

Administrar la arquitectura Cloud Pod en Horizon 7

Diciembre de 2019
VMware Horizon 7 7.11



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2019 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Administrar Arquitectura de Cloud Pod en Horizon 7 6

1 Introducción a Arquitectura de Cloud Pod 7

- Comprender Arquitectura de Cloud Pod 7
 - Compartir datos de clave en el Nivel de datos global 8
 - Enviar mensajes entre pods 8
- Configurar y administrar un entorno de Arquitectura de Cloud Pod 8
- Limitaciones de Arquitectura de Cloud Pod 9

2 Diseñar una topología de Arquitectura de Cloud Pod 10

- Crear sitios de Arquitectura de Cloud Pod 11
- Autorizar usuarios y grupos en la federación de pods 11
- Buscar y asignar aplicaciones y escritorios en la federación de pods 12
 - Comprender la directiva de ámbito 12
 - Información sobre la directiva de varias sesiones por usuario para las autorizaciones de escritorios globales 13
 - Usar sitios principales 13
- Consideraciones para los usuarios sin autenticar 14
- Ejemplo de autorización global 15
- Implementar las restricciones del servidor de conexión para las autorizaciones globales 16
 - Coincidencia de etiquetas 16
 - Requisitos y limitaciones de las restricciones del servidor de conexión 17
 - Ejemplos de restricciones del servidor de conexión 17
- Implementar las restricciones de cliente para las autorizaciones globales 18
- Implementar la función de preinicio de sesión para las autorizaciones de aplicaciones globales 19
- Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales 20
- Habilitar Session Collaboration en las autorizaciones de escritorios globales 20
- Implementar autorizaciones globales de copia de seguridad 21
- Consideraciones para entornos de versión mixta 22
- Consideraciones para el modo Workspace ONE 22
- Consideraciones para VMware Cloud on AWS 22
- Consideraciones para las licencias de acceso de cliente por dispositivo RDS 23
- Límites de la topología de Arquitectura de Cloud Pod 23
- Requisitos de puertos de Arquitectura de Cloud Pod 24
- Consideraciones de seguridad para topologías de Arquitectura de Cloud Pod 24

3 Configurar Arquitectura de Cloud Pod en Horizon Console 26

- Iniciar la función de arquitectura Cloud Pod en Horizon Console 26

Conectar un pod a la federación de pods en Horizon Console	27
Asignar una etiqueta a una instancia del servidor de conexión en Horizon Console	28
Configuración de accesos directos para las autorizaciones globales	29
Hoja de cálculo para configurar una autorización global	30
Crear y configurar una autorización global en Horizon Console	34
Agregar un grupo a una autorización global en Horizon Console	36
Crear y configurar un sitio en Horizon Console	37
Asignar un sitio principal a un usuario o grupo en Horizon Console	38
Crear un sitio principal de reemplazo en Horizon Console	39
Probar la configuración de Arquitectura de Cloud Pod en Horizon Client	40
Ejemplo: establecer una configuración de Arquitectura de Cloud Pod básica	41
Diseñar una topología de ejemplo	42
Inicializar la configuración de ejemplo	43
Conectar los pods de la configuración de ejemplo	43
Crear sitios en la configuración de ejemplo	43
Crear autorizaciones de escritorios globales en la configuración de ejemplo	44
Crear una URL para la configuración de ejemplo	45

4 Administrar un entorno de Arquitectura de Cloud Pod en Horizon Console 46

Consultar la configuración de Arquitectura de Cloud Pod en Horizon Console	46
Consultar el estado de la federación de pods en Horizon Console	48
Ver sesiones de aplicaciones y escritorios en Horizon Console	49
Administrar sitios en Horizon Console	49
Agregar un pod a un sitio en Horizon Console	50
Eliminar un sitio en Horizon Console	50
Cambiar el nombre o la descripción de un sitio en Horizon Console	50
Administrar las autorizaciones globales en Horizon Console	50
Eliminar un grupo de una autorización global en Horizon Console	50
Agregar un grupo o un usuario a una autorización global en Horizon Console	51
Eliminar un grupo o un usuario de una autorización global en Horizon Console	51
Modificar los atributos o las directivas de una autorización global en Horizon Console	52
Eliminar una autorización global en Horizon Console	52
Administrar sitios principales en Horizon Console	53
Modificar una asignación de sitio principal en Horizon Console	53
Eliminar una asignación de sitio principal en Horizon Console	53
Determinar el sitio principal efectivo de un usuario en Horizon Console	53
Modificar un sitio principal de reemplazo en Horizon Console	54
Eliminar un sitio principal de reemplazo en Horizon Console	55
Eliminar un pod de la federación de pods en Horizon Console	55
Anular la inicialización de la función Arquitectura Cloud Pod en Horizon Console	56

5 Administrar Arquitectura de Cloud Pod con Imvutil 57

Uso del comando Imvutil	57
Autenticación del comando Imvutil	58
Salidas del comando Imvutil	58
Opciones del comando Imvutil	59
Inicializar la función Arquitectura de Cloud Pod	61
Deshabilitar la función Arquitectura de Cloud Pod	62
Administrar una federación de pods	62
Conectar un pod a la federación de pods	62
Eliminar un pod de una federación de pods	63
Cambiar el nombre o la descripción de un pod	64
Administrar sitios	65
Crear un sitio	65
Asignar un pod a un sitio	66
Cambiar el nombre o la descripción de un sitio	66
Eliminar un sitio	67
Administrar las autorizaciones globales	67
Crear una autorización global	68
Modificar una autorización global	72
Eliminar una autorización global	76
Agregar un grupo a una autorización global	77
Eliminar un grupo de una autorización global	77
Agregar un grupo o un usuario a una autorización global	78
Eliminar un grupo o un usuario de una autorización global	79
Administrar sitios principales	80
Configurar un sitio principal	80
Eliminar un sitio principal	81
Ver una configuración de Arquitectura de Cloud Pod	82
Lista de autorizaciones globales	83
Lista de grupos de una autorización global	83
Lista de grupos o usuarios de una autorización global	84
Lista de los sitios principales de un usuario o grupo	85
Especificar el sitio principal efectivo de un usuario	85
Listados de asignaciones de grupos de escritorios dedicados	86
Especificar los pods o sitios en una topología de Arquitectura de Cloud Pod	87
Administrar certificados SSL	87
Crear un certificado pendiente	88
Activar un certificado pendiente	88

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 incluye los siguientes temas:

- [Comprender Arquitectura de Cloud Pod](#)
- [Configurar y administrar un entorno de Arquitectura de Cloud Pod](#)
- [Limitaciones de Arquitectura de Cloud Pod](#)

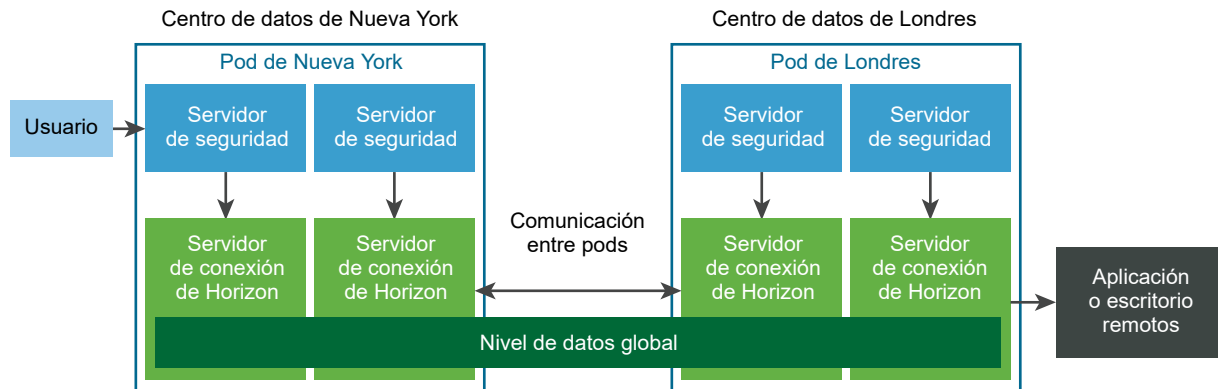
Comprender Arquitectura de Cloud Pod

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 Console y la interfaz de la línea de comandos 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 Console 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 incluye los siguientes temas:

- [Crear sitios de Arquitectura de Cloud Pod](#)
- [Autorizar usuarios y grupos en la federación de pods](#)
- [Buscar y asignar aplicaciones y escritorios en la federación de pods](#)
- [Consideraciones para los usuarios sin autenticar](#)
- [Ejemplo de autorización global](#)
- [Implementar las restricciones del servidor de conexión para las autorizaciones globales](#)
- [Implementar las restricciones de cliente para las autorizaciones globales](#)
- [Implementar la función de preinicio de sesión para las autorizaciones de aplicaciones globales](#)
- [Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales](#)
- [Habilitar Session Collaboration en las autorizaciones de escritorios globales](#)
- [Implementar autorizaciones globales de copia de seguridad](#)
- [Consideraciones para entornos de versión mixta](#)
- [Consideraciones para el modo Workspace ONE](#)
- [Consideraciones para VMware Cloud on AWS](#)
- [Consideraciones para las licencias de acceso de cliente por dispositivo RDS](#)
- [Límites de la topología de Arquitectura de Cloud Pod](#)
- [Requisitos de puertos de Arquitectura de Cloud Pod](#)
- [Consideraciones de seguridad para topologías de Arquitectura de Cloud Pod](#)

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 diferentes 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 sí 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 Console 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 para las autorizaciones de escritorios globales

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.

Si habilita la directiva de varias sesiones por usuario, los usuarios que se conectan a la autorización de escritorios 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 de escritorios global, todos los grupos de escritorios asociados a la autorización de escritorios 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](#).

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 Console.
- 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.

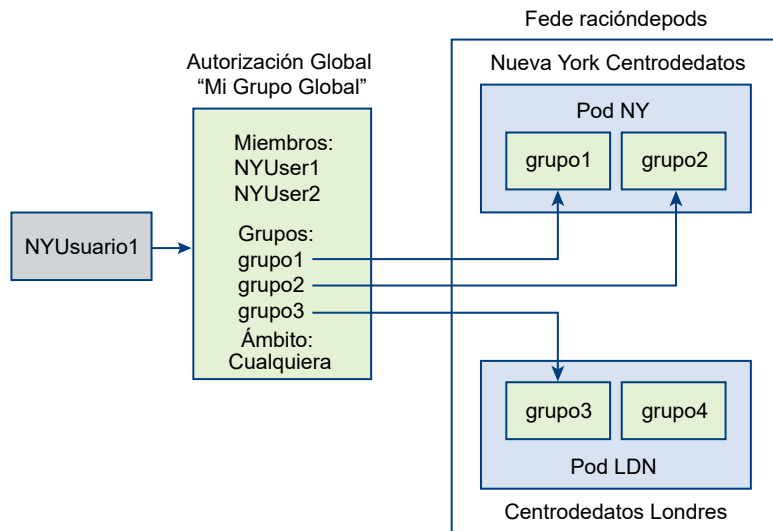
- Solo puede tener un usuario sin autenticar para cada usuario de Active Directory. Si el mismo alias de usuario está asignado a más de un usuario de Active Directory, Horizon Console muestra un mensaje de error en la pestaña **Acceso sin autenticar** del panel Usuarios y grupos.
- Puede asignar sitios principales a usuarios sin autenticar.
- Los usuarios sin autenticar pueden tener varias sesiones.
- Los usuarios con acceso sin autenticar no tienen permiso para autorizaciones de aplicaciones globales que tengan aplicaciones publicadas desde un grupo de escritorios.

Para obtener más información sobre cómo configurar los usuarios sin autenticar, consulte el documento *Administración de Horizon 7*.

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 y grupo2 se encuentran en un pod denominado Pod NY en el centro de datos de Nueva York y grupo3 y grupo4 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 [Ejemplos de restricciones del servidor de conexión](#).

Implementar las restricciones del servidor de conexión para las autorizaciones globales

Puede restringir 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 la función de restricciones del servidor de conexión, puede asignar 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 restricciones del servidor de conexión 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. Reglas de coincidencia de etiquetas](#) 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 restricciones del servidor de conexión solo aplica 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.

Requisitos y limitaciones de las restricciones del servidor de conexión

Antes de implementar las restricciones del servidor de conexión para las autorizaciones globales, debe conocer los requisitos y las 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 las restricciones en la instancia del servidor de conexión con la que el servidor de seguridad está emparejado. No puede configurar las restricciones en un servidor de seguridad.
- Las restricciones del servidor de conexión tienen prioridad 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.

Ejemplos de restricciones del servidor de conexión

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.

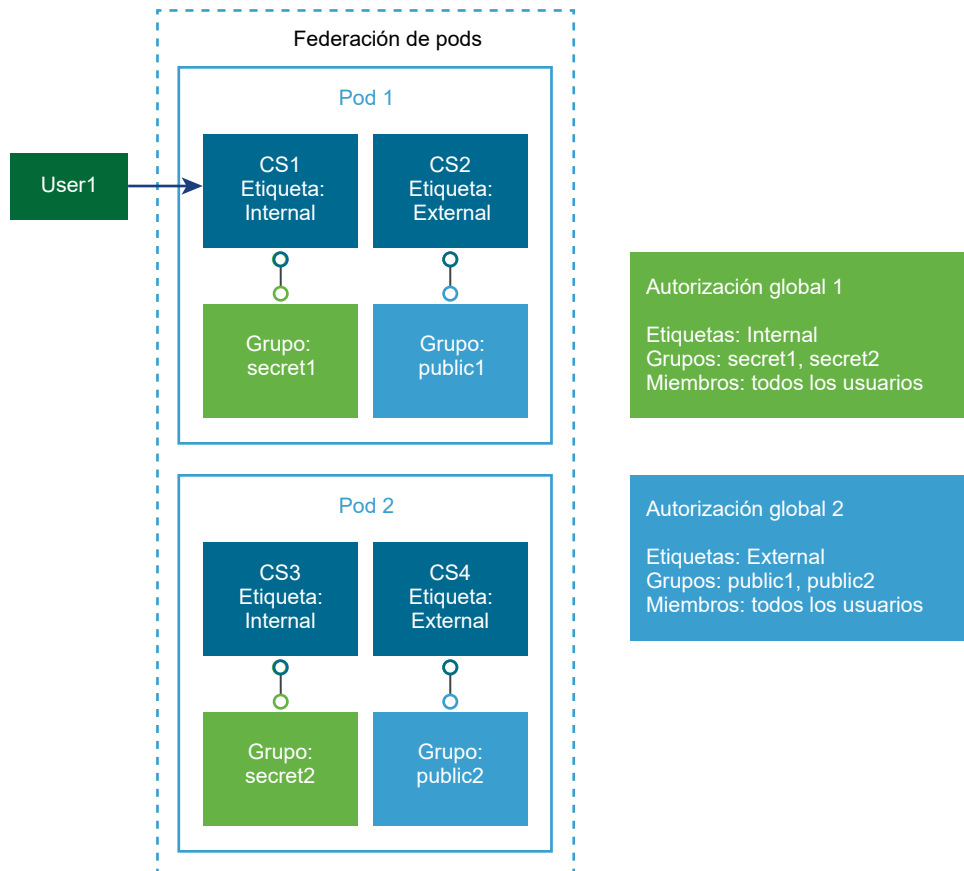
Para evitar que los usuarios externos accedan a determinados grupos de aplicaciones y de escritorios, puede asignar etiquetas como las que se indican a continuación:

- 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. Ejemplos de restricciones del servidor de conexión



Implementar las restricciones de cliente para las autorizaciones globales

Puede limitar el acceso de determinados equipos cliente a las autorizaciones globales. Para restringir el acceso, agregue los nombres de los equipos cliente que pueden acceder a una autorización global en un grupo de seguridad de Active Directory y, a continuación, agregue este grupo a los grupos y los usuarios de la autorización global.

La función de restricciones de cliente tiene los siguientes requisitos y límites.

- Debe habilitar la directiva de restricciones de cliente cuando cree o modifique la autorización global. De forma predeterminada, la directiva de restricciones de cliente está deshabilitada. Puede habilitar esta directiva únicamente para autorizaciones de escritorios flotantes o de aplicaciones globales.
- La opción de directiva de restricciones de cliente en una autorización global reemplaza la opción de directiva de restricciones de cliente a nivel de grupo. Como práctica recomendada, si habilita la directiva de restricciones de cliente en una autorización global, no habilite la directiva de restricciones de cliente en los grupos que contiene la autorización global.
- Debe agregar el grupo de seguridad de Active Directory que contiene los nombres de los equipos cliente que tienen permiso para acceder a la autorización global al crear o modificar la autorización global.
- La función de restricciones de cliente solo permite a determinados equipos clientes acceder a las autorizaciones globales. No proporciona a los usuarios acceso a las autorizaciones globales. Por ejemplo, si un usuario no está en una autorización global (como usuario, miembro o grupo de usuarios), el usuario no puede acceder a la autorización global, aunque el equipo cliente del usuario pueda acceder a la autorización global.
- En esta versión, la función de restricciones de cliente solo se admite en equipos cliente Windows. En los equipos cliente, es necesario Horizon Client 4.6 para Windows o una versión posterior.
- Cuando la directiva de restricciones de cliente está habilitada en una autorización global, los clientes que no sean Windows, los clientes Windows que ejecutan versiones de Horizon Client para Windows anteriores a la versión 4.6 y los clientes HTML Access no pueden iniciar la autorización global.

Implementar la función de preinicio de sesión para las autorizaciones de aplicaciones globales

Con la función de preinicio, un administrador de Horizon puede configurar una aplicación publicada, de forma que la sesión se inicie antes de que el usuario abra la aplicación en Horizon Client. La función de preinicio de sesión permite que las aplicaciones publicadas usadas con frecuencia se inicien con mayor rapidez.

Para habilitar la función de preinicio de sesión para una autorización de aplicaciones global, habilite la directiva de preinicio cuando cree o modifique la autorización de aplicaciones global. Todos los grupos de aplicaciones de la autorización de aplicaciones global deben tener soporte para la función de preinicio de sesiones y el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.

Para obtener más información sobre cómo configurar las granjas y los grupos de aplicaciones para usar la función de preinicio de sesión, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

La función de preinicio de sesión no se admite en escritorios remotos.

Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales

Al crear una autorización de aplicaciones global, puede especificar si los usuarios pueden iniciar varias sesiones de la misma aplicación publicada en diferentes dispositivos cliente. Esta función se denomina modo de sesión múltiple.

Por ejemplo, si un usuario abre una aplicación publicada en modo de sesión múltiple en el cliente A y abre la misma aplicación publicada en el cliente B, la aplicación publicada sigue abierta en el cliente A y se abre una nueva sesión de la aplicación publicada en el cliente B. Por el contrario, si el usuario abre la aplicación publicada en el cliente A en modo de sesión única, la sesión en el cliente A se desconecta y se vuelve a conectar en el cliente B.

Al habilitar el modo de sesión múltiple, puede especificar si está activado de forma predeterminada, desactivado de forma predeterminada o aplicado.

- Cuando el modo de sesión múltiple está activado o desactivado de forma predeterminada, los usuarios que tengan Horizon Client 4.10 o una versión posterior pueden habilitar o deshabilitar el modo de sesión múltiple modificando la opción **Inicio múltiple** en el cliente. Los usuarios que tengan versiones anteriores de Horizon Client no pueden cambiar la opción predeterminada.
- Cuando el modo de sesión múltiple está aplicado, siempre está activado y los usuarios no pueden deshabilitarlo en Horizon Client.

Para obtener más información sobre cómo usar la opción **Inicio múltiple**, consulte la documentación de Horizon Client 4.10 o versiones posteriores.

La función modo de sesión múltiple tiene los siguientes requisitos y limitaciones para las autorizaciones de aplicaciones.

- La opción de modo de sesión múltiple que establece para la autorización de aplicaciones global debe coincidir con la opción que está configurada en los grupos de aplicaciones asociados con la autorización de aplicaciones global. Para obtener más información sobre cómo habilitar el modo de sesión múltiple para los grupos de aplicaciones, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Si el modo de sesión múltiple está habilitado, no puede habilitar la función de preinicio de sesión para la autorización de aplicaciones global o los grupos de aplicaciones asociados a la autorización de aplicaciones global. No se admite la función de preinicio de sesión cuando el modo de sesión múltiple está habilitado.

Habilitar Session Collaboration en las autorizaciones de escritorios globales

Con la función Session Collaboration, los usuarios finales pueden invitar a otros usuarios a que se unan a una sesión de escritorio remoto existente.

Para permitir que los usuarios de escritorios remotos puedan colaborar, un administrador de Horizon debe habilitar la función Session Collaboration en el grupo de escritorios que proporciona el escritorio remoto. En los grupos de escritorios RDS, un administrador de Horizon debe habilitar la función Session Collaboration en la granja en la que se base el grupo de escritorios RDS.

Para que los usuarios invitados puedan unirse a sesiones de pods diferentes al pod del propietario de la sesión, debe habilitar la directiva Session Collaboration en la autorización de escritorios global que contenga el grupo de escritorios.

Para conocer todos los requisitos y limitaciones de la función Session Collaboration, como los requisitos de licencia, consulte cómo configurar Session Collaboration en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Esta función no se admite en aplicaciones publicadas.

Implementar autorizaciones globales de copia de seguridad

Cuando edite una autorización de escritorios global o una autorización de aplicaciones global, puede seleccionar una autorización global de copia de seguridad. Una autorización global de copia de seguridad envía aplicaciones publicadas o escritorios remotos cuando la autorización global principal no puede iniciar una sesión cuando, por ejemplo, la capacidad del grupo no es suficiente o no hay pods disponibles. Una autorización global de copia de seguridad puede contener grupos de cualquier pod de la federación.

Los siguientes ajustes de la autorización global de copia de seguridad deben contener los ajustes de la autorización global primaria correspondientes.

- Tipo de asignación de usuario
- Protocolo de visualización predeterminado (solo si no se permite que los usuarios seleccionen el protocolo de visualización)
- Protocolos de visualización admitidos
- HTML Access
- Permitir a los usuarios restablecer o reiniciar sus máquinas
- Permitir que los usuarios inicien sesiones independientes desde dispositivos cliente diferentes
- Permitir Session Collaboration

La autorización global de copia de seguridad tiene las siguientes restricciones y limitaciones.

- Para las autorizaciones de escritorios globales, puede configurar una autorización global de copia de seguridad solo si la directiva de asignación de usuarios se configura como Flotante.
- Después de configurar una autorización global de copia de seguridad, se deshabilitan la función de edición, las autorizaciones de usuario y la configuración del sitio principal de reemplazo de la autorización global de copia de seguridad.

- No se puede seleccionar una autorización global principal o de copia de seguridad existentes cuando se selecciona una autorización global de copia de seguridad.
- Las autorizaciones globales de copia de seguridad no pueden administrarse en la nube.
- Las autorizaciones globales de copia de seguridad no se pueden asociar a ninguna autorización de grupo o usuario.

Para obtener más información sobre cómo editar una autorización global, consulte [Modificar los atributos o las directivas de una autorización global en Horizon Console](#).

Consideraciones para entornos de versión mixta

Los entornos de versión mixta Arquitectura de Cloud Pod se admiten a partir de la versión 7.4 de Horizon 7. Por ejemplo, una federación de pods puede incluir pods que utilicen la versión 7.4 de Horizon 7 y pods que usen la versión 6.x de Horizon 6.

Las nuevas funciones no funcionan en entornos de versión mixta. Por ejemplo, una nueva función que esté visible en Horizon Administrator para una instancia del servidor de conexión de la versión 7.4 de Horizon 7 no estará visible en Horizon Administrator para una instancia del servidor de conexión de la versión 6.x de Horizon 6. VMware recomienda que actualice todos los pods a la misma versión de Horizon 7.

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 el documento *Administración de Horizon 7*.

Consideraciones para VMware Cloud on AWS

Puede implementar Horizon 7 en un entorno de nube híbrida cuando utilice Arquitectura de Cloud Pod para interconectar Horizon 7 en las instalaciones y pods de Horizon 7 en VMware Cloud on AWS. Puede permitir que los usuarios accedan a escritorios virtuales y a aplicaciones publicadas en las instalaciones y en VMware Cloud on AWS.

Para obtener más información, consulte la sección sobre la arquitectura Cloud Pod de Horizon 7 para VMware Cloud en AWS en la *guía sobre cómo implementar Horizon 7 en VMware Cloud on AWS*, disponible en <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf>.

Consideraciones para las licencias de acceso de cliente por dispositivo RDS

Cuando un dispositivo cliente de Windows se conecta a una aplicación o a un escritorio publicados en un host RDS, este recibe una licencia de acceso de cliente (CAL) por dispositivo RDS, si está configurado el modo de licencias por dispositivo en el host RDS. De forma predeterminada, las CAL se almacenan únicamente en el dispositivo cliente.

A partir de Horizon Client para Windows 4.9, si el dispositivo cliente tiene una licencia, siempre la presenta. Los clientes de Windows que tengan Horizon Client 4.8 o una versión anterior solo presentan la licencia del pod específico, en caso de tenerla. Si el dispositivo cliente no presenta ninguna, se usa la licencia más actualizada de cualquier pod incluido en el inicio de la aplicación o el escritorio publicados. Si no se encuentra ninguna licencia en los pods incluidos en el inicio, se presenta el ID del dispositivo cliente al servidor de licencias y se expide una licencia.

Importante VMware le recomienda que actualice al cliente de Windows y al software del servidor más recientes para gestionar mejor las licencias de RDS.

Para obtener más información, consulte el apartado sobre las licencias de acceso de cliente por dispositivo RDS en Horizon 7 en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

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.

En la siguiente tabla se muestra el número total de sesiones admitidas en esta versión.

Tabla 2-2. Límites de la federación de pods

Objeto	Límite
Sesiones totales	250 000
Pods	50
Sesiones por pod	12.000
Sitios	15
Instancias del servidor de conexión por pod	7
Instancias del servidor de conexión totales	350

Los límites de pods, sitios e instancias del servidor de conexión totales indican el número máximo admitido para cada componente de la federación de pods. Siempre que la configuración se mantenga dentro de los límites especificados, puede diseñar una topología adecuada para alcanzar el número total de sesiones.

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.
tráfico	22636	Se usa para la replicación LDAP segura del nivel de datos global.
tráfico	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.

Nota Microsoft Windows Server requiere un rango dinámico de puertos abiertos entre todas las instancias del servidor de conexión. Microsoft Windows necesita estos puertos para el funcionamiento normal de llamadas a procedimientos remotos (RPC) y réplicación de Active Directory. Para obtener más información sobre el rango de puertos dinámico, consulte la documentación de Microsoft Windows Server.

Consideraciones de seguridad para topologías de Arquitectura de Cloud Pod

Para usar Horizon Console 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, consulte el documento *Administración de Horizon 7*.

Configurar Arquitectura de Cloud Pod en Horizon Console

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.

En este capítulo, se explica cómo configurar un entorno de Arquitectura de Cloud Pod en Horizon Console. Para obtener más información sobre la interfaz de línea de comandos de `lmvutil`, consulte [Capítulo 5 Administrar Arquitectura de Cloud Pod con lmvutil](#).

Este capítulo incluye los siguientes temas:

- [Iniciar la función de arquitectura Cloud Pod en Horizon Console](#)
- [Conectar un pod a la federación de pods en Horizon Console](#)
- [Asignar una etiqueta a una instancia del servidor de conexión en Horizon Console](#)
- [Configuración de accesos directos para las autorizaciones globales](#)
- [Hoja de cálculo para configurar una autorización global](#)
- [Crear y configurar una autorización global en Horizon Console](#)
- [Agregar un grupo a una autorización global en Horizon Console](#)
- [Crear y configurar un sitio en Horizon Console](#)
- [Asignar un sitio principal a un usuario o grupo en Horizon Console](#)
- [Crear un sitio principal de reemplazo en Horizon Console](#)
- [Probar la configuración de Arquitectura de Cloud Pod en Horizon Client](#)
- [Ejemplo: establecer una configuración de Arquitectura de Cloud Pod básica](#)

Iniciar la función de arquitectura Cloud Pod en Horizon Console

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 Console de cualquier instancia del servidor de conexión del pod.

- 2 Seleccione **Configuración > Arquitectura Cloud Pod**, haga clic en **Iniciar la función de arquitectura Cloud Pod** y haga clic en **Aceptar** para iniciar el proceso de inicialización.

Horizon Console muestra el curso del proceso de inicialización. 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.

- 3 (opcional) Para cambiar el nombre predeterminado de la federación de pods, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de texto **Nombre** y haga clic en **Aceptar**.
- 4 (opcional) Para cambiar el nombre predeterminado del pod, seleccione **Configuración > Sitios**, seleccione el pod, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de texto **Nombre** y haga clic en **Aceptar**.
- 5 (opcional) Para cambiar el nombre predeterminado del sitio, seleccione **Configuración > Sitios**, seleccione el sitio, haga clic en **Editar**, escriba el nuevo nombre en el cuadro de diálogo **Nombre** y haga clic en **Aceptar**.

Pasos siguientes

Para agregar más pods a la federación, consulte [Conectar un pod a la federación de pods en Horizon Console](#).

Conectar un pod a la federación de pods en Horizon Console

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 Console 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.

Requisitos previos

- 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 [Iniciar la función de arquitectura Cloud Pod en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión en el pod que va a conectar a la federación de pods.
- 2 Seleccione **Configuración > Arquitectura Cloud Pod** y haga clic en **Unirse a la federación de pods**.
- 3 En el cuadro de texto **Servidor de conexión (nombre de host o dirección IP)**, 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 (dominio/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 Para unir el pod a la federación, haga clic en **Aceptar**.

Horizon Console muestra el curso de la operación de unión. 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.

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 Console. Consulte [Consultar el estado de la federación de pods en Horizon Console](#).

Nota Es posible que se produzca un pequeño retraso una vez que los datos de estado estén disponibles en Horizon Console.

Pasos siguientes

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

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

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.

Requisitos previos

Familiarícese con la función de restricciones del servidor de conexión. Consulte [Implementar las restricciones de cliente para las autorizaciones globales](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de la instancia del servidor de conexión.
- 2 Seleccione **Configuración > 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.

Pasos siguientes

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 en Horizon Console](#) o [Modificar los atributos o las directivas de una autorización global en Horizon Console](#).

Configuración de accesos directos para las autorizaciones globales

Es posible establecer accesos directos para las autorizaciones globales. Cuando un usuario autorizado se conecta a una instancia del servidor de conexión en la federación de pods desde un cliente Windows, Horizon Client para Windows coloca estos accesos directos en el menú Inicio de Windows, en el escritorio o en ambos del dispositivo cliente del usuario. Puede establecer un acceso directo al crear o modificar una autorización global.

Debe seleccionar una carpeta de categorías o la carpeta raíz (/), durante la configuración de acceso directo. Puede agregar sus propias carpetas de categorías y asignarles un nombre. Puede configurar hasta cuatro niveles de carpetas. Por ejemplo, puede agregar una carpeta de categorías denominada Office y seleccionar esa carpeta para todas las aplicaciones de trabajo, como Microsoft Office y Microsoft PowerPoint.

Para los accesos directos del menú Inicio, en dispositivos cliente Windows 7, Horizon Client coloca las carpetas y los accesos directos en la carpeta de aplicaciones de VMware del menú Inicio. Si selecciona la carpeta raíz (/) para un acceso directo, Horizon Client coloca el acceso directo en la carpeta de aplicaciones de VMware. En dispositivos cliente Windows 8 y Windows 10, Horizon Client coloca las carpetas de categorías y los accesos directos en la lista Aplicaciones. Si selecciona la carpeta raíz (/) para un acceso directo, Horizon Client coloca el acceso directo directamente en la lista Aplicaciones.

En clientes Mac, si Horizon Client para Mac está configurado para ejecutar aplicaciones publicadas desde la carpeta Aplicaciones y permite accesos directos automáticos desde el servidor, las carpetas de categorías para las autorizaciones de aplicaciones globales se encuentran en la carpeta Aplicaciones del cliente Mac.

Después de crear un acceso directo, aparece una marca de verificación en la columna Acceso directo de aplicaciones para la autorización global en la página Autorizaciones globales de Horizon Console.

De forma predeterminada, Horizon Client para Windows solicita a los usuarios autorizados que instalen los accesos directos la primera vez que se conectan al servidor. Puede configurar Horizon Client para Windows de forma que instale los accesos directos de forma automática o que no los instale en ningún momento si modifica la opción de directiva de grupo **Instalar automáticamente accesos directos si están configurados en Horizon Server**. Para obtener más información, consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.

De forma predeterminada, los cambios realizados en los accesos directos se sincronizan en el dispositivo cliente Windows de un usuario cada vez que el usuario se conecta al servidor. Los usuarios pueden deshabilitar la función de sincronización de accesos directos en Horizon Client para Windows. Para obtener más información, consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.

Para usuarios de Windows, esta función requiere Horizon Client 4.6 para Windows o versiones posteriores en el sistema cliente. Para usuarios de Mac, esta función requiere Horizon Client para Mac 4.10 o versiones posteriores en el sistema cliente.

Hoja de cálculo para configurar una autorización global

Cuando crea una autorización global en Horizon Console, la interfaz de usuario le solicitará que configure algunas opciones. Use esta hoja de cálculo para preparar las opciones de configuración antes de crear la autorización global.

Puede imprimir esta hoja de cálculo y anotar los valores que desee especificar cuando agregue autorizaciones globales.

Tabla 3-1. Hoja de cálculo: opciones para configurar una autorización global

Opción	Descripción	Introduzca los valores aquí
Nombre	Nombre de la autorización global. El nombre aparece en la lista de aplicaciones y escritorios disponibles en Horizon Client. El nombre puede tener entre 1 y 64 caracteres.	
Descripción	(Opcional) Descripción de la autorización global. La descripción puede tener entre 1 y 1024 caracteres.	

Tabla 3-1. Hoja de cálculo: opciones para configurar una autorización global (continuación)

Opción	Descripción	Introduzca los valores aquí
Restricciones del servidor de conexión	<p>(Opcional) Asocia las etiquetas del servidor de conexión a la autorización global para restringir el acceso a ella desde instancias específicas del servidor de conexión.</p> <hr/> <p>Nota Puede seleccionar solo las etiquetas que están asignadas a las instancias del servidor de conexión del pod local. Para seleccionar las etiquetas asignadas a las instancias del servidor de conexión en otro pod, debe iniciar sesión en una instancia del servidor de conexión del otro pod y modificar la autorización global.</p> <hr/> <p>Si desea obtener más información, consulte Implementar las restricciones del servidor de conexión para las autorizaciones globales.</p>	
Carpeta de categorías	<p>(Opcional) Crea un acceso directo para la autorización global. Puede crear una carpeta de categorías nueva o seleccionar una. Puede configurar hasta cuatro subcarpetas. Puede configurar un acceso directo en el menú Inicio de Windows, en el escritorio o en ambos.</p> <p>Puede tener hasta 64 caracteres de longitud. Para especificar una subcarpeta, introduce una barra diagonal inversa (\), por ejemplo, dir1\dir2\dir3\dir4. Puede especificar hasta cuatro niveles de carpeta. La barra diagonal inversa no puede aparecer al principio ni al final de un nombre y no es posible combinar dos o más barras diagonales inversas. Por ejemplo, \dir1, dir1\dir2\, dir1\\dir2 y dir1\\dir2 no son nombres válidos. No puede introducir palabras clave reservadas de Windows.</p> <p>Si desea obtener más información, consulte Configuración de accesos directos para las autorizaciones globales.</p>	
Autorización global de copia de seguridad	<p>(Solo disponible cuando edita una autorización global) Una autorización global de copia de seguridad distribuye los escritorios remotos o las aplicaciones publicadas cuando la autorización global principal no puede iniciar una sesión. Para conocer los requisitos y las restricciones, consulte Implementar autorizaciones globales de copia de seguridad.</p>	
Asignación de usuarios	<p>(Solo para autorizaciones de escritorios globales) Especifica el tipo de grupo de escritorios que puede contener la autorización global. Puede configurar una de las siguientes directivas de asignación de usuarios:</p> <ul style="list-style-type: none"> ■ Flotante: la autorización global contiene solo grupos de escritorios flotantes. ■ Dedicado: la autorización global contiene solo grupos de escritorios dedicados. 	

Tabla 3-1. Hoja de cálculo: opciones para configurar una autorización global (continuación)

Opción	Descripción	Introduzca los valores aquí
Ámbito	<p>Especifica dónde buscar escritorios o aplicaciones para satisfacer una solicitud de la autorización global. Puede configurar una de las siguientes directivas de ámbito:</p> <ul style="list-style-type: none"> ■ 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. <p>Si desea obtener más información, consulte Comprender la directiva de ámbito.</p>	
Utilizar sitio principal y El usuario autorizado debe tener sitio principal	<p>(Opcional) Si los usuarios tienen sitios principales, configura una directiva del sitio principal para la autorización global. Puede configurar las siguientes directivas de sitio principal:</p> <ul style="list-style-type: none"> ■ Utilizar sitio principal: empieza a buscar escritorios o aplicaciones en el sitio principal de usuario. Si el usuario no tiene un sitio principal y la opción El usuario autorizado debe tener sitio principal no está seleccionada, se asumirá 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. Esta opción estará disponible solo si la opción Utilizar sitio principal está seleccionada. <p>Si desea obtener más información, consulte Usar sitios principales.</p>	
Limpiar automáticamente las sesiones redundantes	<p>(Opcional) Especifica si se van a limpiar las sesiones redundantes.</p> <p>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.</p>	
Protocolo de visualización predeterminado	<p>Especifica el protocolo de visualización predeterminado de las aplicaciones y los escritorios en la autorización global. Puede configurar PCoIP o VMware Blast.</p>	
Permitir que los usuarios elijan el protocolo	<p>Si habilita esta directiva, los usuarios podrán anular el protocolo de visualización predeterminado.</p>	

Tabla 3-1. Hoja de cálculo: opciones para configurar una autorización global (continuación)

Opción	Descripción	Introduzca los valores aquí
Permitir a los usuarios restablecer o reiniciar sus máquinas	(Solo para autorizaciones de escritorios globales) Si se habilita esta directiva, los usuarios podrán restablecer y reiniciar los escritorios en la autorización de escritorios global.	
HTML Access	<p>Si habilita esta directiva, 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.</p> <p>Para obtener más información, consulte el documento <i>Guía de usuario de VMware Horizon HTML Access</i>.</p>	
Preinicio	<p>(Solo para autorizaciones de aplicaciones globales) Si se habilita esta directiva, los usuarios podrán iniciar las autorizaciones de aplicaciones globales con mayor rapidez.</p> <p>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.</p>	
Permitir Session Collaboration	<p>Si habilita esta directiva, los usuarios podrán invitar a otros usuarios a unirse a sus sesiones de escritorio remoto.</p> <p>Nota Si habilita esta directiva, todos los grupos de escritorios de la autorización de escritorios global también deben tener soporte para la función Session Collaboration. En los grupos de escritorios RDS, esta función está habilitada a nivel de granja.</p> <p>Si desea obtener más información, consulte Habilitar Session Collaboration en las autorizaciones de escritorios globales.</p>	
Permitir que los usuarios inicien sesiones independientes desde dispositivos cliente diferentes	<p>(Solo para autorizaciones de escritorios globales) Si habilita esta directiva, los usuarios que se conecten a la autorización global desde dispositivos cliente diferentes recibirán 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.</p> <p>Nota Si habilita esta directiva, todos los grupos de escritorios de la autorización global también deben admitir varias sesiones por usuario.</p> <p>Si desea obtener más información, consulte Información sobre la directiva de varias sesiones por usuario para las autorizaciones de escritorios globales.</p>	

Tabla 3-1. Hoja de cálculo: opciones para configurar una autorización global (continuación)

Opción	Descripción	Introduzca los valores aquí
Restricciones de cliente	<p>Si habilita esta directiva, el acceso a la autorización global se restringirá a equipos cliente específicos. Puede habilitar esta directiva únicamente para autorizaciones de escritorios flotantes o de aplicaciones globales.</p> <p>Debe agregar los nombres de los equipos que pueden acceder a la autorización global en un grupo de seguridad de Active Directory. Puede seleccionar este grupo de seguridad cuando agregue usuarios o grupos a la autorización global.</p> <p>Si desea obtener más información, consulte Implementar las restricciones de cliente para las autorizaciones globales.</p>	
Modo de sesión múltiple	<p>(Solo autorización de aplicaciones global) Utilice esta directiva para configurar el modo de sesión múltiple para una autorización de aplicaciones global. Los valores válidos son los siguientes.</p> <ul style="list-style-type: none"> ■ Deshabilitado: no se admite el modo de sesión múltiple. ■ Habilitado (deshabilitado de forma predeterminada): se admite el modo de sesión múltiple, pero está deshabilitado de forma predeterminada. Para usar el modo de sesión múltiple, los usuarios deben habilitar la opción Inicio múltiple en Horizon Client 4.10 o versiones posteriores. Para los usuarios con una versión anterior de Horizon Client, la aplicación siempre se inicia en modo de sesión única ■ Habilitado (habilitado de forma predeterminada): se admite el modo de sesión múltiple y está habilitado de forma predeterminada. Los usuarios pueden deshabilitar el modo de sesión múltiple si deshabilitan la opción Inicio múltiple en Horizon Client 4.10 o una versión posterior. Para los usuarios con una versión anterior de Horizon Client, la aplicación siempre se inicia en modo de sesión única ■ Habilitado (forzado): se admite el modo de sesión múltiple y la aplicación se inicia siempre en modo de sesión múltiple. Los usuarios no pueden deshabilitar el modo de sesión múltiple deshabilitando la opción Inicio múltiple en Horizon Client 4.10 o versiones posteriores. Los usuarios que tengan una versión anterior de Horizon Client reciben un mensaje de error que indica que no se admite el modo de inicio solicitado. <p>Si desea obtener más información, consulte Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales.</p>	

Crear y configurar una autorización global en Horizon Console

Puede utilizar Horizon Console para crear y configurar las autorizaciones globales. Las autorizaciones globales permiten a los usuarios y a los grupos acceder a los escritorios y aplicaciones de 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.

Requisitos previos

- Inicie la función Arquitectura de Cloud Pod. Consulte [Iniciar la función de arquitectura Cloud Pod en Horizon Console](#).
- Decida qué tipo de autorización de escritorios global desea crear y los usuarios y grupos que se incluirán en ella. Consulte [Autorizar usuarios y grupos en la federación de pods](#).
- Decida qué opciones de la autorización global desea configurar. Consulte [Hoja de cálculo para configurar una autorización global](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales** y haga clic en **Agregar**.
- 3 Seleccione el tipo de autorización global que desea agregar.

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

- 4 Haga clic en **Siguiente** y siga las instrucciones para configurar la autorización global.

Use la información de configuración que recopiló en la hoja de cálculo de configuración de autorizaciones globales.

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

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

Para restringir el acceso de determinados equipos cliente a la autorización global, seleccione el grupo de seguridad de Active Directory que contenga los nombres de los equipos que pueden acceder a la autorización global.

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.

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

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.

Pasos siguientes

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 en Horizon Console](#)

Agregar un grupo a una autorización global en Horizon Console

Horizon Console 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.

Requisitos previos

- Crear y configurar una autorización global. Consulte [Crear y configurar una autorización global en Horizon Console](#).
- 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 Console de cualquier instancia del servidor de conexión del pod que contiene el grupo que desea agregar a la autorización global.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Haga clic en el nombre de 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 en Horizon Console

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.

Requisitos previos

- Decida si la topología de Arquitectura de Cloud Pod debe incluir estos sitios. Consulte [Crear sitios de Arquitectura de Cloud Pod](#).
- Inicie la función Arquitectura de Cloud Pod. Consulte [Iniciar la función de arquitectura Cloud Pod en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.

2 Cree el sitio.

a En Horizon Console, seleccione **Configuración > 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 Para crear el sitio, haga clic en **Aceptar**.

3 Agregue un pod a un sitio.

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

a En Horizon Console, seleccione **Configuración > Sitios**.

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

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

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

Asignar un sitio principal a un usuario o grupo en Horizon Console

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 7 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 en Horizon Console](#).

Requisitos previos

- Decida si desea asignar sitios principales a usuarios o grupos en su entorno de Arquitectura de Cloud Pod. Consulte [Usar sitios principales](#).
- Agrupe los pods de la federación de pods en sitios. Consulte [Crear y configurar un sitio en Horizon Console](#).
- 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 7 utilice el sitio principal de un usuario cuando se asignen escritorios desde dicha autorización global. Consulte [Crear y configurar una autorización global en Horizon Console](#).
- Inicie la función Arquitectura de Cloud Pod. Consulte [Iniciar la función de arquitectura Cloud Pod en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Usuarios y grupos**, haga clic en la pestaña **Asignación de sitio principal** y haga clic en **Agregar**.
- 3 Para filtrar los grupos o los usuarios según sus criterios de búsqueda, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar**.

Puede seleccionar la casilla de verificación **Usuarios sin autenticar** para buscar usuarios de acceso sin autenticar en la federación de pods.
- 4 Seleccione un usuario o un grupo y haga clic en **Siguiente**.
- 5 Seleccione el sitio principal que desee asignar al usuario o al grupo en el menú desplegable **Sitio principal** y haga clic en **Enviar**.

Crear un sitio principal de reemplazo en Horizon Console

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.

Requisitos previos

- Verifique que la autorización global tenga la directiva **Utilizar sitio principal** habilitada. Si desea obtener más información, consulte [Modificar los atributos o las directivas de una autorización global en Horizon Console](#).
- 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 en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Seleccione el nombre de la autorización global que desea asociar a un sitio principal y haga clic en la pestaña **Sitio principal de reemplazo**.

4 Haga clic en **Agregar**.

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 desea reemplazar y haga clic en **Siguiente**.

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 de reemplazo** y haga clic en **Enviar**.

Probar la configuración de Arquitectura de Cloud Pod en Horizon Client

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

Requisitos previos

- 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 una aplicación publicada o a un escritorio remoto.

La aplicación publicada o el escritorio remoto se iniciarán correctamente. La aplicación publicada o el escritorio remoto que se inicie 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 una aplicación o un escritorio desde el pod al que está conectado.

Pasos siguientes

Si la autorización global no aparece cuando se conecta a la instancia del servidor de conexión, use Horizon Console para comprobar que la autorización está configurada correctamente. Si la autorización global aparece pero no se inicia ninguna aplicación publicada ni ningún escritorio remoto, 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.

Procedimiento

1 Diseñar una topología de ejemplo

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

2 Inicializar la configuración de ejemplo

Para inicializar la función Arquitectura de Cloud Pod, el administrador de Horizon debe iniciar sesión en la interfaz de usuario de Horizon Console de la instancia del servidor de conexión de Horizon en Pod Oriental 1, seleccionar **Configuración > Arquitectura Cloud Pod** y hacer clic en **Iniciar la función de arquitectura Cloud Pod**.

3 Conectar los pods de la configuración de ejemplo

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

4 Crear sitios en la configuración de ejemplo

El administrador de Horizon usa Horizon Console 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

El administrador de Horizon usa Horizon Console 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.

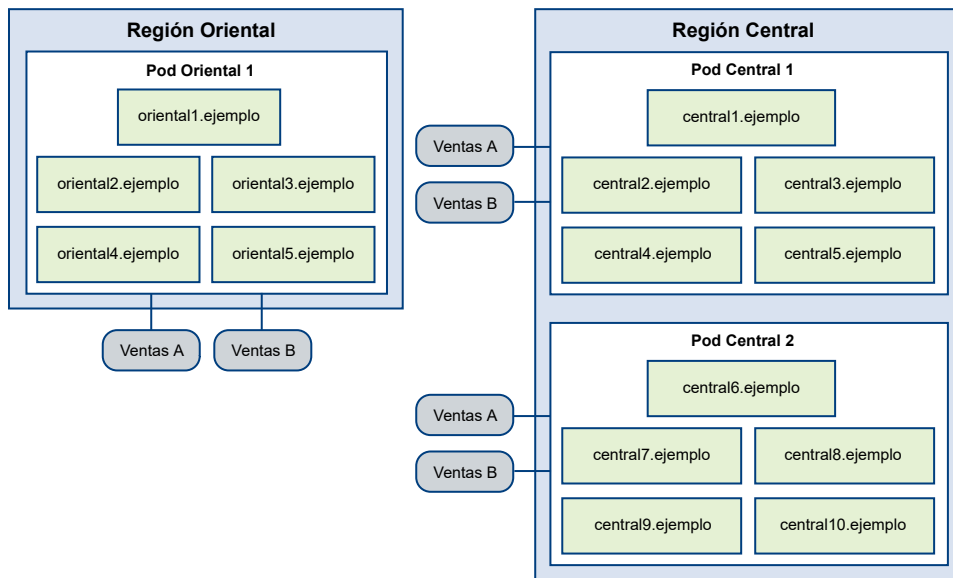
6 Crear una URL para la configuración de ejemplo

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 debe iniciar sesión en la interfaz de usuario de Horizon Console de la instancia del servidor de conexión de Horizon en Pod Oriental 1, seleccionar **Configuración > Arquitectura Cloud Pod** y hacer clic en **Iniciar la función de arquitectura Cloud Pod**.

Dado que el administrador de Horizon usa la interfaz de usuario de Horizon Console 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 Console para conectar el Pod Central 1 y el Pod Central 2 a la federación de pods.

- 1 Para conectar el Pod Central 1, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Console de una instancia del servidor de conexión del Pod Central 1, selecciona **Configuración > 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 el Pod Central 2, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Console de una instancia del servidor de conexión del Pod Central 2, selecciona **Configuración > 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 Console 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 Console de todas las instancias del servidor de conexión de la federación de pods.
- 2 Para crear un sitio para el centro de datos oriental, el administrador de Horizon debe seleccionar **Configuración > Sitios** y hacer clic en **Agregar**.
- 3 Para crear un sitio para el centro de datos central, el administrador de Horizon debe seleccionar **Configuración > 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 > 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 central, el administrador de Horizon debe seleccionar **Configuración > 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 central, el administrador de Horizon debe seleccionar **Configuración > 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 Console 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 agregar usuarios a la autorización de escritorios global, el administrador de Horizon inicia sesión en la interfaz de usuario de Horizon Console de un servidor de conexión de la federación de pods, selecciona **Inventario > Autorizaciones globales**, hace clic en la pestaña **Usuarios y grupos** y hace clic en **Agregar autorizaciones**.

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 Console de una instancia del servidor de conexión en el Pod Oriental 1, seleccionar **Inventario > Autorizaciones globales**, hacer clic en el nombre de 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 Console de una instancia del servidor de conexión en el Pod Central 1, seleccionar **Inventario > Autorizaciones globales**, hacer clic en el nombre de 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 Console de una instancia del servidor de conexión en el Pod Central 2, seleccionar **Inventario > Autorizaciones globales**, hacer clic en el nombre de 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 en Horizon Console

4

Horizon Console permite ver, modificar y mantener el entorno de Arquitectura de Cloud Pod.

Para obtener información general sobre el uso de Horizon Console, consulte cómo usar VMware Horizon Console en el documento *Administración de VMware Horizon Console*. Para obtener más información sobre la interfaz de línea de comandos de `lmvutil`, consulte [Capítulo 5 Administrar Arquitectura de Cloud Pod con lmvutil](#).

Este capítulo incluye los siguientes temas:

- [Consultar la configuración de Arquitectura de Cloud Pod en Horizon Console](#)
- [Consultar el estado de la federación de pods en Horizon Console](#)
- [Ver sesiones de aplicaciones y escritorios en Horizon Console](#)
- [Administrar sitios en Horizon Console](#)
- [Administrar las autorizaciones globales en Horizon Console](#)
- [Administrar sitios principales en Horizon Console](#)
- [Eliminar un pod de la federación de pods en Horizon Console](#)
- [Anular la inicialización de la función Arquitectura Cloud Pod en Horizon Console](#)

Consultar la configuración de Arquitectura de Cloud Pod en Horizon Console

Puede usar Horizon Console para consultar información sobre las autorizaciones globales, los pods, los sitios y los sitios principales.

Procedimiento

- ◆ Para ver una lista de todas las autorizaciones globales de la configuración, seleccione **Inventario > Autorizaciones globales**.

Puede usar la interfaz de usuario de Horizon Console 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, seleccione **Inventario > Autorizaciones globales**, haga 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 Console de la instancia del servidor de conexión en el pod remoto para ver dichos grupos.

- ◆ Para ver qué autorización de escritorios global contiene un grupo de escritorios concreto, selecciona **Inventario > Escritorios**.

El nombre de la autorización de escritorios global que contiene el grupo de escritorios aparece en la columna Autorización global de ese grupo de escritorios en la página Grupos de escritorios. También puede hacer clic en el nombre de un grupo de escritorios en la página Grupos de escritorios para consultar el nombre de la autorización de escritorios global en la pestaña **Resumen**.

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

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

- ◆ Para identificar rápidamente el pod en el que inició sesión en Horizon Console, busque el nombre del pod en el encabezado situado en la parte superior de la ventana de Horizon Console.

Esta función es útil si inicia sesión en varios pods.

- ◆ Para ver una lista de los pods de la federación, seleccione **Configuración > Arquitectura Cloud Pod**.

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

- ◆ Para ver una lista de los sitios de la federación, incluidos los pods de cada sitio, seleccione **Configuración > Sitios**.

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

- ◆ Para ver una lista de las asignaciones del sitio principal para los usuarios y los grupos, seleccione **Usuarios y grupos** y haga clic en la pestaña **Asignación de sitio principal**.

- ◆ Para ver una lista de sitios principales de un usuario o de un grupo según la autorización global, siga estos pasos.

- a Seleccione **Usuarios y grupos** y haga clic en la pestaña **Resolución del sitio principal**.
- b Haga clic en **Buscar 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**.

El nombre de la autorización global aparece en la columna Autorizaciones 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 **Inventario > Autorizaciones globales**, haga 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.

Consultar el estado de la federación de pods en Horizon Console

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 Console.

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 Horizon 7*.

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 Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 En Horizon Console, seleccione **Supervisar > Panel**.
- 3 En el panel **Estado del sistema**, haga clic en **Ver** y, a continuación, en **Pods remotos**.

La página Pods remotos 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 en Horizon Console

Puede usar Horizon Console 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 Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 En Horizon Console, seleccione **Buscar sesiones**.
- 3 Seleccione los criterios e inicie la búsqueda.

Opción	Acción
Buscar por usuario	a Seleccione Usuario en el menú desplegable y haga clic en Buscar usuario . b Seleccione los criterios de búsqueda en el cuadro de diálogo Buscar usuario y haga clic en Buscar .
Buscar por pod	a Seleccione Pod en el menú desplegable. b Seleccione un pod de la lista y haga clic en Buscar .
Buscar por pods de brokering	a Seleccione Pod de brokering en el menú desplegable. b Seleccione un pod de la lista y haga clic en Buscar .

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 Console entre dos y tres minutos después de iniciar la sesión.

Pasos siguientes

En la página de resultados de búsqueda es posible desconectar o cerrar la sesión, reiniciar un escritorio, restablecer una máquina virtual o enviar un mensaje a un usuario de un escritorio.

Administrar sitios en Horizon Console

Horizon Console permite crear, modificar y eliminar sitios de Arquitectura de Cloud Pod. Un sitio es un grupo de pods.

Agregar un pod a un sitio en Horizon Console

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

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Configuración > Sitios**.
- 3 Seleccione el sitio que contiene el pod que desea agregar.
- 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**.

Eliminar un sitio en Horizon Console

Horizon Console permite eliminar un sitio de una federación de pods.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Configuración > Sitios**.
- 3 Seleccione el sitio que quiere eliminar, haga clic en **Eliminar** y haga clic en **Aceptar**.

Cambiar el nombre o la descripción de un sitio en Horizon Console

Horizon Console permite editar el nombre o la descripción de un sitio.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Configuración > Sitios**.
- 3 Seleccione el sitio que quiere editar, haga clic en **Editar**, realice los cambios y haga clic en **Aceptar**.

Administrar las autorizaciones globales en Horizon Console

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

Eliminar un grupo de una autorización global en Horizon Console

Horizon Console permite eliminar un grupo de una autorización global.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de todas las instancias del servidor de conexión del pod que contengan el grupo que desea eliminar.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Haga clic en el nombre de la autorización global.
- 4 En la pestaña **Grupos locales**, haga clic en la fila que contenga el grupo, haga clic en **Eliminar** y haga clic en **Aceptar**.

Agregar un grupo o un usuario a una autorización global en Horizon Console

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

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales** y haga clic en el nombre de la autorización global.
- 3 En la pestaña **Usuarios y grupos**, haga clic en **Agregar autorizaciones**.
- 4 Para buscar grupos o usuarios de Active Directory, haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar**.

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.
- 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.

Para restringir el acceso de determinados equipos cliente a la autorización global, seleccione el grupo de seguridad de Active Directory que contenga los nombres de los equipos que pueden acceder a la autorización global.
- 6 Para guardar los cambios, haga clic en **Aceptar**.

Eliminar un grupo o un usuario de una autorización global en Horizon Console

Horizon Console permite eliminar un usuario o un grupo de una autorización global.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.

- 2 Seleccione **Inventario > Autorizaciones globales** y haga clic en el nombre de la autorización global.
- 3 En la pestaña Usuarios y grupos, seleccione la casilla de verificación del usuario o del grupo que desee eliminar y haga clic en **Eliminar autorizaciones**.
- 4 Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

Modificar los atributos o las directivas de una autorización global en Horizon Console

Horizon Console permite modificar los atributos y las directivas de las autorizaciones globales.

Puede modificar el nombre y la descripción de las autorizaciones globales, las etiquetas del servidor de conexión asociadas a la autorización global, así como la carpeta de categorías de un acceso directo del menú Inicio de Windows. Puede cambiar las directivas de ámbito, sitio principal, sesiones redundantes, protocolo de visualización predeterminado, HTML Access, preinicio, Session Collaboration y restricciones del cliente. También puede agregar una autorización global de copia de seguridad.

En las autorizaciones de aplicaciones globales, puede modificar la ruta, la versión y el editor de la aplicación después de agregar el primer grupo de aplicaciones. Si agrega un grupo de aplicaciones a una autorización de aplicación global que ya contiene un grupo de aplicaciones, se conservan los valores anteriores de la ruta, la versión y el editor de la aplicación.

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

Requisitos previos

Utilice la hoja de cálculo de configuración de autorizaciones globales para registrar los atributos y las directivas que quiera modificar. Consulte [Hoja de cálculo para configurar una autorización global](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Seleccione la fila de la autorización global y haga clic en **Editar**.
- 4 Modifique los atributos y las directivas de la autorización global.

Use la información de configuración que recopiló en la hoja de cálculo de configuración de autorizaciones globales.

- 5 Para guardar los cambios, haga clic en **Enviar**.

Eliminar una autorización global en Horizon Console

Horizon Console 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 Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Haga clic en la fila de la autorización global que desea eliminar y, a continuación en **Eliminar**.
- 4 Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

Administrar sitios principales en Horizon Console

Horizon Console permite crear, modificar, eliminar y realizar listas de sitios principales.

Modificar una asignación de sitio principal en Horizon Console

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

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Usuarios y grupos** y haga clic en la pestaña **Asignación de sitio principal**.
- 3 Seleccione la fila del usuario o grupo y haga clic en **Editar**.
- 4 Seleccione otro sitio principal en el menú desplegable **Sitio principal** y haga clic en **Aceptar**.

Eliminar una asignación de sitio principal en Horizon Console

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

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 en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Usuarios y grupos** y haga clic en la pestaña **Asignación de sitio principal**.
- 3 Seleccione la fila del usuario o grupo y haga clic en **Eliminar**.
- 4 Para eliminar la asignación de sitio principal, haga clic en **Aceptar**.

Determinar el sitio principal efectivo de un usuario en Horizon Console

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 Console permite determinar el sitio principal efectivo de un usuario.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Usuarios y grupos** y haga clic en la pestaña **Resolución del sitio principal**.
- 3 Haga clic en **Buscar usuario**.
- 4 Para buscar usuarios de Active Directory, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar**.
- 5 Seleccione el usuario de Active Directory cuyo sitio principal efectivo desea ver y haga clic en **Aceptar**.

Horizon Console 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 Autorizaciones. Puede expandir esta carpeta para que muestre las asignaciones de los sitios principales que no tienen efecto en la autorización global. Horizon Console usa un texto tachado para indicar que un sitio principal no se está utilizando.

Horizon Console muestra el origen de la asignación de 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 Console muestra el nombre del grupo, por ejemplo, **(a través de Usuarios del dominio)**. Si el sitio principal se creó desde la asignación de sitio principal del usuario, Horizon Console muestra **(Predeterminado)**. Si el sitio principal se creó desde la autorización global (un sitio principal de reemplazo), Horizon Console muestra **(Directo)**.

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

Modificar un sitio principal de reemplazo en Horizon Console

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

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Seleccione el nombre de la autorización global y haga clic en la pestaña **Sitio principal de reemplazo**.

- 4 Seleccione la asignación del sitio principal que desee reemplazar y haga clic en **Editar**.
- 5 Seleccione otro sitio principal en el menú desplegable **Sitio principal de reemplazo** y haga clic en **Aceptar**.

Eliminar un sitio principal de reemplazo en Horizon Console

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 Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Inventario > Autorizaciones globales**.
- 3 Seleccione el nombre de la autorización global y haga clic en la pestaña **Sitio principal de reemplazo**.
- 4 Seleccione el sitio principal de reemplazo y haga clic en **Quitar**.
- 5 Para eliminar el sitio principal de reemplazo, haga clic en **Aceptar**.

Eliminar un pod de la federación de pods en Horizon Console

Puede usar Horizon Console 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 Arquitectura de Cloud Pod. Consulte [Anular la inicialización de la función Arquitectura Cloud Pod en Horizon Console](#).

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 Console de cualquier instancia del servidor de conexión del pod que desea eliminar de la federación de pods.
- 2 Seleccione **Configuración > Arquitectura Cloud Pod**, seleccione el pod que desee eliminar y haga clic en **Separar**.
- 3 Para comenzar la operación de separación, haga clic en **Aceptar**.

Horizon Console muestra el curso del proceso de separación.

Anular la inicialización de la función Arquitectura Cloud Pod en Horizon Console

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

Requisitos previos

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 en Horizon Console](#).

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de Horizon Console de cualquier instancia del servidor de conexión de la federación de pods.
- 2 Seleccione **Configuración > Arquitectura Cloud Pod** y haga clic en **Desinicializar**.
- 3 Para comenzar el proceso de desinicialización, haga clic en **Aceptar**.

Horizon Console muestra el progreso del proceso de desinicialización. 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.

Administrar Arquitectura de Cloud Pod con lmvutil

5

La interfaz de la línea de comandos 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 incluye los siguientes temas:

- [Uso del comando lmvutil](#)
- [Inicializar la función Arquitectura de Cloud Pod](#)
- [Deshabilitar la función Arquitectura de Cloud Pod](#)
- [Administrar una federación de pods](#)
- [Administrar sitios](#)
- [Administrar las autorizaciones globales](#)
- [Administrar sitios principales](#)
- [Ver una configuración de Arquitectura de Cloud Pod](#)
- [Administrar certificados SSL](#)

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 Console permite asignar la función de administrador a un usuario. Consulte el documento *Administración de Horizon 7*.

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
<code>--authAs</code>	Nombre de un usuario administrador de Horizon. No use <i>dominio\nombredeusuario</i> ni el formato de nombre principal de usuario (UPN).
<code>--authDomain</code>	Nombre de dominio completo del usuario administrador de Horizon especificado en la opción <code>--authAs</code> .
<code>--authPassword</code>	Contraseña del usuario administrador de Horizon especificado en la opción <code>--authAs</code> . Si introduce "*" en lugar de una contraseña, el comando <code>lmvutil</code> 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](#).

Tabla 5-2. Opciones del comando lmvutil

Opción	Descripción
--activatePendingCertificate	Activa un certificado SSL pendiente. Consulte Activar un certificado pendiente .
--addGroupEntitlement	Asocia un grupo de usuarios con una autorización global. Consulte Agregar un grupo o un usuario a una autorización global .
--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 .
--addUserEntitlement	Asocia un usuario con una autorización global. Consulte Agregar un grupo o un usuario a una autorización global .
--assignPodToSite	Asigna un pod a un sitio. Consulte Asignar un pod a un sitio .
--createGlobalApplicationEntitlement	Crea una autorización de aplicaciones global. Consulte Crear una autorización global .
--createGlobalEntitlement	Crea una autorización de escritorios global. Consulte Crear una autorización global .
--createSite	Crear un sitio. Consulte Crear un sitio .
--createGroupHomeSite	Asocia un grupo de usuarios con un sitio principal. Consulte Configurar un sitio principal .
--createPendingCertificate	Crea un certificado SSL pendiente. Consulte Crear un certificado pendiente .
--createUserHomeSite	Asocia un usuario con un sitio principal. Consulte Configurar un sitio principal .
--deleteGlobalApplicationEntitlement	Elimina una autorización de aplicaciones global. Consulte Eliminar una autorización global .
--deleteGlobalEntitlement	Elimina una autorización de escritorios global. Consulte Eliminar una autorización global .
--deleteSite	Elimina un sitio. Consulte Eliminar un sitio .
--deleteGroupHomeSite	Elimina la asociación entre un grupo de usuarios y un sitio principal. Consulte Eliminar un sitio principal .
--deleteUserHomeSite	Elimina la asociación entre un usuario y un sitio principal. Consulte Eliminar un sitio principal .
--editSite	Modifica el nombre o la descripción de un sitio. Consulte Cambiar el nombre o la descripción de un sitio .

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

Opción	Descripción
--ejectPod	Elimina un pod que no se encuentra disponible de una federación. Consulte Eliminar un pod de una federación de pods .
--help	Especifica las opciones del comando lmvutil.
--initialize	Inicia la función Arquitectura de Cloud Pod. Consulte Inicializar la función Arquitectura de Cloud Pod .
--join	Conecta un pod a una federación de pods. Consulte Conectar un pod a la federación de pods .
--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 .
--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
--listGlobalApplicationEntitlements	Especifica todas las autorizaciones de aplicaciones globales. Consulte Lista de autorizaciones globales .
--listGlobalEntitlements	Especifica todas las autorizaciones de escritorios globales. Consulte Lista de autorizaciones globales .
--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 .
--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 .
--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 .
--removePoolAssociation	Elimina la asociación entre un grupo de escritorios y una autorización global. Consulte Eliminar un grupo de una autorización global .
--resolveUserHomeSite	Muestra el sitio principal efectivo de un usuario. Consulte Especificar el sitio principal efectivo de un usuario .
--removeGroupEntitlement	Elimina un grupo de usuarios de una autorización global. Consulte Eliminar un grupo o un usuario de una autorización global .
--removeUserEntitlement	Elimina un usuario de una autorización global. Consulte Eliminar un grupo o un usuario de una autorización global .
--showGroupHomeSites	Muestra todos los sitios principales de un grupo. Consulte Lista de los sitios principales de un usuario o grupo .

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

Opción	Descripción
--showUserHomeSites	Muestra todos los sitios principales de un usuario. Consulte Lista de los sitios principales de un usuario o grupo .
--uninitialize	Deshabilita la función Arquitectura de Cloud Pod. Consulte Deshabilitar la función Arquitectura de Cloud Pod .
--unjoin	Elimina un pod que se encuentra disponible de una federación. Consulte Eliminar un pod de una federación de pods .
--updateGlobalApplicationEntitlement	Modifica una autorización de aplicaciones global. Consulte Modificar una autorización global .
--updateGlobalEntitlement	Modifica una autorización de escritorios global. Consulte Modificar una autorización global .
--updatePod	Modifica el nombre o la descripción de un pod. Consulte Cambiar el nombre o la descripción de un pod .
--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 una federación de pods

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

- [Conectar un pod a la federación de pods](#)

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

- [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.

- [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.

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 direccióndeservidor --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
<code>--joinServer</code>	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.
<code>--userName</code>	Nombre de un usuario administrador de Horizon en el pod ya iniciado. Use el formato <i>dominio \nombredeusuario</i> .
<code>--password</code>	Contraseña del usuario especificado en la opción <code>--userName</code> .

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
<code>--podName</code>	Nombre de pod que desea actualizar.
<code>--newPodName</code>	(Opcional) Nombre nuevo del pod. Un nombre de pod puede tener entre 1 y 64 caracteres.
<code>--description</code>	(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**

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**

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

- **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.

- **Eliminar un sitio**

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
<code>--siteName</code>	Nombre del sitio nuevo. Un nombre de sitio puede tener entre 1 y 64 caracteres.
<code>--description</code>	(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 nombredeIpod --siteName nombredeIsitio
```

Notas de uso

Antes de asignar un pod a un sitio, debe crear el sitio. Consulte [Crear un sitio](#).

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
<code>--podName</code>	Nombre del pod que desea asignar al sitio.
<code>--siteName</code>	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](#).

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 nombredeIsitio [--newSiteName nombredeIsitio] [--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](#)

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**

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**

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**

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**

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**

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**

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] [--categoryFolder nombredecarpeta] [--clientRestrictions] [--collaboration]
[--shortcutLocations {desktop | launcher | desktop,launcher}]
```

```
lmvutil --createGlobalApplicationEntitlement --entitlementName nombre --scope ámbito
[--description texto] [--disabled] [--fromHome] [--multipleSessionAutoClean]
[--requireHomeSite] [--defaultProtocol valor] [--preventProtocolOverride] [--htmlAccess]
[--preLaunch] [--tags etiquetas] [--categoryFolder nombredecarpeta] [--clientRestrictions]
[--shortcutLocations {desktop | launcher | desktop,launcher}] [--multiSessionMode valor]
```

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: <ul style="list-style-type: none"> ■ 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.
--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.

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

Opción	Descripción
<code>--fromHome</code>	(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.
<code>--multipleSessionAutoClean</code>	<p>(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.</p> <p>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.</p> <p>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.</p>
<code>--requireHomeSite</code>	(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 <code>--fromHome</code> .
<code>--defaultProtocol</code>	(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.
<code>--preventProtocolOverride</code>	(Opcional) Evita que los usuarios sobrescriban el protocolo de visualización predeterminado.
<code>--allowReset</code>	(Opcional) Permite que los usuarios restablezcan los escritorios. Se aplican únicamente a las autorizaciones de escritorios globales.
<code>--htmlAccess</code>	(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.
<code>--multipleSessionsPerUser</code>	(Opcional) Habilita la directiva 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.
<code>--preLaunch</code>	(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 tener soporte para la función de preinicio de sesiones y el tiempo de espera de la sesión de preinicio debe ser el mismo para todas las granjas.

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

Opción	Descripción
--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 Implementar las restricciones del servidor de conexión para las autorizaciones globales .
--categoryFolder	(Opcional) Especifica el nombre de la carpeta de categorías que contiene un acceso directo para la autorización global en dispositivos cliente. Puede configurar hasta cuatro niveles de carpetas. Puede tener hasta 64 caracteres de longitud. Para especificar una subcarpeta, introduce una barra diagonal inversa (\), por ejemplo, dir1\dir2\dir3\dir4. Puede especificar hasta cuatro niveles de carpeta. La barra diagonal inversa no puede aparecer al principio ni al final de un nombre y no es posible combinar dos o más barras diagonales inversas. Por ejemplo, \dir1, dir1\dir2\, dir1\\dir2 y dir1\\ \dir2 no son nombres válidos. No puede introducir palabras clave reservadas de Windows. También debe especificar la opción --shortcutLocations para indicar la ubicación del acceso directo en un dispositivo cliente Windows. Si desea obtener más información, consulte Configuración de accesos directos para las autorizaciones globales .
--clientRestrictions	(Opcional) Permite la directiva de restricciones del cliente, que restringe el acceso a la autorización global para equipos cliente específicos. Si desea obtener más información, consulte Implementar las restricciones de cliente para las autorizaciones globales .
--collaboration	(Opcional) Habilita la directiva de Session Collaboration, que permite a los usuarios de sesiones de escritorio remoto invitar a otros usuarios a unirse a sus sesiones. Todos los grupos de escritorios de la autorización de escritorios global deben tener soporte para la función Session Collaboration. Se aplican únicamente a las autorizaciones de escritorios globales.
--shortcutLocations	(Opcional) Utilice esta opción con la opción --categoryFolder para especificar la ubicación del acceso directo en el dispositivo cliente. Los valores válidos son desktop, que crea el acceso directo en el escritorio Windows, y launcher, que crea el acceso directo en el menú Inicio de Windows. También puede especificar desktop y launcher, separados por comas, para crear accesos directos, tanto en el escritorio Windows como en el menú Inicio de Windows.
--multiSessionMode	(Opcional) Configura la función de modo de sesión múltiple en la autorización de aplicaciones global. Especifique uno de los siguientes valores: DISABLED, ENABLED_DEFAULT_OFF, ENABLED_DEFAULT_ON o ENABLED_ENFORCED. Si desea obtener más información, consulte Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales .

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] [--categoryFolder nombredecarpeta] [--disableCategoryFolder]
[--clientRestrictions] [--disableClientRestrictions] [--collaboration]
[--disableCollaboration] [--shortcutLocations {desktop | launcher | desktop,launcher}]
[--backupEntitlementName nombre] [--disableBackupEntitlement]
```

```
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] [--categoryFolder nombredecarpeta] [--disableCategoryFolder]
[--clientRestrictions] [--disableClientRestrictions] [--shortcutLocations {desktop | launcher |
desktop,launcher}]
[--multiSessionMode valor] [--backupEntitlementName nombre] [--disableBackupEntitlement]
```

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
<code>--entitlementName</code>	Nombre de la autorización global que desea modificar.
<code>--scope</code>	<p>Ámbito de la autorización global. Los valores válidos son los siguientes:</p> <ul style="list-style-type: none"> ■ 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.
<code>--description</code>	(Opcional) Descripción de la autorización global. La descripción puede tener entre 1 y 1024 caracteres.
<code>--disabled</code>	(Opcional) Deshabilita una autorización global previamente habilitada.
<code>--enabled</code>	(Opcional) Habilita una autorización global previamente deshabilitada.
<code>--fromHome</code>	(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.
<code>--disableFromHome</code>	(Opcional) Deshabilita la función <code>--fromHome</code> para la autorización global.
<code>--multipleSessionAutoClean</code>	<p>(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.</p> <p>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.</p> <p>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.</p>
<code>--disableMultipleSessionAutoClean</code>	(Opcional) Deshabilita la función <code>--multipleSessionAutoClean</code> para la autorización global.
<code>--multipleSessionsPerUser</code>	(Opcional) Habilita la directiva 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.
<code>--disableMultipleSessionsPerUser</code>	(Opcional) Deshabilita la directiva de varias sesiones por usuario para la autorización de escritorios global.
<code>--requireHomeSite</code>	(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 <code>--fromHome</code> .
<code>--disableRequireHomeSite</code>	(Opcional) Deshabilita la función <code>--requireHomeSite</code> para la autorización global.

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

Opción	Descripción
--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 Implementar las restricciones del servidor de conexión para las autorizaciones globales .
--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 tener soporte para 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.

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

Opción	Descripción
<code>--categoryFolder</code>	(Opcional) Especifica el nombre de la carpeta de categorías que contiene un acceso directo para la autorización global en dispositivos cliente. Puede configurar hasta cuatro niveles de carpetas. Puede tener hasta 64 caracteres de longitud. Para especificar una subcarpeta, introduce una barra diagonal inversa (\), por ejemplo, <code>dir1\dir2\dir3\dir4</code> . Puede especificar hasta cuatro niveles de carpeta. La barra diagonal inversa no puede aparecer al principio ni al final de un nombre y no es posible combinar dos o más barras diagonales inversas. Por ejemplo, <code>\dir1</code> , <code>dir1\dir2\</code> , <code>dir1\\dir2</code> y <code>dir1\\dir2</code> no son nombres válidos. No puede introducir palabras clave reservadas de Windows. También debe especificar la opción <code>--shortcutLocations</code> para indicar la ubicación del acceso directo en un dispositivo cliente Windows. Si desea obtener más información, consulte Configuración de accesos directos para las autorizaciones globales .
<code>--disableCategoryFolder</code>	(Opcional) Elimina la carpeta de categorías para la autorización global.
<code>--clientRestrictions</code>	(Opcional) Permite la directiva de restricciones del cliente, que restringe el acceso a la autorización global para equipos cliente específicos. Si desea obtener más información, consulte Implementar las restricciones de cliente para las autorizaciones globales .
<code>--disableClientRestrictions</code>	(Opcional) Deshabilita la directiva de restricciones del cliente para la autorización global.
<code>--collaboration</code>	(Opcional) Habilita la directiva de Session Collaboration, que permite a los usuarios de sesiones de escritorio remoto invitar a otros usuarios a unirse a sus sesiones. Todos los grupos de escritorios de la autorización de escritorios global deben tener soporte para la función Session Collaboration. Se aplican únicamente a las autorizaciones de escritorios globales.
<code>--disableCollaboration</code>	(Opcional) Deshabilita la directiva de Session Collaboration para la autorización de escritorios global.
<code>--shortcutLocations</code>	<p>(Opcional) Utilice esta opción para modificar o crear un acceso directo en el dispositivo cliente. Los valores válidos son <code>desktop</code>, que crea el acceso directo en el escritorio, y <code>launcher</code>, que crea el acceso directo en el menú Inicio de Windows. También puede especificar ambos valores, <code>desktop</code> y <code>launcher</code>, separados por comas, para crear accesos directos tanto en el escritorio como en el menú Inicio de Windows.</p> <p>Si va a modificar un acceso directo (es decir, si la carpeta de categorías ya se ha creado), no necesita especificar la opción <code>--categoryFolder</code>, a menos que desee cambiar el nombre de la carpeta de categorías.</p> <p>Si aún no se ha creado la carpeta de categorías, deberá especificar la opción <code>--categoryFolder</code> junto con la opción <code>--shortcutLocations</code>.</p> <p>Nota No utilice esta opción con <code>--disableCategoryFolder</code>.</p>
<code>--multiSessionMode</code>	(Opcional) Configura la función de modo de sesión múltiple en la autorización de aplicaciones global. Especifique uno de los siguientes valores: <code>DISABLED</code> , <code>ENABLED_DEFAULT_OFF</code> , <code>ENABLED_DEFAULT_ON</code> o <code>ENABLED_ENFORCED</code> . Si desea obtener más información, consulte Habilitar el modo de sesión múltiple para autorizaciones de aplicaciones globales .

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

Opción	Descripción
<code>--backupEntitlementName</code>	(Opcional) Especifique el nombre de una autorización global de copia de seguridad. Una autorización global de copia de seguridad distribuye los escritorios remotos o las aplicaciones publicadas cuando la autorización global principal no puede iniciar una sesión. Para las autorizaciones de escritorios globales, el tipo de asignación de usuario debe ser Flotante. Si desea obtener más información, consulte Implementar autorizaciones globales de copia de seguridad .
<code>--disableBackupEntitlement</code>	(Opcional) Deshabilita la autorización global de copia de seguridad.

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 iddegupo
```

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
<code>--entitlementName</code>	Nombre de la autorización global.
<code>--poolId</code>	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 iddegupo
```

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 <i>dominio \nombredeusuario</i> .
--groupName	Nombre del grupo que desea agregar a la autorización global. Use el formato <i>dominio \nombredegrupo</i> .
--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 <i>dominio \nombredeusuario</i> .
--groupName	Nombre del grupo que desea eliminar de la autorización global. Use el formato <i>dominio \nombredegrupo</i> .
--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

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

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](#).

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 <i>dominio\nombredeusuario</i> .
--groupName	Nombre del grupo que se asocia al sitio principal. Use el formato <i>dominio\nombredegrupo</i> .
--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
<code>--userName</code>	Nombre de un usuario. Use el formato <i>dominio\nombredeusuario</i> .
<code>--groupName</code>	Nombre de un grupo. Use el formato <i>dominio\nombredegrupo</i> .
<code>--entitlementName</code>	(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](#)

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](#)

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](#)

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](#)

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](#)

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**

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**

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
<code>--userName</code>	Nombre del usuario del que desea ver las autorizaciones globales. Use el formato <i>dominio\nombredeusuario</i> . Esta opción muestra todas las autorizaciones globales asociadas al usuario especificado.
<code>--groupName</code>	Nombre del grupo del que desea ver las autorizaciones globales. Use el formato <i>dominio\nombredegrupo</i> . Esta opción muestra todas las autorizaciones globales asociadas al grupo especificado.
<code>--entitlementName</code>	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
<code>--userName</code>	Nombre de un usuario. Use el formato <i>dominio\nombredeusuario</i> .
<code>--groupName</code>	Nombre de un grupo. Use el formato <i>dominio\nombredegrupo</i> .
<code>--entitlementName</code>	(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
<code>--entitlementName</code>	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.
<code>--userName</code>	Nombre del usuario cuyo sitio desea incluir en la lista. Use el formato <i>dominio\nombredeusuario</i> .

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

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

- **Activar un certificado pendiente**

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
```