar** para crear el sitio.

3 Agregue un pod a un sitio.

Repita este paso en cada pod que desee agregar al sitio.

a En Horizon Administrator, seleccione **Configuración de View > Sitios** y seleccione el sitio que contenga en ese momento el pod que desee agregar al sitio.

Los nombres de los pods del sitio aparecen en el panel inferior.

b Seleccione el pod que desea agregar al sitio y haga clic en **Editar**.

c Seleccione el sitio en cuestión en el menú desplegable **Sitio** y haga clic en **Aceptar**.

Asignar un sitio principal a un usuario o grupo

Un sitio principal es la relación entre un usuario o un grupo y un sitio de Arquitectura de Cloud Pod. Con los sitios principales, Horizon comienza a buscar los escritorios y las aplicaciones desde un sitio específico en lugar de buscar escritorios y aplicaciones según la ubicación actual del usuario. La opción de asignar sitios principales es opcional.

Puede asociar una autorización global al sitio principal para que el sitio principal de la autorización sustituya al del usuario cuando este seleccione una autorización global. Si desea obtener más información, consulte "Crear un sitio principal de reemplazo," página 28.

Prerequisitos

- Decida si desea asignar sitios principales a usuarios o grupos en su entorno de Arquitectura de Cloud Pod. Consulte "Usar sitios principales," página 11.
- Agrupe los pods de la federación de pods en sitios. Consulte "Crear y configurar un sitio," página 26.
- De forma predeterminada, las autorizaciones globales no utilizan sitios principales. Al crear autorizaciones globales, debe seleccionar la opción **Utilizar sitio principal** para hacer que Horizon utilice el sitio principal de un usuario cuando se asignen escritorios desde dicha autorización global. Consulte "Crear y configurar una autorización global," página 22.
- Inicie la función Arquitectura de Cloud Pod. Consulte "Inicializar la función Arquitectura de Cloud Pod," página 19.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Usuarios y grupos** y haga clic en la pestaña **Sitio principal**.

3 En la pestaña **Sitio principal** haga clic en **Agregar**.

4 Seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos o los usuarios de acuerdo a estos criterios.

Puede seleccionar la casilla de verificación **Usuarios sin autenticar** para buscar usuarios de acceso sin autenticar en la federación de pods.

5 Seleccione un usuario o un grupo y haga clic en **Siguiente**.

6 Seleccione el sitio principal que desee asignar al usuario o al grupo en el menú desplegable **Sitio principal** y haga clic en **Finalizar**.

Crear un sitio principal de reemplazo

Puede asociar una autorización global al sitio principal para que el sitio principal de la autorización reemplace al del usuario cuando este seleccione una autorización global.

Para crear un sitio principal de reemplazo, debe asociar un sitio principal con una autorización global y un usuario o un grupo en particular. Cuando el usuario (o un usuario del grupo seleccionado) accede a la autorización global, el sitio principal de la autorización global reemplaza al del usuario.

Por ejemplo, si un usuario que tiene el sitio principal en Nueva York accede a una autorización global que asocia dicho usuario al sitio principal de Londres, Horizon busca en el sitio de Londres para cumplir la solicitud de aplicación del usuario en lugar de asignar una aplicación del sitio de Nueva York.

Prerequisitos

- Verifique que la autorización global tenge la directiva **Utilizar sitio principal** habilitada. Si desea obtener más información, consulte "Modificar atributos o directivas de una autorización global," página 39.
- Verifique que el usuario o el grupo esté incluido en la autorización global. Si desea obtener más información, consulte "Agregar un grupo o un usuario a una autorización global," página 39.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.

3 Haga doble clic en la autorización global para asociarla con un sitio principal.

4 En la pestaña **Sitio principal de reemplazo** haga clic en **Agregar**.

NOTA: El botón **Agregar** no está disponible si la directiva **Utilizar sitio principal** no está habilitada para la autorización global.

5 Seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos y los usuarios de Active Directory según sus criterios de búsqueda.

6 Seleccione el grupo o el usuario de Active Directory que tenga un sitio principal que desee sobrescribir.

El usuario o el grupo ya deben estar incluidos en la autorización global que seleccionó.

7 Seleccione el sitio principal que desea asociar con la autorización global en el menú desplegable **Sitio principal**.

8 Haga clic en **Finalizar** para crear el sitio principal de reemplazo.

Probar una configuración de Arquitectura de Cloud Pod

Después de inicializar y configurar un entorno de Arquitectura de Cloud Pod, realice algunos pasos para verificar que el entorno esté configurado correctamente.

Prerequisitos

- Instale la última versión de Horizon Client en un equipo o un dispositivo móvil compatibles.
- Compruebe que tenga credenciales para un usuario en una de sus autorizaciones globales recientemente creadas.

Procedimiento

1 Inicie Horizon Client.

2 Conéctese a cualquier instancia del servidor de conexión en la federación de pods con las credenciales de un usuario de una de sus nuevas autorizaciones globales.

  Después de conectarse a la instancia del servidor de conexión, el nombre de la autorización global aparece en la lista de aplicaciones y de escritorios disponibles.

3 Seleccione la autorización global y conéctese a un escritorio o a una aplicación.

El escritorio o la aplicación se inicia correctamente. El escritorio o la aplicación que se inicia depende de la configuración individual de la autorización global, los pods y los grupos de aplicaciones y de escritorios. La función Arquitectura de Cloud Pod intenta asignar un escritorio o una aplicación desde el pod al que está conectado.

Qué hacer a continuación

Si la autorización global no aparece cuando se conecta a la instancia del servidor de conexión, use Horizon Administrator para comprobar que la autorización está configurada correctamente. Si la autorización global aparece pero no se inicia ninguna aplicación ni ningún escritorio, todos los grupos de aplicaciones o de escritorios podrían estar asignados a otros usuarios.

Ejemplo: establecer una configuración de Arquitectura de Cloud Pod básica

Este ejemplo le muestra cómo puede usar la función Arquitectura de Cloud Pod para completar una configuración de Arquitectura de Cloud Pod.

En este ejemplo, una empresa aseguradora tiene una fuerza de ventas móvil que trabaja en dos regiones: la región central y la región oriental. Los agentes de ventas usan dispositivos móviles para presentar los contratos de seguros a los clientes y los clientes ven y firman documentos digitales.

En lugar de almacenar los datos de los clientes en los dispositivos móviles, los agentes de ventas usan escritorios flotantes normalizados. El acceso a los datos de los clientes en los centros de datos de la empresa aseguradora es seguro.

La empresa aseguradora cuenta con un centro de datos en cada región. Los problemas ocasionales de capacidad hacen que los agentes de ventas busquen escritorios disponibles en un centro de datos que no sea el local y, a veces, se producen problemas latencia de WAN. Si los agentes de ventas se desconectan de los escritorios pero mantienen las sesiones iniciadas, deben recordar los centros de datos que alojan las sesiones para volver a conectarse a los escritorios.

Para solucionar estos problemas, la empresa aseguradora diseña una topología de Arquitectura de Cloud Pod, inicia la función Arquitectura de Cloud Pod, conecta los pods existentes en la federación, crea los sitios de cada centro de datos, autoriza a los agentes de ventas para usar todos los grupos de escritorios e implementa una URL única.

1 Diseñar una topología de ejemplo página 30

La empresa aseguradora diseña una topología de Arquitectura de Cloud Pod que incluye un sitio para cada región.

2 Inicializar la configuración de ejemplo página 31

Para inicializar la función Arquitectura de Cloud Pod, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de la instancia del servidor de conexión de Horizon en Pod Oriental 1, selecciona **Configuración de View > Arquitectura Cloud Pod** y hace clic en **Iniciar la función de arquitectura Cloud Pod**.

3 Conectar los pods de la configuración de ejemplo página 31

El administrador de Horizon utiliza Horizon Administrator para conectar Pod Central 1 y Pod Central 2 a la federación de pods.

4 Crear sitios en la configuración de ejemplo página 31

El administrador de Horizon usa Horizon Administrator para crear un sitio para los centros de datos central y oriental, y para agregar pods a esos sitios.

5 Crear autorizaciones de escritorios globales en la configuración de ejemplo página 32

El administrador de Horizon usa Horizon Administrator para crear una única autorización de escritorios global que autorice a todos los agentes de ventas para que puedan utilizar todos los escritorios del grupo de escritorios de agentes de ventas en todas las federaciones de pods.

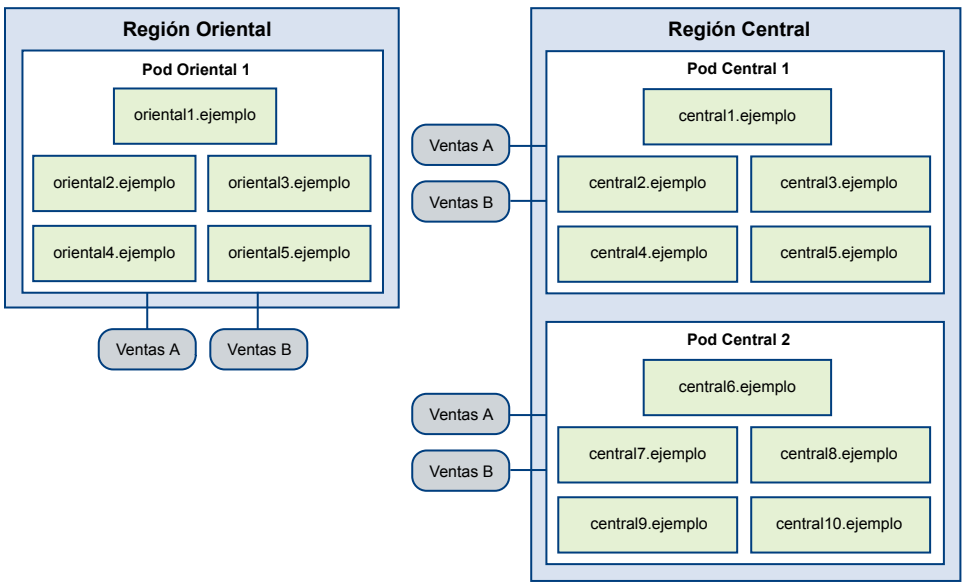
6 Crear una URL para la configuración de ejemplo página 33

La empresa aseguradora usa una URL única y emplea un servicio DNS para resolver ventas.ejemplo en el pod del centro de datos más cercano. Con esta organización, los agentes de ventas no necesitan recordar distintas URL para cada pod y se dirigen siempre al centro de datos más cercano, sin tener en cuenta dónde se encuentran.

Diseñar una topología de ejemplo

La empresa aseguradora diseña una topología de Arquitectura de Cloud Pod que incluye un sitio para cada región.

Figura 3-1. Topología de Arquitectura de Cloud Pod de ejemplo



En esta topología, el sitio de la región oriental contiene un pod único, Pod Oriental 1, que consta de cinco instancias del servidor de conexión cuyos nombres van de oriental1.ejemplo a oriental5.ejemplo.

El sitio de la región central contiene dos pods, Pod Central 1 y Pod Central 2. Cada pod contiene cinco instancias del servidor de conexión. Los servidores de conexión que se encuentran en el primer pod tienen nombres que van desde central1.ejemplo a central5.ejemplo. Las instancias de los servidores de conexión que se encuentran en el segundo pod tienen nombres que van desde central6.ejemplo a central10.ejemplo.

Cada pod de la topología contiene dos grupos de escritorios de agentes de ventas denominados Ventas A y Ventas B.

Inicializar la configuración de ejemplo

Para inicializar la función Arquitectura de Cloud Pod, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de la instancia del servidor de conexión de Horizon en Pod Oriental 1, selecciona **Configuración de View > Arquitectura Cloud Pod** y hace clic en **Iniciar la función de arquitectura Cloud Pod**.

Dado que el administrador de Horizon usa la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión en el Pod Oriental 1, la federación de pods contiene este pod inicialmente. La federación de pods también contiene un sitio único, denominado Primer sitio predeterminado, que contiene el Pod Oriental 1.

Conectar los pods de la configuración de ejemplo

El administrador de Horizon utiliza Horizon Administrator para conectar Pod Central 1 y Pod Central 2 a la federación de pods.

1 Para conectar Pod Central 1, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión de Pod Central 1, selecciona **Configuración de View > Arquitectura Cloud Pod**, hace clic en **Unirse a la federación de pods** y proporciona el nombre del host o la dirección IP de una instancia del servidor de conexión del Pod Oriental 1.

   El Pod Central 1 ya está conectado a la federación de pods.

2 Para conectar Pod Central 2, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión de Pod Central 2, selecciona **Configuración de View > Arquitectura Cloud Pod**, hace clic en **Unirse a la federación de pods** y proporciona el nombre del host o la dirección IP de una instancia del servidor de conexión del Pod Oriental 1 o en el Pod Central 1.

   El Pod Central 2 ya está conectado a la federación de pods.

Tras conectar el Pod Central 1 y el Pod Central 2 a la federación, las 10 instancias del servidor de conexión de ambos pods de la región central también formarán parte de la federación.

Crear sitios en la configuración de ejemplo

El administrador de Horizon usa Horizon Administrator para crear un sitio para los centros de datos central y oriental, y para agregar pods a esos sitios.

1 El administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 Para crear un sitio del centro de datos oriental, el administrador de Horizon debe seleccionar **Configuración de View > Sitios** y hacer clic en **Agregar**.

3 Para crear un sitio del centro de datos central, el administrador de Horizon debe seleccionar **Configuración de View > Sitios** y hacer clic en **Agregar**.

4 Para mover el Pod Oriental 1 al sitio del centro de datos oriental, el administrador de Horizon debe seleccionar **Configuración de View > Sitios**, seleccionar el sitio que contiene el Pod Oriental 1 en ese momento, seleccionar dicho pod, hacer clic en **Editar** y seleccionar el sitio del centro de datos oriental en el menú desplegable **Sitio**.

5 Para mover el Pod Central 1 al sitio del centro de datos oriental, el administrador de Horizon debe seleccionar **Configuración de View > Sitios**, seleccionar el sitio que contiene el Pod Central 1 en ese momento, seleccionar dicho pod, hacer clic en **Editar** y seleccionar el sitio del centro de datos central en el menú desplegable **Sitio**.

6 Para mover el Pod Central 2 al sitio del centro de datos oriental, el administrador de Horizon debe seleccionar **Configuración de View > Sitios**, seleccionar el sitio que contiene el Pod Central 2 en ese momento, seleccionar dicho pod, hacer clic en **Editar** y seleccionar el sitio del centro de datos central en el menú desplegable **Sitio**.

La topología del sitio de la federación de pods mostrará ahora la distribución geográfica de los pods de la red de la empresa aseguradora.

Crear autorizaciones de escritorios globales en la configuración de ejemplo

El administrador de Horizon usa Horizon Administrator para crear una única autorización de escritorios global que autorice a todos los agentes de ventas para que puedan utilizar todos los escritorios del grupo de escritorios de agentes de ventas en todas las federaciones de pods.

1 Para crear y agregar usuarios a la autorización de escritorios global, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Administrator de un servidor de conexión de la federación de pods, selecciona **Catálogo > Autorizaciones globales**, hace clic en **Agregar** y selecciona **Autorización de escritorio**.

   El administrador de Horizon agrega el grupo de agentes de ventas a la autorización de escritorios global. Este grupo se define en Active Directory y contiene todos los usuarios agentes de ventas. Si agrega el grupo de agentes de ventas a la autorización de escritorios global de agentes de ventas, los agentes podrán acceder a los grupos de escritorios Ventas A y Ventas B en los pods de las regiones central y oriental.

2 Para agregar grupos de escritorios del Pod Oriental 1 a la autorización de escritorios global, el administrador de Horizon debe iniciar sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión en el Pod Oriental 1, seleccionar **Catálogo > Autorizaciones globales**, hacer doble clic en la autorización de escritorios global, hacer clic en **Agregar** en la pestaña **Grupos locales**, seleccionar los grupos de escritorios que desea agregar y hacer clic en **Agregar**.

3 Para agregar grupos de escritorios del Pod Central 1 a la autorización de escritorios global, el administrador de Horizon debe iniciar sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión en el Pod Central 1, seleccionar **Catálogo > Autorizaciones globales**, hacer doble clic en la autorización de escritorios global, hacer clic en **Agregar** en la pestaña **Grupos locales**, seleccionar los grupos de escritorios que desea agregar y hacer clic en **Agregar**.

4 Para agregar grupos de escritorios del Pod Central 2 a la autorización de escritorios global, el administrador de Horizon debe iniciar sesión en la interfaz de usuario de Horizon Administrator de una instancia del servidor de conexión en el Pod Central 2, seleccionar **Catálogo > Autorizaciones globales**, hacer doble clic en la autorización de escritorios global, hacer clic en **Agregar** en la pestaña **Grupos locales**, seleccionar los grupos de escritorios que desea agregar y hacer clic en **Agregar**.

Crear una URL para la configuración de ejemplo

La empresa aseguradora usa una URL única y emplea un servicio DNS para resolver ventas.ejemplo en el pod del centro de datos más cercano. Con esta organización, los agentes de ventas no necesitan recordar distintas URL para cada pod y se dirigen siempre al centro de datos más cercano, sin tener en cuenta dónde se encuentran.

Cuando un agente de ventas se conecta a la URL de Horizon Client, la autorización global de los agentes de ventas aparece en la lista de grupos de escritorios disponibles. Cuando un agente de ventas selecciona una autorización de escritorios global, la función Arquitectura de Cloud Pod envía el escritorio disponible más cercano de la federación de pods. Si se utilizan todos los escritorios del centro de datos local, la función Arquitectura de Cloud Pod selecciona un escritorio de otro centro de datos. Si un agente de ventas deja una sesión de escritorio iniciada, la función Arquitectura de Cloud Pod hace que dicho agente vuelva a ese escritorio, aunque se traslade a otra región.

Administrar un entorno de Arquitectura de Cloud Pod 4

Use Horizon Administrator y el comando `lmvutil` para ver, modificar y mantener el entorno de Arquitectura de Cloud Pod. También puede usar Horizon Administrator para supervisar el estado de los pods de la federación.

Este capítulo cubre los siguientes temas:

Ver una configuración de Arquitectura de Cloud Pod

Puede usar Horizon Administrator o el comando `lmvutil` para ver la información sobre las autorizaciones globales, los pods, los sitios y los sitios principales.

Este procedimiento muestra cómo usar Horizon Administrator para ver la información sobre las autorizaciones globales, los pods, los sitios y los sitios principales. Para usar el comando `lmvutil` para ver esta información, consulte Capítulo 5, "Referencia del comando lmvutil," página 45.

Este procedimiento muestra cómo usar el comando `lmvutil` para ver una lista de las etiquetas asociadas a una autorización global. Horizon Administrator no muestra las etiquetas asociadas a una autorización global.

Procedimiento

- Para ver una lista de todas las autorizaciones globales de la configuración, en Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.

  Puede usar la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

- Para ver una lista de los grupos de aplicaciones o de escritorios de una autorización global, en Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**, haga doble clic en el nombre de la autorización global y haga clic en la pestaña **Grupos locales**.

  Solo aparecen los grupos del pod local en la pestaña **Grupos locales**. Si una autorización global incluye grupos de aplicaciones o de escritorios en un pod remoto, debe iniciar sesión en la interfaz de usuario de Horizon Administrator de la instancia del servidor de conexión en el pod remoto para ver dichos grupos.

- Para ver una lista de los grupos o los usuarios asociados a una autorización global, en Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**, haga doble clic en la autorización global y haga clic en la pestaña **Usuarios y grupos**.

  Puede usar la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

- Si desea consultar las autorizaciones globales que se asignan a un usuario específico, utilice Horizon Help Desk Tool. Horizon Help Desk Tool es una aplicación web que puede utilizar para obtener el estado de las sesiones de usuario de Horizon 7 y para realizar operaciones de mantenimiento y de solución de problemas.

  Para obtener más información, consulte el documento *Administración de View*.

- Para ver una lista de los pods de la federación, en Horizon Administrator, seleccione **Configuración de View > Arquitectura Cloud Pod**.

  Puede usar la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

- Para ver una lista de los sitios de la federación, en Horizon Administrator, seleccione **Configuración de View > Sitios**.

  Puede usar la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

- Para ver una lista de sitios principales de un usuario según la autorización global, siga estos pasos en Horizon Administrator.

  a Seleccione **Usuarios y grupos**, haga clic en la pestaña **Sitio principal** y seleccione **Resolución**.

  b Haga clic en el cuadro de texto **Haga clic aquí para buscar el usuario**.

  c Seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los usuarios de Active Directory según sus criterios de búsqueda.

  d Seleccione el usuario de Active Directory y haga clic en **Aceptar**.

  e Haga clic en **Buscar** para mostrar los sitios principales del usuario.

  El nombre de la autorización global aparece en la columna Autorización y se muestra el sitio principal efectivo de la autorización global en la columna Resolución del sitio principal. El origen de una asignación de sitio principal aparece entre paréntesis después del nombre del sitio principal. Si un usuario tiene varios sitios principales, un icono de carpeta aparece junto al nombre de la autorización global. Puede expandir esta carpeta para que muestre las asignaciones de los sitios principales que no tienen efecto en la autorización global.

- Para mostrar las etiquetas que están asociadas a una autorización global, seleccione **Catálogo > Autorizaciones globales**, haga doble clic en la autorización global y, a continuación, en la pestaña **Resumen**.

  Las etiquetas asociadas a la autorización global aparecen en el campo **Restricciones del servidor de conexión**.

Ver el estado de la federación de pods en Horizon Administrator

Horizon supervisa constantemente el estado de la federación de pods comprobando el estado de cada pod y de las instancias del servidor de conexión en dichos pods. Puede ver el estado de una federación de pods en Horizon Administrator.

También puede ver el estado de una federación de pods desde la línea de comandos utilizando el comando `vdmadmin` con la opción `–H`. Para obtener más información sobre la sintaxis de `vdmadmin`, consulte el documento *Administración de View*.

IMPORTANTE: Las bases de datos de los eventos de Horizon no se comparten a través de los pods de una federación.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Inventario > Panel**.

La sección Pods remotos del panel Estado del sistema muestra todos los pods, las instancias del servidor de conexión que son miembros y el estado conocido de cada instancia de dicho servidor de conexión.

Un icono de estado verde indica que el servidor de conexión está conectado y disponible para la función Arquitectura de Cloud Pod. Un icono de estado rojo indica que la instancia del servidor de conexión está sin conexión o que la función Arquitectura de Cloud Pod no se puede conectar a la instancia del servidor de conexión para confirmar su disponibilidad.

Ver sesiones de aplicaciones y escritorios de la federación de pods

Puede usar Horizon Administrator para buscar y ver las sesiones de los escritorios y de las aplicaciones de la federación de pods.

Puede buscar sesiones de aplicaciones y escritorios por usuario, pods o pods de brokering. El usuario es el usuario final que está conectado al escritorio o a la aplicación, el pod es en el que están alojados el escritorio o la aplicación y el pod de brokering es al que el usuario se conectó cuando la aplicación o el escritorio se asignaron por primera vez.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Inventario > Buscar sesiones**.

3 Seleccione los criterios e inicie la búsqueda.

Opción	Acción
Buscar por usuario	a Seleccione **Usuario** en el menú desplegable. b Haga clic en el cuadro de texto. c Seleccione los criterios de búsqueda en el cuadro de diálogo Buscar usuario y haga clic en **Aceptar**. d Haga clic en **Buscar** para comenzar la búsqueda.
Buscar por pod	a Seleccione **Pod** en el menú desplegable y seleccione un pod de la lista de pods que aparece. b Haga clic en **Buscar** para comenzar la búsqueda.
Buscar por pods de brokering	a Seleccione **Pod de brokering** en el menú desplegable y seleccione un pod de la lista de pods que aparece. b Haga clic en **Buscar** para comenzar la búsqueda.

Los resultados de la búsqueda incluyen los valores del usuario, del tipo de sesión (escritorio o aplicación), del equipo, del grupo o de la granja, del pod, del ID del pod de brokering, del sitio y de la autorización global asociados con cada sesión. La hora de inicio de sesión, la duración y el estado también aparece en los resultados.

NOTA: El ID del pod de brokering de las sesiones nuevas no se rellena inmediatamente en los resultados de búsqueda. Este ID suele aparecer en Horizon Administrator entre dos y tres minutos después del inicio de una sesión.

Agregar un pod a un sitio

Horizon Administrator permite agregar un pod a un sitio ya existente.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Configuración de View > Sitios**.

3 Seleccione el sitio que contiene el pod que desea agregar.

Los nombres de los pods del sitio aparecen en el panel inferior.

4 Seleccione el pod que desea agregar al sitio y haga clic en **Editar**.

5 Seleccione el sitio en cuestión en el menú desplegable **Sitio** y haga clic en **Aceptar**.

Modificar autorizaciones globales

Puede agregar y eliminar grupos, usuarios y grupos de autorizaciones globales. También puede eliminar autorizaciones globales y modificar sus atributos y directivas.

Para obtener información sobre cómo agregar un grupo a una autorización global, consulte "Agregar un grupo a una autorización global," página 25.

Eliminar un grupo de una autorización global

Puede usar Horizon Administrator para eliminar un grupo de una autorización global.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión del pod que contengan el grupo que desea eliminar.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.

3 En la pestaña **Grupos locales**, seleccione el grupo que desea eliminar de la autorización global y haga clic en **Eliminar**.

Agregar un grupo o un usuario a una autorización global

Horizon Administrator permite agregar un usuario o un grupo a una autorización global existente.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales** y haga doble clic en la autorización global.

3 En la pestaña **Usuarios y grupos**, haga clic en **Agregar**.

4 Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos o los usuarios de Active Directory según sus criterios de búsqueda.

Puede seleccionar la casilla de verificación **Usuarios sin autenticar** para buscar y agregar usuarios con acceso sin autenticar a las autorizaciones de aplicaciones globales. No puede agregar usuarios con acceso sin autenticar a las autorizaciones de escritorios globales. Si intenta agregar un usuario con acceso sin autenticar a una autorización de escritorios global, Horizon Administrator devuelve un mensaje de error.

5 Seleccione el grupo o el usuario de Active Directory que desea agregar a la autorización global y haga clic en **Aceptar**.

Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.

Eliminar un grupo o un usuario de una autorización global

Puede usar Horizon Administrator para eliminar un usuario o un grupo de una autorización global.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales** y haga doble clic en la autorización global.

3 En la pestaña Usuarios y grupos, seleccione el usuario o el grupo que desee eliminar y haga clic en **Eliminar**.

Puede pulsar Ctrl y Mayús para seleccionar varios grupos y usuarios.

4 Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

Modificar atributos o directivas de una autorización global

Puede usar Horizon Administrator para modificar el nombre, la descripción, los atributos, las etiquetas, los ámbitos y otras directivas de una autorización global.

No puede modificar el tipo de grupo de escritorios que una autorización de escritorios global puede incluir.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.

3 Seleccione la autorización global y haga clic en **Editar**.

4 Para modificar el nombre o la descripción de la autorización global, escriba un nuevo nombre o una nueva descripción en los cuadros de texto **Nombre** o **Descripción** en el panel General.

El nombre puede tener entre 1 y 64 caracteres. La descripción puede tener entre 1 y 1024 caracteres.

5 Para eliminar o modificar las etiquetas que estén asociadas a la autorización global, haga clic en **Examinar**.

Puede seleccionar **Sin restricciones** para eliminar todas las etiquetas existentes, o bien puede seleccionar **Elemento restringido a estas etiquetas** para asociar la autorización global a otras etiquetas. Solo las instancias del servidor de conexión que tengan las etiquetas seleccionadas pueden acceder a la autorización global.

NOTA: Solo puede seleccionar las etiquetas asignadas a las instancias del servidor de conexión en el pod local. Para seleccionar las etiquetas asignadas a las instancias del servidor de conexión de otro pod, debe iniciar sesión en el Horizon Administrator que se encuentra en una instancia del servidor de conexión del otro pod y volver modificar la autorización global.

6 Para modificar una directiva de autorización global, selecciónela o desmárquela en el panel Directiva.

Directiva	Descripción
Ámbito	Especifica dónde buscar escritorios o aplicaciones que cumplan las solicitudes de aplicaciones o escritorios de la autorización global. Solo puede seleccionar una directiva de ámbito. ■ **Todos los sitios**: busca escritorios o aplicaciones en los pods de la federación. ■ **Dentro del sitio**: busca escritorios o aplicaciones únicamente en los pods del mismo sitio en el que se encuentra el pod al que el usuario está conectado. ■ **Dentro del pod**: busca escritorios o aplicaciones únicamente en el pod al que el usuario está conectado.
Utilizar sitio principal	Determina si se debe empezar a buscar escritorios o aplicaciones en el sitio principal del usuario. Si el usuario no tiene un sitio principal y la opción **El usuario autorizado debe tener sitio principal** no está seleccionada, se asume que el sitio al que el usuario está conectado en ese momento es el principal.
El usuario autorizado debe tener sitio principal	Hace que la autorización global esté disponible únicamente si el usuario tiene un sitio principal. La opción está disponible solo cuando la opción **Utilizar sitio principal** está seleccionada.
Limpiar automáticamente las sesiones redundantes	Cierra las sesiones adicionales del usuario que tienen la misma autorización. Esta opción está disponible únicamente para autorizaciones de escritorios flotantes y autorizaciones de aplicaciones. Pueden aparecer varias sesiones cuando un pod que contiene una sesión se desconecta, el usuario inicia otra sesión y el pod con el problema vuelve a conectarse con la sesión original. Cuando aparecen varias sesiones, Horizon Client solicita que el usuario seleccione una de ellas. Esta opción determina qué sucede con las sesiones que el usuario no selecciona. Si no selecciona esta opción, los usuarios deben cerrar las sesiones adicionales de forma manual. Para hacerlo, pueden cerrar sesión en Horizon Client, o bien iniciar las sesiones y cerrarlas.
Protocolo de visualización predeterminado	Especifica el protocolo de visualización predeterminado de las aplicaciones y los escritorios en la autorización global.
HTML Access	Determina si desea permitir que los usuarios utilicen la función HTML Access para acceder a escritorios o aplicaciones en la autorización global. Cuando habilita la directiva HTML Access, los usuarios finales pueden usar un navegador web para conectarse a escritorios remotos y no es necesario instalar ningún software cliente en los sistemas locales.

Directiva	Descripción
Permitir que los usuarios inicien sesiones independientes desde dispositivos cliente diferentes	Determina si se permite que los usuarios inicien sesiones de escritorios independientes desde dispositivos cliente diferentes. Cuando habilite la directiva de varias sesiones por usuario, los usuarios que se conectan a la autorización global desde dispositivos cliente diferentes reciben sesiones de escritorios diferentes. Para volver a conectarse a una sesión de escritorios existente, los usuarios deben usar el mismo dispositivo desde el que se inició la sesión. Si no habilita esta directiva, los usuarios siempre se volverán a conectar a las sesiones de escritorios existentes, independientemente del dispositivo cliente que usen. Solo puede habilitar esta directiva para las autorizaciones de escritorios flotantes. **NOTA:** Si habilita esta directiva, todos los grupos de escritorios de la autorización global también deben admitir varias sesiones por usuario.
Preinicio	Determina si debe iniciar la sesión de aplicación antes de que un usuario abra la autorización de aplicaciones global en Horizon Client. Cuando habilite la directiva de preinicio, los usuarios pueden iniciar la autorización global de aplicaciones con mayor rapidez. **NOTA:** Si habilita esta directiva, todos los grupos de aplicaciones de la autorización de aplicaciones global también deben ser compatibles con la función de preinicio de sesiones y, a su vez, el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.

7 Para modificar la ruta de la aplicación, la versión y la información del editor de una autorización de aplicaciones global, escriba los valores en los cuadros de texto de la aplicación.

NOTA: Si agrega un grupo de aplicaciones a la autorización de aplicaciones global después de modificar estos valores, los valores del grupo de aplicaciones sobrescriben estos valores.

8 Haga clic en **Aceptar** para guardar los cambios.

Eliminar una autorización global

Horizon Administrator permite eliminar de forma permanente una autorización global. Cuando elimina una autorización global, todos los usuarios que dependen de dicha autorización de escritorios global no pueden acceder a ellos. Las sesiones de los escritorios existentes permanecen conectadas.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.

3 Haga clic en la autorización global que desea eliminar y, a continuación en **Eliminar**.

4 Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

Administrar las asignaciones de sitios principales

Puede modificar y eliminar asignaciones de sitios principales. También puede visualizar el sitio principal efectivo de cada autorización global a la que pertenece un usuario.

Modificar una asignación de sitio principal

Puede cambiar una asignación de sitio principal existente de un grupo o un usuario específicos.

Para modificar la asociación entre una autorización global y un sitio principal de un grupo o un usuario específicos, consulte "Modificar un sitio principal de reemplazo," página 43.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Usuarios y grupos** y haga clic en la pestaña **Sitio principal** y seleccione **Asignación**.

3 Seleccione la asignación del sitio principal que desee modificar y haga clic en **Editar**.

4 Seleccione otro sitio principal en el menú desplegable **Sitio principal**.

5 Haga clic en **Aceptar** para guardar la nueva asignación.

Eliminar una asignación de sitio principal

Puede eliminar la asociación entre un grupo de usuarios y un sitio principal.

Para eliminar la asociación entre una autorización global y un sitio principal de un grupo o un usuario específicos, consulte "Eliminar un sitio principal de reemplazo," página 43.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Usuarios y grupos** y haga clic en la pestaña **Sitio principal** y seleccione **Asignación**.

3 Seleccione la asignación del sitio principal que desee eliminar y haga clic en **Eliminar**.

4 Haga clic en **Aceptar** para eliminarla.

Determinar el sitio principal efectivo de un usuario

Dado que puede asignar sitios principales tanto a usuarios como a grupos, un único usuario puede tener varios sitios principales. Además, los sitios principales asociados con las autorizaciones globales pueden sobrescribir el sitio principal de un usuario. Horizon Administrator permite determinar el sitio principal efectivo de un usuario.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.

2 En Horizon Administrator, seleccione **Usuarios y grupos** y haga clic en la pestaña **Sitio principal** y seleccione **Resolución**.

3 Haga clic en el cuadro de texto **Haga clic aquí para buscar el usuario**.

4 Seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los usuarios de Active Directory según sus criterios de búsqueda.

5 Seleccione el usuario de Active Directory cuyo sitio principal efectivo desea ver y haga clic en **Aceptar**.

6 Haga clic en **Buscar**.

Horizon Administrator muestra el sitio principal efectivo de cada autorización global a la que pertenece el usuario. Solo se muestran las autorizaciones globales que tienen habilitada la directiva **Utilizar sitio principal**.

El sitio principal que está en uso aparece en la columna Resolución del sitio principal. Si un usuario tiene varios sitios principales, aparecerá un icono de carpeta junto al nombre de la autorización global en la columna Autorización. Puede expandir esta carpeta para que muestre las asignaciones de los sitios principales que no tienen efecto en la autorización global. Horizon Administrator usa un texto tachado para indicar que un sitio principal no se está utilizando.

Horizon Administrator muestra el origen de la asignación del sitio principal entre paréntesis después del nombre del sitio principal en la columna Resolución del sitio principal. Si el sitio principal se creó desde un grupo al que pertenece el usuario, Horizon Administrator muestra el mismo nombre del grupo, por ejemplo, **(a través de los usuarios del dominio)**. Si el sitio principal se creó desde la asignación del sitio principal del usuario, Horizon Administrator muestra **(Predeterminado)**. Si el sitio principal se creó desde la autorización global (un sitio principal de reemplazo), Horizon Administrator muestra **(Directo)**.

Si un usuario no cuenta con un sitio principal, Horizon Administrator muestra **No se definió ningún sitio principal** en la columna Resolución del sitio principal.

Modificar un sitio principal de reemplazo

Puede modificar la asociación entre una autorización global y un sitio principal de un grupo o un usuario específicos.

Procedimiento

1. Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.
2. En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.
3. Haga doble clic en la autorización global.
4. En la pestaña **Sitio principal de reemplazo**, seleccione un usuario o grupo y haga clic en **Editar**.
5. Seleccione otro sitio principal en el menú desplegable **Sitio principal**.
6. Haga clic en **Aceptar** para guardar los cambios.

Eliminar un sitio principal de reemplazo

Puede eliminar la asociación entre una autorización global y un sitio principal de un grupo o un usuario específicos.

Procedimiento

1. Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión de la federación de pods.
2. En Horizon Administrator, seleccione **Catálogo > Autorizaciones globales**.
3. Haga doble clic en la autorización global.
4. En la pestaña **Sitio principal de reemplazo**, seleccione un usuario o grupo y haga clic en **Eliminar**.
5. Haga clic en **Aceptar** para eliminar el sitio principal de reemplazo.

Eliminar un pod de la federación de pods

Puede usar Horizon Administrator para eliminar un pod conectado a la federación. Es posible que desee eliminar un pod de la federación si se va a utilizar para otro propósito o si no se configuró correctamente.

Para eliminar el pod más reciente de la federación, anule la inicialización de la función de Arquitectura de Cloud Pod. Consulte "Anular la inicialización de la función Arquitectura Cloud Pod," página 44.

IMPORTANTE: No detenga ni inicie una instancia de servidor de conexión mientras se elimina de una federación de pods. Es posible que el servicio del servidor de conexión no se reinicie correctamente.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de cualquier instancia del servidor de conexión del pod que desea eliminar de la federación de pods.

2 En Horizon Administrator, seleccione **Arquitectura Cloud Pod** y haga clic en **Separarse** en el panel Federación de pods.

3 Haga clic en **Aceptar** para iniciar la operación de separación.

Horizon Administrator muestra el curso de la operación de separación.

4 Cuando Horizon Administrator le solicite que vuelva a cargar el cliente, haga clic en **Aceptar**.

Después de actualizar la interfaz de usuario de Horizon Administrator, la opción **Autorizaciones globales** ya no aparece en la sección **Catálogo**, y **Sitios** tampoco aparece en la sección **Configuración de View** del panel del inventario de Horizon Administrator.

Anular la inicialización de la función Arquitectura Cloud Pod

Puede usar Horizon Administrator para anular la inicialización de la función Arquitectura de Cloud Pod.

Prerequisitos

Es necesario que anule la inicialización de la función Arquitectura de Cloud Pod únicamente en un pod de la federación de pods. Si la federación de pods contiene varios pods, debe desconectar los otros pods antes de comenzar el proceso para anular la inicialización. Consulte "Eliminar un pod de la federación de pods," página 44.

Procedimiento

1 Inicie sesión en la interfaz de usuario de Horizon Administrator de todas las instancias del servidor de conexión del pod.

2 En Horizon Administrator, seleccione **Configuración de View > Arquitectura Cloud Pod**.

3 En al panel Federación de pods, haga clic en **Desinicializar**.

4 Haga clic en **Aceptar** para iniciar el proceso.

Después de que finalice el proceso, se elimina toda la configuración de Arquitectura de Cloud Pod, incluidos los sitios, los sitios principales y las autorizaciones globales.

5 Cuando Horizon Administrator le solicite que vuelva a cargar el cliente, haga clic en **Aceptar**.

Después de actualizar la interfaz de usuario de Horizon Administrator, la opción **Autorizaciones globales** ya no aparece en la sección **Catálogo**, y **Sitios** tampoco aparece en la sección **Configuración de View** del panel del inventario de Horizon Administrator.

Referencia del comando lmvutil 5

La interfaz de la línea de comando `lmvutil` permite configurar y administrar una implementación de Arquitectura de Cloud Pod.

NOTA: La interfaz de la línea de comando `vdmutil` permite realizar las mismas operaciones que `lmvutil`.

Este capítulo cubre los siguientes temas:

Uso del comando lmvutil

La sintaxis de los comandos de `lmvutil` controla su funcionamiento.

Use el siguiente formato del comando de `lmvutil` en una ventana de símbolo de sistema de Windows.

`lmvutil` *`opción_comando`* [*`argumento opción_adicional`*] ...

De forma alternativa, puede usar el comando `vdmutil` para realizar las mismas operaciones que el comando `lmvutil`. Use el siguiente formato del comando de `vdmutil` en una ventana de símbolo de sistema de Windows.

`vdmutil` *`opción_comando`* [*`argumento opción_adicional`*] ...

Las opciones adicionales que puede usar dependen de la opción del comando.

De forma predeterminada, la ruta de los archivos ejecutables de los comandos `lmvutil` y `vdmutil` es `C:\Program Files\VMware\VMware View\Server\tools\bin`. Si desea evitar introducir la ruta en la línea de comando, agréguela a la variable de entorno PATH.

Autenticación del comando lmvutil

Si desea usar el comando `lmvutil` para configurar y administrar un entorno de Arquitectura de Cloud Pod, debe ejecutarlo como un usuario con función de administradores.

Horizon Administrator permite asignar la función de administradores a un usuario. Consulte el documento *Administración de View*.

El comando `lmvutil` incluye opciones para especificar el nombre de usuario, el dominio y la contraseña que se deben usar en la autenticación.

Tabla 5-1. Opciones de autenticación del comando lmvutil

Opción	Descripción
`--authAs`	Nombre de un usuario administrador de Horizon. No use *dominio\nombredeusuario* ni el formato de nombre principal de usuario (UPN).
`--authDomain`	Nombre de dominio completo del usuario administrador de Horizon especificado en la opción `--authAs`.
`--authPassword`	Contraseña del usuario administrador de Horizon especificado en la opción `--authAs`. Si introduce **"*"** en lugar de una contraseña, el comando `lmvutil` solicitará la contraseña y no permitirá contraseñas que distingan entre mayúsculas y minúsculas en el historial de la línea de comandos.

Por ejemplo, el siguiente comando `lmvutil` inicia la sesión del usuario domainEast\adminEast e inicializa la función Arquitectura de Cloud Pod.

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

Debe usar las opciones de autenticación con todas las opciones del comando `lmvutil` excepto con `--help` y con `--verbose`.

Salidas del comando lmvutil

El comando `lmvutil` devuelve 0 cuando una operación se realiza correctamente y un código que no es cero específico de errores cuando una operación no se realiza correctamente.

El comando `lmvutil` escribe mensajes de error de los errores estándar. Cuando una operación genera una salida o cuando el registro detallado está habilitado con la opción `--verbose`, el comando `lmvutil` escribe la salida estándar.

El comando `lmvutil` solo escribe las salidas en inglés (Estados Unidos).

Opciones del comando lmvutil

Las opciones del comando `lmvutil` permiten especificar la operación que desea realizar. Todas las opciones aparecen precedidas de dos guiones (--).

Para las opciones de autenticación del comando `lmvutil`, consulte "Autenticación del comando lmvutil," página 46.

Tabla 5-2. Opciones del comando lmvutil

Opción	Descripción
`--activatePendingCertificate`	Activa un certificado SSL pendiente. Consulte "Activar un certificado pendiente," página 70.
`--addGroupEntitlement`	Asocia un grupo de usuarios con una autorización global. Consulte "Agregar un grupo o un usuario a una autorización global," página 61.

Tabla 5-2. Opciones del comando lmvutil (Continua)

Opción	Descripción
`--addPoolAssociation`	Asocia un grupo de escritorios con una autorización de escritorios global o un grupo de aplicaciones con una autorización de aplicaciones global. Consulte "Agregar un grupo a una autorización global," página 60.
`--addUserEntitlement`	Asocia un usuario con una autorización global. Consulte "Agregar un grupo o un usuario a una autorización global," página 61
`--assignPodToSite`	Asigna un pod a un sitio. Consulte "Asignar un pod a un sitio," página 52.
`--createGlobalApplicationEntitlement`	Crea una autorización de aplicaciones global. Consulte "Crear una autorización global," página 55.
`--createGlobalEntitlement`	Crea una autorización de escritorios global. Consulte "Crear una autorización global," página 55.
`--createSite`	Crear un sitio. Consulte "Crear un sitio," página 52.
`--createGroupHomeSite`	Asocia un grupo de usuarios con un sitio principal. Consulte "Configurar un sitio principal," página 63.
`--createPendingCertificate`	Crea un certificado SSL pendiente. Consulte "Crear un certificado pendiente," página 70.
`--createUserHomeSite`	Asocia un usuario con un sitio principal. Consulte "Configurar un sitio principal," página 63.
`--deleteGlobalApplicationEntitlement`	Elimina una autorización de aplicaciones global. Consulte "Eliminar una autorización global," página 60.
`--deleteGlobalEntitlement`	Elimina una autorización de escritorios global. Consulte "Eliminar una autorización global," página 60.
`--deleteSite`	Elimina un sitio. Consulte "Eliminar un sitio," página 54.
`--deleteGroupHomeSite`	Elimina la asociación entre un grupo de usuarios y un sitio principal. Consulte "Eliminar un sitio principal," página 64.
`--deleteUserHomeSite`	Elimina la asociación entre un usuario y un sitio principal. Consulte "Eliminar un sitio principal," página 64.
`--editSite`	Modifica el nombre o la descripción de un sitio. Consulte "Cambiar el nombre o la descripción de un sitio," página 53.
`--ejectPod`	Elimina un pod que no se encuentra disponible de una federación. Consulte "Eliminar un pod de una federación de pods," página 50.
`--help`	Especifica las opciones del comando `lmvutil`.
`--initialize`	Inicia la función Arquitectura de Cloud Pod. Consulte "Inicializar la función Arquitectura de Cloud Pod," página 49.
`--join`	Conecta un pod a una federación de pods. Consulte "Conectar un pod a la federación de pods," página 50.
`--listAssociatedPools`	Especifica los grupos de escritorios que están asociados a una autorización de escritorios global o de los grupos de aplicaciones que están asociadas a una autorización de aplicaciones global. Consulte "Lista de grupos de una autorización global," página 66.
`--listEntitlements`	Especifica las asociaciones entre los usuarios o los grupos de usuarios y las autorizaciones globales. "Lista de grupos o usuarios de una autorización global," página 66

Tabla 5-2. Opciones del comando lmvutil (Continua)

Opción	Descripción
`--listGlobalApplicationEntitlements`	Especifica todas las autorizaciones de aplicaciones globales. Consulte "Lista de autorizaciones globales," página 66.
`--listGlobalEntitlements`	Especifica todas las autorizaciones de escritorios globales. Consulte "Lista de autorizaciones globales," página 66.
`--listPods`	Especifica los pods en una topología de Arquitectura de Cloud Pod. Consulte "Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod," página 69.
`--listSites`	Especifica los sitios en una topología de Arquitectura de Cloud Pod. Consulte "Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod," página 69.
`--listUserAssignments`	Especifica las asignaciones de pods de escritorios dedicados de un usuario y una combinación de autorizaciones globales. Consulte "Listados de asignaciones de grupos de escritorios dedicados," página 68.
`--removePoolAssociation`	Elimina la asociación entre un grupo de escritorios y una autorización global. Consulte "Eliminar un grupo de una autorización global," página 61.
`--resolveUserHomeSite`	Muestra el sitio principal efectivo de un usuario. Consulte "Especificar el sitio principal efectivo de un usuario," página 68.
`--removeGroupEntitlement`	Elimina un grupo de usuarios de una autorización global. Consulte "Eliminar un grupo o un usuario de una autorización global," página 62.
`--removeUserEntitlement`	Elimina un usuario de una autorización global. Consulte "Eliminar un grupo o un usuario de una autorización global," página 62.
`--showGroupHomeSites`	Muestra todos los sitios principales de un grupo. Consulte "Lista de los sitios principales de un usuario o grupo," página 67.
`--showUserHomeSites`	Muestra todos los sitios principales de un usuario. Consulte "Lista de los sitios principales de un usuario o grupo," página 67.
`--uninitialize`	Deshabilita la función Arquitectura de Cloud Pod. Consulte "Deshabilitar la función Arquitectura de Cloud Pod," página 49.
`--unjoin`	Elimina un pod que se encuentra disponible de una federación. Consulte "Eliminar un pod de una federación de pods," página 50.
`--updateGlobalApplicationEntitlement`	Modifica una autorización de aplicaciones global. Consulte "Modificar una autorización global," página 57.
`--updateGlobalEntitlement`	Modifica una autorización de escritorios global. Consulte "Modificar una autorización global," página 57.
`--updatePod`	Modifica el nombre o la descripción de un pod. Consulte "Cambiar el nombre o la descripción de un pod," página 51.
`--verbose`	Habilita el registro detallado. Puede agregar esta opción a cualquier otra para obtener la salida detallada del comando. El comando `lmvutil` escribe la salida estándar.

Inicializar la función Arquitectura de Cloud Pod

El comando `lmvutil` con la opción `--initialize` permite inicializar la función Arquitectura de Cloud Pod. Cuando inicie la función Arquitectura de Cloud Pod, Horizon configura el Nivel de datos global en cada instancia del servidor de conexión del pod y configura el canal de comunicación VIPA.

Sintaxis

```
lmvutil --initialize
```

Notas de uso

Ejecute este comando solo una vez en una instancia del servidor de conexión del pod. Puede ejecutar el comando en cualquier instancia del servidor de conexión del pod. No es necesario ejecutarlo con otros pods. El resto de pods se conectan al inicializado.

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod ya se inició o si el comando no puede completar la operación.

Ejemplo

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

Deshabilitar la función Arquitectura de Cloud Pod

El comando `lmvutil` con la opción `--uninitialize` permite deshabilitar la función Arquitectura de Cloud Pod.

Sintaxis

```
lmvutil --uninitialize
```

Notas de uso

Antes de ejecutar este comando, use el comando `lmvutil` con la opción `--unjoin` para eliminar todos los pods de la federación.

Ejecute este comando en una sola instancia del servidor de conexión de un pod. Puede ejecutar el comando en cualquier instancia del servidor de conexión del pod. Si la federación de pods contiene varios pods, es necesario ejecutar este comando únicamente en un pod.

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició, si el comando no encuentra el pod o si la federación de pods contiene otros pods.

Ejemplo

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

Administrar federaciones de pods

El comando `lmvutil` proporciona opciones para configurar y modificar las federaciones de pods.

- Conectar un pod a la federación de pods página 50

  El comando `lmvutil` con la opción `--join` permite conectar un pod a la federación.

Conectar un pod a la federación de pods

El comando `lmvutil` con la opción `--join` permite conectar un pod a la federación.

Sintaxis

`lmvutil --join joinServer` *`direcciónde servidor`* `--userName` *`dominio\nombredeusuario`* `--password` *`contraseña`*

Notas de uso

Debe ejecutar este comando en cada pod que desee unir a la federación de pods. Puede ejecutar el comando en cualquier instancia del servidor de conexión de un pod.

Este comando devuelve un mensaje de error si proporciona credenciales no válidas, si las instancias del servidor de conexión no existen, si una federación no existe en el servidor especificado o si el comando no puede completar la operación.

Opciones

Debe especificar varias opciones cuando conecte un pod a una federación.

Tabla 5-3. Opciones de conexión de un pod a una federación

Opción	Descripción
`--joinServer`	Nombre DNS o dirección IP de una instancia del servidor de conexión de cualquier pod inicializado o que ya sea parte de la federación de pods.
`--userName`	Nombre de un usuario administrador de Horizon en el pod ya iniciado. Use el formato *dominio\nombredeusuario*.
`--password`	Contraseña del usuario especificado en la opción `--userName`.

Ejemplo

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

Eliminar un pod de una federación de pods

Use el comando `lmvutil` con la opción `--unjoin` o la opción `--ejectPod` para eliminar un pod de la federación.

Sintaxis

```
lmvutil --unjoin
```

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

Notas de uso

Para eliminar un pod de una federación de pods, use la opción `--unjoin`. Puede ejecutar el comando en cualquier instancia del servidor de conexión del pod.

Para eliminar un pod que no está disponible de una federación de pods, use la opción `--ejectPod`. Por ejemplo, un pod puede dejar de estar disponible si se produce un error de hardware. Puede realizar esta operación en cualquier pod de la federación de pods.

IMPORTANTE: En la mayoría de casos, debe usar la opción `--unjoin` para eliminar un pod de la federación.

Estos comandos devuelven un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó, si el pod no está conectado a una federación o si el comando no puede realizar las operaciones especificadas.

Opciones

Cuando use la opción `--ejectPod`, utilice `--pod` para identificar el pod que desea eliminar de la federación.

Ejemplo

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

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

Cambiar el nombre o la descripción de un pod

El comando `lmvutil` con la opción `--updatePod` permite actualizar o modificar el nombre o la descripción de un pod.

Sintaxis

```
lmvutil --updatePod --podName nombredepod [--newPodName nombredepod] [--description texto]
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició o si el comando no puede encontrar ni actualizar el pod.

Opciones

Puede especificar estas opciones cuando actualice un nombre o una descripción de pod.

Tabla 5-4. Opciones para cambiar el nombre o la descripción de pod

Opción	Descripción
`--podName`	Nombre de pod que desea actualizar.
`--newPodName`	(Opcional) Nombre nuevo del pod. Un nombre de pod puede tener entre 1 y 64 caracteres.
`--description`	(Opcional) Descripción del sitio. La descripción puede tener entre 1 y 1024 caracteres.

Ejemplo

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

Administrar sitios

Puede usar las opciones del comando `lmvutil` para crear, modificar y eliminar sitios de Arquitectura de Cloud Pod. Un sitio es un grupo de pods.

- Crear un sitio página 52

  El comando `lmvutil` con la opción `--createSite` permite crear un sitio en una topología de Arquitectura de Cloud Pod.

- Asignar un pod a un sitio página 52

  El comando `lmvutil` con la opción `--assignPodToSite` permite asignar un pod a un sitio.

- Cambiar el nombre o la descripción de un sitio página 53

  El comando `lmvutil` con la opción `--editSite` permite editar el nombre o la descripción de un sitio.

- Eliminar un sitio página 54

  El comando `lmvutil` con la opción `--deleteSite` permite eliminar un sitio.

Crear un sitio

El comando `lmvutil` con la opción `--createSite` permite crear un sitio en una topología de Arquitectura de Cloud Pod.

Sintaxis

```
lmvutil --createSite --siteName nombredelsitio [--description texto]
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició, si el sitio especificado ya existe o si el comando no puede crear el certificado.

Opciones

Puede especificar estas opciones cuando crea un sitio.

Tabla 5-5. Opciones para crear un sitio

Opción	Descripción
`--siteName`	Nombre del sitio nuevo. Un nombre de sitio puede tener entre 1 y 64 caracteres.
`--description`	(Opcional) Descripción del sitio. La descripción puede tener entre 1 y 1024 caracteres.

Ejemplo

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

Asignar un pod a un sitio

El comando `lmvutil` con la opción `--assignPodToSite` permite asignar un pod a un sitio.

Sintaxis

```
lmvutil --assignPodToSite --podName nombredelpod --siteName nombredelsitio
```

Notas de uso

Antes de asignar un pod a un sitio, debe crear el sitio. Consulte "Crear un sitio," página 52.

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició, si el comando no encuentra el sitio o el pod especificados o si el comando no puede asignar el pod al sitio.

Opciones

Cuando asigne un pod a un sitio, debe especificar estas opciones.

Tabla 5-6. Opciones para asignar un pod a un sitio

Opción	Descripción
`--podName`	Nombre del pod que desea asignar al sitio.
`--siteName`	Nombre del sitio.

El comando `lmvutil` con la opción `--listPods` permite enumerar los nombres de los pods siguiendo una topología de Arquitectura de Cloud Pod. Consulte "Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod," página 69.

Ejemplo

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

Cambiar el nombre o la descripción de un sitio

El comando `lmvutil` con la opción `--editSite` permite editar el nombre o la descripción de un sitio.

Sintaxis

```
lmvutil --editSite --siteName nombredelsitio [--newSiteName nombredelsitio] [--description texto]
```

Notas de uso

Este comando devuelve un mensaje de error si el sitio especificado no existe o si el comando no puede encontrar ni actualizar el sitio.

Opciones

Puede especificar estas opciones cuando cambie un nombre o una descripción de sitio.

Tabla 5-7. Opciones para cambiar un nombre o una descripción de sitio

Opción	Descripción
`--siteName`	Nombre del sitio que desea editar.
`--newSiteName`	(Opcional) Nombre nuevo del sitio. Un nombre de sitio puede tener entre 1 y 64 caracteres.
`--description`	(Opcional) Descripción del sitio. La descripción puede tener entre 1 y 1024 caracteres.

Ejemplo

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

Eliminar un sitio

El comando `lmvutil` con la opción `--deleteSite` permite eliminar un sitio.

Sintaxis

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

Notas de uso

Este comando devuelve un mensaje de error si el sitio especificado no existe o si el comando no puede encontrar ni eliminar el sitio.

Opciones

La opción `--sitename` permite especificar el nombre del sitio que desea eliminar.

Ejemplo

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

Administrar las autorizaciones globales

Puede usar las opciones del comando `lmvutil` para crear, modificar y hacer una lista de las autorizaciones de escritorios globales y las autorizaciones de aplicaciones globales de un entorno de Arquitectura de Cloud Pod.

- Crear una autorización global página 55

  Para crear una autorización de escritorios global, use el comando `lmvutil` con la opción `--createGlobalEntitlement`. Para crear una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--createGlobalApplicationEntitlement`.

- Modificar una autorización global página 57

  Para modificar una autorización de escritorios global, use el comando `lmvutil` con la opción `--updateGlobalEntitlement`. Para modificar una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--updateGlobalApplicationEntitlement`.

- Eliminar una autorización global página 60

  Para eliminar una autorización de escritorios global, use el comando `lmvutil` con la opción `--deleteGlobalEntitlement`. Para eliminar una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--deleteGlobalApplicationEntitlement`.

- Agregar un grupo a una autorización global página 60

  El comando `lmvutil` con la opción `--addPoolAssociation` permite agregar un grupo de escritorios a una autorización de escritorios global, o bien un grupo de aplicaciones a una autorización de aplicaciones global.

- Eliminar un grupo de una autorización global página 61

  El comando `lmvutil` con la opción `--removePoolAssociation` permite eliminar un grupo de escritorios de una autorización de escritorios global, o bien un grupo de aplicaciones de una autorización de aplicaciones global.

- Agregar un grupo o un usuario a una autorización global página 61

  Para agregar un usuario a una autorización global, use el comando `lmvutil` con la opción `--addUserEntitlement`. Para agregar un grupo a una autorización global, use el comando `lmvutil` con la opción `--addGroupEntitlement`.

- Eliminar un grupo o un usuario de una autorización global página 62

  Para eliminar un usuario de una autorización global, use el comando `lmvutil` con la opción `--removeUserEntitlement`. Para eliminar un grupo de una autorización global, use el comando `lmvutil` con la opción `--removeGroupEntitlement`.

Crear una autorización global

Para crear una autorización de escritorios global, use el comando `lmvutil` con la opción `--createGlobalEntitlement`. Para crear una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--createGlobalApplicationEntitlement`.

Las autorizaciones globales suponen un vínculo entre los usuarios y sus escritorios y aplicaciones, sin tener en cuenta cuál de esos escritorios y esas aplicaciones residen en la federación de pods. Las autorizaciones globales también incluyen directivas que determinan cómo la función Arquitectura de Cloud Pod asigna los escritorios y las aplicaciones a los usuarios autorizados.

Sintaxis

```
lmvutil --createGlobalEntitlement --entitlementName nombre --scope ámbito
{--isDedicated | --isFloating} [--description texto] [--disabled]
[--fromHome] [--multipleSessionAutoClean] [--requireHomeSite] [--defaultProtocol valor]
[--preventProtocolOverride] [--allowReset] [--htmlAccess] [--multipleSessionsPerUser]
[--tags etiquetas]
```

```
lmvutil --createGlobalApplicationEntitlement --entitlementName nombre --scope ámbito
[--description texto] [--disabled] [--fromHome] [--multipleSessionAutoClean]
[--requireHomeSite] [--defaultProtocol valor] [--preventProtocolOverride] [--htmlAccess]
[--preLaunch] [--tags etiquetas]
```

Notas de uso

Puede usar estos comandos en cualquier instancia del servidor de conexión de una federación de pods. La función Arquitectura de Cloud Pod almacena nuevos datos en el Nivel de datos global y replica dichos datos en todos los pods de la federación de pods.

Estos comandos devuelven un mensaje de error si la autorización global ya existe, el ámbito no es válido, la función Arquitectura de Cloud Pod no se inició o los comandos no pueden crear la autorización global.

Opciones

Puede especificar estas opciones cuando crea una autorización global. Algunas opciones se aplican únicamente a las autorizaciones de escritorios globales.

Tabla 5-8. Opciones para crear autorizaciones globales

Opción	Descripción
`--entitlementName`	Nombre de la autorización global. El nombre puede tener entre 1 y 64 caracteres. El nombre de la autorización global aparece en la lista de las aplicaciones y los escritorios de Horizon Client para los usuarios autorizados.
`--scope`	Ámbito de la autorización global. Los valores válidos son los siguientes: ■ CUALQUIERA. Horizon busca recursos en los pods de la federación. ■ SITIO. Horizon busca recursos únicamente en los pods del mismo sitio en el que se encuentra el pod al que el usuario está conectado. ■ LOCAL. Horizon busca recursos únicamente en el pod al que el usuario está conectado.

Tabla 5-8. Opciones para crear autorizaciones globales (Continua)

Opción	Descripción
`--isDedicated`	Crea una autorización de escritorios dedicados. Una autorización de escritorios dedicados solo puede contener grupos de escritorios dedicados. Para crear una autorización de escritorios flotantes, use la opción `--isFloating`. Una autorización de escritorios global puede ser dedicada o flotante. No puede especificar la opción `--isDedicated` con la opción `--multipleSessionAutoClean`. Se aplican únicamente a las autorizaciones de escritorios globales.
`--isFloating`	Crea una autorización de escritorio flotante. Una autorización de escritorio flotante solo puede tener grupos de escritorios flotantes. Para crear una autorización de escritorios dedicados, especifique la opción `--isDedicated`. Una autorización de escritorios global puede ser dedicada o flotante. Se aplican únicamente a las autorizaciones de escritorios globales.
`--disabled`	(Opcional) Crea la autorización global en estado deshabilitado.
`--description`	(Opcional) Descripción de la autorización global. La descripción puede tener entre 1 y 1024 caracteres.
`--fromHome`	(Opcional) Si el usuario tiene un sitio principal, Horizon empieza a buscar recursos en el sitio principal del usuario. Si el usuario no tiene un sitio principal, Horizon empieza a buscar recursos en el sitio al que el usuario está conectado en ese momento.
`--multipleSessionAutoClean`	(Opcional) Cierra las sesiones adicionales del usuario con la misma autorización. Pueden aparecer varias sesiones cuando un pod que contiene una sesión se desconecta, el usuario inicia otra sesión y el pod con el problema vuelve a conectarse con la sesión original. Cuando aparecen varias sesiones, Horizon Client solicita que el usuario seleccione una de ellas. Esta opción determina qué sucede con las sesiones que el usuario no selecciona. Si no especifica esta opción, los usuarios deben cerrar las sesiones adicionales de forma manual. Para hacerlo, pueden cerrar sesión en Horizon Client, o bien iniciar las sesiones y cerrarlas.
`--requireHomeSite`	(Opcional) Hace que la autorización global esté disponible únicamente si el usuario tiene un sitio principal. Esta opción solo se aplica cuando se especifica también la opción `--fromHome`.
`--defaultProtocol`	(Opcional) Especifica el protocolo de visualización predeterminado de las aplicaciones o los escritorios de la autorización global. Los valores válidos son RDP, PCOIP y BLAST para autorizaciones de escritorios globales, y PCOIP y BLAST para autorizaciones de aplicaciones globales.
`--preventProtocolOverride`	(Opcional) Evita que los usuarios sobrescriban el protocolo de visualización predeterminado.
`--allowReset`	(Opcional) Permite que los usuarios restablezcan los escritorios. Se aplican únicamente a las autorizaciones de escritorios globales.
`--htmlAccess`	(Opcional) Habilita la directiva de HTML Access, que permite que los usuarios utilicen la función HTML Access para acceder a los recursos de la autorización global. La opción HTML Access permite a los usuarios finales usar un navegador web para acceder a recursos remotos y no es necesario instalar ningún software cliente en los sistemas locales.

Tabla 5-8. Opciones para crear autorizaciones globales (Continua)

Opción	Descripción
`--multipleSessionsPerUser`	(Opcional) Habilita la directivas de varias sesiones por usuario, lo que permite a los usuarios iniciar sesiones de escritorio independientes desde diferentes dispositivos cliente. Los usuarios que se conectan a la autorización de escritorios global desde dispositivos cliente diferentes obtienen sesiones de escritorios diferentes. Para volver a conectarse a una sesión de escritorios existente, los usuarios deben usar el mismo dispositivo desde el que se inició la sesión. Si no habilita esta directiva, los usuarios siempre se volverán a conectar a las sesiones de escritorios existentes, independientemente del dispositivo cliente que usen. Se aplica únicamente a las autorizaciones de escritorios globales.
`--preLaunch`	(Opcional) Habilita la directiva de preinicio, que inicia la sesión de aplicación antes de que un usuario abra la autorización de aplicaciones de Horizon Client. Cuando habilite la directiva de preinicio, los usuarios pueden iniciar la autorización global de aplicaciones con mayor rapidez. Todos los grupos de aplicaciones de la autorización de aplicaciones global deben ser compatibles con la función de preinicio de sesiones y el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.
`--tags`	(Opcional) Especifica una o más etiquetas que limitan el acceso a la autorización global desde las instancias del servidor de conexión. Para especificar varias etiquetas, escriba una lista entre comillas de nombres de etiquetas separados por comas o por punto y coma. Si desea obtener más información, consulte "Restringir acceso a las autorizaciones globales," página 13.

Ejemplos

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

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

Modificar una autorización global

Para modificar una autorización de escritorios global, use el comando `lmvutil` con la opción `--updateGlobalEntitlement`. Para modificar una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--updateGlobalApplicationEntitlement`.

Sintaxis

```
lmvutil --updateGlobalEntitlement --entitlementName nombre [--description texto]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--multipleSessionsPerUser] [--
disableMultipleSessionsPerUser]
[--requireHomeSite] [--disableRequireHomeSite] [--defaultProtocol valor]
[--scope ámbito] [--htmlAccess] [--disableHtmlAccess] [--tags etiquetas] [--notags]
```

```
lmvutil --updateGlobalApplicationEntitlement --entitlementName nombre [--description texto]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--requireHomeSite] [--disableRequireHomeSite]
[--defaultProtocol valor] [--scope ámbito] [--htmlAccess] [--disableHtmlAccess]
[--appVersion valor] [--appPublisher valor] [--appPath valor] [--tags etiquetas] [--notags]
[--preLaunch] [--disablePreLaunch]
```

Notas de uso

Puede usar estos comandos en cualquier instancia del servidor de conexión de una federación de pods. La función Arquitectura de Cloud Pod almacena nuevos datos en el Nivel de datos global y replica dichos datos en todos los pods de la federación de pods.

Estos comandos devuelven un mensaje de error si la autorización global no existe, el ámbito no es válido, la función Arquitectura de Cloud Pod no se inició o los comandos no pueden crear la autorización global.

Opciones

Puede especificar estas opciones cuando modifica una autorización global. Algunas opciones se aplican únicamente a las autorizaciones de escritorios globales o a las autorizaciones de aplicaciones globales.

Tabla 5-9. Opciones para modificar autorizaciones globales

Opción	Descripción
`--entitlementName`	Nombre de la autorización global que desea modificar.
`--scope`	Ámbito de la autorización global. Los valores válidos son los siguientes: ■ CUALQUIERA. Horizon busca recursos en los pods de la federación. ■ SITIO. Horizon busca recursos únicamente en los pods del mismo sitio en el que se encuentra el pod al que el usuario está conectado. ■ LOCAL. Horizon busca recursos únicamente en el pod al que el usuario está conectado.
`--description`	(Opcional) Descripción de la autorización global. La descripción puede tener entre 1 y 1024 caracteres.
`--disabled`	(Opcional) Deshabilita una autorización global previamente habilitada.
`--enabled`	(Opcional) Habilita una autorización global previamente deshabilitada.
`--fromHome`	(Opcional) Si el usuario tiene un sitio principal, Horizon empieza a buscar recursos en el sitio principal del usuario. Si el usuario no tiene un sitio principal, Horizon empieza a buscar recursos en el sitio al que el usuario está conectado en ese momento.
`--disableFromHome`	(Opcional) Deshabilita la función `--fromHome` para la autorización global.
`--multipleSessionAutoClean`	(Opcional) Cierra las sesiones adicionales del usuario con la misma autorización. Pueden aparecer varias sesiones cuando un pod que contiene una sesión se desconecta, el usuario inicia otra sesión y el pod con el problema vuelve a conectarse con la sesión original. Cuando aparecen varias sesiones, Horizon Client solicita que el usuario seleccione una de ellas. Esta opción determina qué sucede con las sesiones que el usuario no selecciona. Si no especifica esta opción, los usuarios deben cerrar las sesiones adicionales de forma manual. Para hacerlo, pueden cerrar sesión en Horizon Client, o bien iniciar las sesiones y cerrarlas.
`--disableMultipleSessionAutoClean`	(Opcional) Deshabilita la función `--multipleSessionAutoClean` para la autorización global.
`--multipleSessionsPerUser`	(Opcional) Habilita la directivas de varias sesiones por usuario, lo que permite a los usuarios iniciar sesiones de escritorio independientes desde diferentes dispositivos cliente. Los usuarios que se conectan a la autorización de escritorios global desde dispositivos cliente diferentes obtienen sesiones de escritorios diferentes. Para volver a conectarse a una sesión de escritorios existente, los usuarios deben usar el mismo dispositivo desde el que se inició la sesión. Si no habilita esta directiva, los usuarios siempre se volverán a conectar a las sesiones de escritorios existentes, independientemente del dispositivo cliente que usen. Se aplica únicamente a las autorizaciones de escritorios globales.

Tabla 5-9. Opciones para modificar autorizaciones globales (Continua)

Opción	Descripción
`--disableMultipleSessionsPerUser`	(Opcional) Deshabilita la directivas de varias sesiones por usuario de la autorización de escritorios global.
`--requireHomeSite`	(Opcional) Hace que la autorización global esté disponible únicamente si el usuario tiene un sitio principal. Esta opción solo se aplica cuando se especifica también la opción `--fromHome`.
`--disableRequireHomeSite`	(Opcional) Deshabilita la función `--requireHomeSite` para la autorización global.
`--defaultProtocol`	(Opcional) Especifica el protocolo de visualización predeterminado de las aplicaciones o los escritorios de la autorización global. Los valores válidos son RDP, PCOIP y BLAST para autorizaciones de escritorios globales, y PCOIP y BLAST para autorizaciones de aplicaciones globales.
`--htmlAccess`	(Opcional) Habilita la directiva de HTML Access, que permite que los usuarios utilicen la función HTML Access para acceder a los recursos de la autorización global. La opción HTML Access permite a los usuarios finales usar un navegador web para acceder a recursos remotos y no es necesario instalar ningún software cliente en los sistemas locales.
`--disableHtmlAccess`	(Opcional) Deshabilita la directiva de HTML Access para la autorización global.
`--appVersion`	(Opcional) Versión de la aplicación. Se aplican únicamente a las autorizaciones de aplicaciones globales.
`--appPublisher`	(Opcional) Editor de la aplicación. Se aplican únicamente a las autorizaciones de aplicaciones globales.
`--appPath`	(Opcional) Ruta de acceso de la aplicación, por ejemplo, `C:\Program Files\app1.exe`. Se aplican únicamente a las autorizaciones de aplicaciones globales.
`--tags`	(Opcional) Especifica una o más etiquetas que limitan el acceso a la autorización global desde las instancias del servidor de conexión. Para especificar varias etiquetas, escriba una lista entre comillas de nombres de etiquetas separados por comas o por punto y coma. Si desea obtener más información, consulte "Restringir acceso a las autorizaciones globales," página 13.
`--notags`	(Opcional) Elimina las etiquetas de la autorización global.
`--preLaunch`	(Opcional) Habilita la directiva de preinicio, que inicia la sesión de aplicación antes de que un usuario abra la autorización de aplicaciones de Horizon Client. Cuando habilite la directiva de preinicio, los usuarios pueden iniciar la autorización global de aplicaciones con mayor rapidez. Todos los grupos de aplicaciones de la autorización de aplicaciones global deben ser compatibles con la función de preinicio de sesiones y el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.
`--disablePreLaunch`	(Opcional) Deshabilita la directiva de preinicio para la autorización global de aplicaciones.

Ejemplos

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

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

Eliminar una autorización global

Para eliminar una autorización de escritorios global, use el comando `lmvutil` con la opción `--deleteGlobalEntitlement`. Para eliminar una autorización de aplicaciones global, use el comando `lmvutil` con la opción `--deleteGlobalApplicationEntitlement`.

Sintaxis

```
lmvutil --deleteGlobalEntitlement --entitlementName nombre
```

```
lmvutil --deleteGlobalApplicationEntitlement --entitlementName nombre
```

Uso de los comandos

Estos comandos devuelven un mensaje de error si la autorización global especificada no existe, la función Arquitectura de Cloud Pod no se inició o los comandos no pueden eliminar la autorización global.

Opciones

La opción `--entitlementName` permite especificar el nombre de la autorización global que desee eliminar.

Ejemplos

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

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

Agregar un grupo a una autorización global

El comando `lmvutil` con la opción `--addPoolAssociation` permite agregar un grupo de escritorios a una autorización de escritorios global, o bien un grupo de aplicaciones a una autorización de aplicaciones global.

Sintaxis

```
lmvutil --addPoolAssociation --entitlementName nombre --poolId iddegrupo
```

Notas de uso

Debe usar este comando en una instancia del servidor de conexión del pod que contiene el grupo. Por ejemplo, si pod1 contiene un grupo de escritorios para asociarlo con una autorización de escritorios global, debe ejecutar el comando en la instancia del servidor de conexión que reside en pod1.

Repita este comando para que cada grupo forme parte de la autorización global. También puede agregar un grupo concreto a una única autorización global.

IMPORTANTE: Si agrega varios grupos de aplicaciones a una autorización de aplicaciones global, debe agregar la misma aplicación. Por ejemplo, no agregue Calculadora y Microsoft Office PowerPoint a la misma autorización de aplicaciones global. Si agrega distintas aplicaciones, los resultados serán impredecibles y los usuarios autorizados recibirán diferentes aplicaciones en distintos momentos.

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició, la autorización específica no existe, el grupo ya está asociado con la autorización especificada, el grupo no existe o el comando no puede agregar el grupo a la autorización global.

Opciones

Puede especificar estas opciones cuando agrega un grupo a la autorización global.

Tabla 5-10. Opciones para agregar un grupo a una autorización global

Opción	Descripción
`--entitlementName`	Nombre de la autorización global.
`--poolID`	ID del grupo que desea agregar a la autorización global. El ID del grupo debe coincidir con el nombre del grupo, tal como aparece en el pod.

Ejemplo

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

Eliminar un grupo de una autorización global

El comando `lmvutil` con la opción `--removePoolAssociation` permite eliminar un grupo de escritorios de una autorización de escritorios global, o bien un grupo de aplicaciones de una autorización de aplicaciones global.

Sintaxis

```
lmvutil --removePoolAssociation --entitlementName nombre --poolID iddegrupo
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no está inicializada, si la autorización global especificada o el grupo no existen o si el comando no puede eliminar el grupo de la autorización global.

Opciones

Puede especificar estas opciones cuando elimina un grupo de la autorización global.

Tabla 5-11. Opciones para eliminar un grupo de una autorización global

Opción	Descripción
`--entitlementName`	Nombre de la autorización global.
`--poolID`	ID del grupo que desea eliminar de la autorización global. El ID del grupo debe coincidir con el nombre del grupo, tal como aparece en el pod.

Ejemplo

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

Agregar un grupo o un usuario a una autorización global

Para agregar un usuario a una autorización global, use el comando `lmvutil` con la opción `--addUserEntitlement`. Para agregar un grupo a una autorización global, use el comando `lmvutil` con la opción `--addGroupEntitlement`.

Sintaxis

```
lmvutil --addUserEntitlement --userName dominio\nombredeusuario --entitlementName nombre
```

```
lmvutil --addGroupEntitlement --groupName dominio\nombredegrupo --entitlementName nombre
```

Notas de uso

Repita estos comandos con cada usuario o grupo que desee agregar a la autorización global.

Estos comandos devuelven un mensaje de error si la autorización especificada, el usuario o el grupo no existen o si el comando no puede agregar el usuario o el grupo a la autorización.

Opciones

Puede especificar estas opciones cuando agregue un usuario o un grupo a la autorización global.

Tabla 5-12. Opciones para agregar un grupo o un usuario a una autorización global

Opción	Descripción
`--userName`	Nombre del usuario que desea agregar a la autorización global. Use el formato *dominio\nombredeusuario*.
`--groupName`	Nombre del grupo que desea agregar a la autorización global. Use el formato *dominio\nombredegrupo*.
`--entitlementName`	Nombre de la autorización global a la que desea agregar el usuario o el grupo.

Ejemplos

```
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"
```

Eliminar un grupo o un usuario de una autorización global

Para eliminar un usuario de una autorización global, use el comando `lmvutil` con la opción `--removeUserEntitlement`. Para eliminar un grupo de una autorización global, use el comando `lmvutil` con la opción `--removeGroupEntitlement`.

Sintaxis

```
lmvutil --removeUserEntitlement --userName dominio\nombredeusuario --entitlementName nombre
```

```
lmvutil --removeGroupEntitlement --groupName dominio\nombredegrupo --entitlementName nombre
```

Notas de uso

Estos comandos devuelven un mensaje de error si la función Arquitectura de Cloud Pod no está inicializada, si el nombre de usuario, el nombre de grupo o la autorización especificada no existen o si el comando no puede eliminar el usuario o el grupo de la autorización.

Opciones

Debe especificar estas opciones cuando elimine un usuario o un grupo de la autorización global.

Tabla 5-13. Opciones para eliminar un grupo o un usuario de una autorización global

Opción	Descripción
`--userName`	Nombre del usuario que desea eliminar de la autorización global. Use el formato *dominio\nombredeusuario*.
`--groupName`	Nombre del grupo que desea eliminar de la autorización global. Use el formato *dominio\nombredegrupo*.
`--entitlementName`	Nombre de la autorización global de la que desea eliminar el usuario o el grupo.

Ejemplos

```
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"
```

Administrar sitios principales

Puede usar las opciones del comando `lmvutil` para crear, modificar, eliminar y realizar listas de sitios principales.

- Configurar un sitio principal página 63

  Para crear un sitio principal para un usuario, utilice el comando `lmvutil` con la opción `--createUserHomeSite`. Para crear un sitio principal para un grupo, utilice el comando `lmvutil` con la opción `--createGroupHomeSite`. También puede usar estas opciones para asociar un sitio principal con una autorización de escritorios global o una autorización de aplicaciones global.

- Eliminar un sitio principal página 64

  Para eliminar la asociación entre un usuario y un sitio principal, use el comando `lmvutil` con la opción `--deleteUserHomeSite`. Para eliminar la asociación entre un grupo y un sitio principal, use el comando `lmvutil` con la opción `--deleteGroupHomeSite`.

Configurar un sitio principal

Para crear un sitio principal para un usuario, utilice el comando `lmvutil` con la opción `--createUserHomeSite`. Para crear un sitio principal para un grupo, utilice el comando `lmvutil` con la opción `--createGroupHomeSite`. También puede usar estas opciones para asociar un sitio principal con una autorización de escritorios global o una autorización de aplicaciones global.

Sintaxis

`lmvutil --createUserHomeSite --userName` *`dominio\nombredeusuario`* `--siteName` *`nombre`* `[--entitlementName` *`nombre`*`]`

`lmvutil --createGroupHomeSite --groupName` *`dominio\nombredegrupo`* `--siteName` *`nombre`* `[--entitlementName` *`nombre`*`]`

Notas de uso

Para poder configurar un sitio como sitio principal, en primer lugar deberá crearlo. Consulte "Crear un sitio," página 52.

Estos comandos devuelven un mensaje de error si no se inició la función Arquitectura de Cloud Pod, el usuario o el grupo especificados no existen, el sitio especificado no existe, la autorización especificada no existe o los comandos no pueden crear el sitio principal.

Opciones

Puede especificar estas opciones cuando cree un sitio principal para un usuario o un grupo.

Tabla 5-14. Opciones para crear un sitio principal para un usuario o un grupo

Opción	Descripción
`--userName`	Nombre del usuario que se asocia al sitio principal. Use el formato *dominio\nombredeusuario*.
`--groupName`	Nombre del grupo que se asocia al sitio principal. Use el formato *dominio\nombredegrupo*.
`--siteName`	Nombre del sitio que se asocia al usuario o al grupo como sitio principal.
`--entitlementName`	(Opcional) Nombre de una autorización de escritorios global o de una autorización de aplicaciones global que desea asociar al sitio principal. Cuando un usuario selecciona la autorización global especificada, este sitio principal reemplaza al del usuario. Si no especifica esta opción, el comando crea un sitio principal de grupos o de usuarios global.

Ejemplos

```
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"
```

Eliminar un sitio principal

Para eliminar la asociación entre un usuario y un sitio principal, use el comando `lmvutil` con la opción `--deleteUserHomeSite`. Para eliminar la asociación entre un grupo y un sitio principal, use el comando `lmvutil` con la opción `--deleteGroupHomeSite`.

Sintaxis

```
lmvutil --deleteUserHomeSite --userName dominio\nombredeusuario [--entitlementName nombre]
```

```
lmvutil --deleteGroupHomeSite --groupName dominio\nombredegrupo [--entitlementName nombre]
```

Notas de uso

Estos comandos devuelven un mensaje de error si el grupo o el usuario especificados no existen, la autorización global especificada no existe o si los comandos no pueden eliminar la configuración del sitio principal.

Opciones

Puede especificar estas opciones cuando elimina la asociación entre un usuario o un grupo y un sitio principal.

Tabla 5-15. Opciones para eliminar un sitio principal

Opción	Descripción
`--userName`	Nombre de un usuario. Use el formato *dominio\nombredeusuario*.
`--groupName`	Nombre de un grupo. Use el formato *dominio\nombredegrupo*.
`--entitlementName`	(Opcional) Nombre de una autorización de escritorios global o una autorización de aplicaciones global. Esta opción permite eliminar la asociación entre el sitio principal y una autorización global para el grupo o el usuario especificados.

Ejemplos

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

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

Ver una configuración de Arquitectura de Cloud Pod

Puede usar las opciones del comando `lmvutil` para ver una lista con la información de una configuración de Arquitectura de Cloud Pod.

- Lista de autorizaciones globales página 66

  Para obtener información sobre todas las autorizaciones de escritorios globales, incluidos sus atributos y directivas, use el comando `lmvutil` con la opción `--listGlobalEntitlements`. Para obtener información sobre todas las autorizaciones de aplicaciones globales, incluidos sus atributos y directivas, use el comando `lmvutil` con la opción `--listGlobalApplicationEntitlements`.

- Lista de grupos de una autorización global página 66

  El comando `lmvutil` con la opción `--listAssociatedPools` permite especificar los grupos de aplicaciones o escritorios que están asociados con una autorización global específica.

- Lista de grupos o usuarios de una autorización global página 66

  El comando `lmvutil` con la opción `--listEntitlements` permite especificar los usuarios o grupos que están asociados con una autorización global específica.

- Lista de los sitios principales de un usuario o grupo página 67

  Para especificar los sitios principales configurados para un usuario concreto, utilice el comando `lmvutil` con la opción `--showUserHomeSites`. Para especificar los sitios principales configurados para un grupo concreto, utilice el comando `lmvutil` con la opción `--showGroupHomeSites`.

- Especificar el sitio principal efectivo de un usuario página 68

  El comando `lmvutil` con la opción `--resolveUserHomeSite` permite determinar el sitio principal efectivo de un usuario específico. Dado que a los sitios principales se pueden asignar usuarios, grupos y autorizaciones globales, es posible configurar más de un sitio principal para un usuario.

- Listados de asignaciones de grupos de escritorios dedicados página 68

  El comando `lmvutil` con la opción `--listUserAssignments` permite mostrar las asignaciones de grupos de escritorios dedicados de una combinación de usuario y de autorización global.

- Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod página 69

  Para ver los pods de la federación, use el comando `lmvutil` con la opción `--listPods`. Para ver los sitios de la federación, use el comando `lmvutil` con la opción `--listSites`.

Lista de autorizaciones globales

Para obtener información sobre todas las autorizaciones de escritorios globales, incluidos sus atributos y directivas, use el comando `lmvutil` con la opción `--listGlobalEntitlements`. Para obtener información sobre todas las autorizaciones de aplicaciones globales, incluidos sus atributos y directivas, use el comando `lmvutil` con la opción `--listGlobalApplicationEntitlements`.

Sintaxis

```
lmvutil --listGlobalEntitlements
```

```
lmvutil --listGlobalApplicationEntitlements
```

Notas de uso

Estos comandos devuelven un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si estos comandos no pueden mostrar las autorizaciones globales.

Ejemplos

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

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

Lista de grupos de una autorización global

El comando `lmvutil` con la opción `--listAssociatedPools` permite especificar los grupos de aplicaciones o escritorios que están asociados con una autorización global específica.

Sintaxis

```
lmvutil --listAssociatedPools --entitlementName nombre
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si la autorización global especificada no existe.

Opciones

Use la opción `--entitlementName` para especificar el nombre de la autorización global de la que desea especificar los grupos de aplicaciones o escritorios asociados.

Ejemplo

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

Lista de grupos o usuarios de una autorización global

El comando `lmvutil` con la opción `--listEntitlements` permite especificar los usuarios o grupos que están asociados con una autorización global específica.

Sintaxis

```
lmvutil --listEntitlements {--userName dominio\nombredeusuario | --groupName
dominio\nombredegrupo | --entitlementName nombre}
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si el usuario especificado, el grupo o la autorización no existen.

Opciones

Puede especificar estas opciones cuando enumere las asociaciones de autorizaciones globales.

Tabla 5-16. Opciones para especificar las asociaciones de autorizaciones globales

Opción	Descripción
`--userName`	Nombre del usuario del que desea ver las autorizaciones globales. Use el formato *dominio\nombredeusuario*. Esta opción muestra todas las autorizaciones globales asociadas al usuario especificado.
`--groupName`	Nombre del grupo del que desea ver las autorizaciones globales. Use el formato *dominio\nombredegrupo*. Esta opción muestra todas las autorizaciones globales asociadas al grupo especificado.
`--entitlementName`	Nombre de la autorización global. Esta opción muestra todos los usuarios y grupos en la autorización global especificada.

Ejemplo

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

Lista de los sitios principales de un usuario o grupo

Para especificar los sitios principales configurados para un usuario concreto, utilice el comando `lmvutil` con la opción `--showUserHomeSites`. Para especificar los sitios principales configurados para un grupo concreto, utilice el comando `lmvutil` con la opción `--showGroupHomeSites`.

Sintaxis

```
lmvutil --showUserHomeSites --userName dominio\nombredeusuario [--entitlementName nombre]
```

```
lmvutil --showGroupHomeSites --groupName dominio\nombredegrupo [--entitlementName nombre]
```

Notas de uso

Estos comandos devuelven un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si el usuario especificado, el grupo o la autorización global no existen.

Opciones

Puede especificar estas opciones cuando especifique sitios principales para un usuario o un grupo.

Tabla 5-17. Opciones para especificar los sitios principales de un usuario o un grupo

Opción	Descripción
`--userName`	Nombre de un usuario. Use el formato *dominio\nombredeusuario*.
`--groupName`	Nombre de un grupo. Use el formato *dominio\nombredegrupo*.
`--entitlementName`	(Opcional) Nombre de la autorización global. Esta opción permite mostrar los sitios principales para un usuario o grupo y la combinación de autorizaciones globales.

Ejemplo

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

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

Especificar el sitio principal efectivo de un usuario

El comando `lmvutil` con la opción `--resolveUserHomeSite` permite determinar el sitio principal efectivo de un usuario específico. Dado que a los sitios principales se pueden asignar usuarios, grupos y autorizaciones globales, es posible configurar más de un sitio principal para un usuario.

Sintaxis

```
lmvutil --resolveUserHomeSite --entitlementName nombre --userName dominio\nombredeusuario
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si la autorización global especificada o el usuario no existen.

Opciones

Debe especificar estas opciones cuando especifique el sitio principal efectivo de un usuario.

Tabla 5-18. Opciones para especificar el sitio principal efectivo de un usuario

Opción	Descripción
`--entitlementName`	Nombre de la autorización global. Esta opción le permite determinar el sitio principal efectivo de un usuario y la combinación de autorizaciones globales, que puede cambiar con respecto al sitio principal que está configurado para el usuario.
`--userName`	Nombre del usuario cuyo sitio desea incluir en la lista. Use el formato *dominio\nombredeusuario*.

Ejemplo

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

Listados de asignaciones de grupos de escritorios dedicados

El comando `lmvutil` con la opción `--listUserAssignments` permite mostrar las asignaciones de grupos de escritorios dedicados de una combinación de usuario y de autorización global.

Sintaxis

```
lmvutil --listUserAssignments {--userName dominio\nombredeusuario | --entitlementName nombre | --
podName nombre | --siteName nombre}
```

Notas de uso

El software de administración Arquitectura de Cloud Pod gestiona de forma interna los datos originados por este comando.

Este comando devuelve un error si la función Arquitectura de Cloud Pod no se inició o si el comando no puede encontrar el sitio, el pod, la autorización global o el usuario especificados.

Opciones

Al enumerar las asignaciones de usuarios, debe especificar una de las opciones siguientes.

Tabla 5-19. Opciones para especificar las asignaciones de usuarios

Opción	Descripción
`--userName`	Nombre del usuario del que desea ver las asignaciones. Use el formato *dominio\nombredeusuario*. Esta opción muestra las asignaciones del sitio, el pod y la autorización global del usuario especificado.
`--entitlementName`	Nombre de la autorización global. Esta opción muestra los usuarios asignados a la autorización global especificada.
`--podName`	Nombre de un pod. Esta opción muestra los usuarios asignados al pod especificado.
`--siteName`	Nombre de un sitio. Esta opción muestra los usuarios asignados al sitio especificado.

Ejemplo

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

Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod

Para ver los pods de la federación, use el comando `lmvutil` con la opción `--listPods`. Para ver los sitios de la federación, use el comando `lmvutil` con la opción `--listSites`.

Sintaxis

```
lmvutil --listPods
```

```
lmvutil --listSites
```

Notas de uso

Estos comandos devuelven un mensaje de error si la función Arquitectura de Cloud Pod no se inicializó o si estos comandos no pueden mostrar los pods o los sitios.

Ejemplo

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

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

Administrar certificados SSL

Puede usar las opciones del comando `lmvutil` para crear y activar certificados SSL pendientes en un entorno de Arquitectura de Cloud Pod.

La función Arquitectura de Cloud Pod usa certificados firmados para que los SSL bidireccionales protejan y validen el canal de comunicación VIPA. Los certificados se distribuyen en el Nivel de datos global. La función Arquitectura de Cloud Pod reemplaza estos certificados cada siete días.

Para cambiar un certificado en una instancia del servidor de conexión, cree un certificado pendiente, espere a que el proceso de replicación del Nivel de datos global distribuya el certificado a todas las instancias del servidor de conexión y active el certificado.

Las opciones del certificado del comando `lmvutil` solo se usarán si un certificado se encuentra en peligro y un administrador de Horizon desea actualizarlo en un periodo menor a siete días. Estas opciones solo afectan a la instancia del servidor de conexión en la que se están ejecutando. Para cambiar todos los certificados, debe ejecutar las opciones en cada instancia del servidor de conexión.

- Crear un certificado pendiente página 70

  El comando `lmvutil` con la opción `--createPendingCertificate` permite crear un certificado SSL pendiente.

- Activar un certificado pendiente página 70

  El comando `lmvutil` con la opción `--activatePendingCertificate` permite activar un certificado pendiente.

Crear un certificado pendiente

El comando `lmvutil` con la opción `--createPendingCertificate` permite crear un certificado SSL pendiente.

Sintaxis

```
lmvutil --createPendingCertificate
```

Notas de uso

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició o si el comando no puede crear el certificado.

Ejemplo

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

Activar un certificado pendiente

El comando `lmvutil` con la opción `--activatePendingCertificate` permite activar un certificado pendiente.

Sintaxis

```
lmvutil --activatePendingCertificate
```

Notas de uso

Debe usar el comando `lmvutil` con la opción `--createPendingCertificate` para crear un certificado pendiente antes de poder utilizar este comando. Espere a que el proceso de replicación Nivel de datos global distribuya el certificado a todas las instancias del servidor de conexión antes de activar el certificado pendiente. Se pueden producir errores en la conexión VIPA y problemas de administración si activa un certificado pendiente antes de que esté totalmente replicado en todas las instancias del servidor de conexión.

Este comando devuelve un mensaje de error si la función Arquitectura de Cloud Pod no se inició o si el comando no puede activar el certificado.

Ejemplo

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

Índice

T

U

V