

Uso de HTML Access

VMware Horizon HTML Access 4.5

VMware Horizon 7 7.2



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 © 2013-2017 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Usar HTML Access 5

1 Instalación y configuración 6

- Requisitos del sistema para HTML Access 6
- Preparar el servidor de conexión y los servidores de seguridad para HTML Access 8
 - Reglas de firewall de HTML Access 10
- Configurar View para eliminar credenciales de la caché 10
- Preparar escritorios, grupos y granjas para HTML Access 11
- Configurar los agentes HTML Access para usar nuevos certificados SSL 13
 - Agregar el complemento del certificado a MMC en un escritorio de View 14
 - Importar un certificado para el agente HTML Access al almacén de certificados de Windows 15
 - Importar certificados raíz e intermedio para el agente HTML Access 16
 - Configurar la huella digital de certificado en el Registro de Windows 16
- Configurar los agentes HTML Access para usar conjuntos de cifrado específicos 17
- Configurar iOS para usar certificados firmados por una entidad de certificación 18
- Actualizar el software de HTML Access 18
- Desinstalar HTML Access del servidor de conexión de View 19
- Datos recopilados por VMware 19

2 Configurar HTML Access para usuarios finales 21

- Configurar la página del portal web de VMware Horizon para los usuarios finales 21
- Utilizar URI para configurar clientes web de HTML Access 25
 - Sintaxis para crear URI para HTML Access 25
 - Ejemplos de URI 28
- Configuración de las directivas de grupo de HTML Access 31

3 Usar una aplicación o un escritorio remotos 32

- Matriz de compatibilidad de funciones 33
- Internacionalización 34
- Conectarse a una aplicación o escritorio remotos 34
 - Confiar en un certificado raíz autofirmado 36
- Conectarse a un servidor en el modo Workspace ONE 37
- Utilizar la función Acceso sin autenticar para conectarse a aplicaciones remotas 38
- Combinaciones de teclas de método abreviado 39
- Teclados internacionales 43
- Resolución de pantalla 43
- Decodificación H.264 44
- Establecer la zona horaria 45

Utilizar la barra lateral	45
Utilizar varios monitores	49
Usar la sincronización PPP	50
Sonido	51
Copiar y pegar texto	51
Usar la función de copiar y pegar	52
Transferir archivos entre el cliente y un escritorio remoto	54
Descargar archivos de un escritorio en el cliente	54
Cargar archivos del cliente a un escritorio	55
Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos	55
Cerrar sesión o desconectarse	56
Restablecer un escritorio remoto o aplicaciones remotas	57
Reiniciar un escritorio remoto	58

Usar HTML Access

Esta guía, *Usar HTML Access*, proporciona información sobre la instalación y el uso de la función HTML Access de VMware Horizon™ 7 para conectarse a escritorios virtuales sin la necesidad de instalar ningún software en el sistema cliente.

Este documento incluye información sobre los requisitos del sistema e instrucciones para instalar el software de HTML Access en un servidor de View y en una máquina virtual del escritorio remoto para que los usuarios finales puedan usar un navegador web para acceder a los escritorios remotos.

Importante Esta información está destinada a administradores que ya tienen experiencia utilizando View y VMware vSphere. Si es un usuario sin experiencia en el uso de View, es posible que tenga que consultar las instrucciones paso a paso de los procedimientos básicos en los documentos *Instalación de View* y *Administración de View*.

Instalación y configuración

La configuración de una implementación de View para HTML Access incluye la instalación de HTML Access en el servidor de conexión de View, la apertura de los puertos necesarios y la instalación también del componente HTML Access en la máquina virtual del escritorio remoto.

Los usuarios finales pueden acceder entonces a los escritorios remotos abriendo un navegador compatible y escribiendo la URL del servidor de conexión de View.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema para HTML Access](#)
- [Preparar el servidor de conexión y los servidores de seguridad para HTML Access](#)
- [Configurar View para eliminar credenciales de la caché](#)
- [Preparar escritorios, grupos y granjas para HTML Access](#)
- [Configurar los agentes HTML Access para usar nuevos certificados SSL](#)
- [Configurar los agentes HTML Access para usar conjuntos de cifrado específicos](#)
- [Configurar iOS para usar certificados firmados por una entidad de certificación](#)
- [Actualizar el software de HTML Access](#)
- [Desinstalar HTML Access del servidor de conexión de View](#)
- [Datos recopilados por VMware](#)

Requisitos del sistema para HTML Access

Con HTML Access, un navegador compatible es el único software que necesita el sistema cliente. La implementación de View debe cumplir algunos requisitos de software.

Nota A partir de la versión 7.0, View Agent pasa a ser Horizon Agent.

Sistemas cliente o de navegador

Navegador	Versión
Chrome	57, 58
Internet Explorer	11
Safari	9, 10
Safari en dispositivos móviles	iOS 9, iOS 10

Navegador	Versión
Firefox	52, 53
Microsoft Edge	38, 40

Sistemas operativos cliente

Sistema operativo	Versión
Windows	7 SP1 (32-y 64 bits)
Windows	8.x (32 y 64 bits)
Windows	10 (32 y 64 bits)
Mac OS X	10.11 (El Capitan)
macOS	10.12.x (Sierra)
iOS	9
iOS	10
Chrome OS	28.x y versiones posteriores

Escritorios remotos

HTML Access necesita Horizon Agent 7.0 o versiones posteriores y es compatible con todos los sistemas operativos de escritorio que admite Horizon 7.0. Para obtener más información, consulte el tema "Sistemas operativos compatibles con Horizon Agent" de la versión 7.0 o posterior de *Instalación de View*.

Configuración de grupo

HTML Access necesita la siguiente configuración de grupo en Horizon Administrator:

- La configuración **Resolución máxima de los monitores** debe ser una resolución de **1920 x 1200** o superior para que el escritorio remoto tenga al menos 17,63 MB de RAM de vídeo.

Si tiene previsto utilizar aplicaciones 3D o los usuarios finales utilizan un Macbook con pantalla Retina o un Chromebook Pixel de Google, consulte [Resolución de pantalla](#).

- La opción **HTML Access** debe estar habilitada.

Las instrucciones de configuración se encuentran en [Preparar escritorios, grupos y granjas para HTML Access](#).

Servidor de conexión

Se debe instalar en el servidor el servidor de conexión con la opción HTML Access.

Al instalar el componente HTML Access, la regla del **servidor de conexión de VMware Horizon View (integrado)** está habilitada en el firewall de Windows para que este se configure automáticamente y se permita el tráfico entrante al puerto TCP 8443.

Servidor de seguridad

Se debe instalar la misma versión que tenga el servidor de conexión en el servidor de seguridad.

Si los sistemas cliente se conectan desde fuera del firewall corporativo, VMware le recomienda que use un servidor de seguridad. Con un servidor de seguridad, los sistemas cliente no necesitarán una conexión VPN.

Nota Un único servidor de seguridad puede admitir hasta 800 conexiones simultáneas a clientes web.

Firewalls de terceros

Agregue reglas para permitir el siguiente tráfico:

- Servidores (como servidores de seguridad, de réplicas e instancias del servidor de conexión): tráfico entrante al puerto TCP 8443.
- Máquinas virtuales de escritorios remotos: tráfico entrante (de servidores) al puerto TCP 22443.

Protocolo de visualización para Horizon

VMware Blast

Cuando utilice un navegador web para acceder a un escritorio remoto, se utiliza el protocolo VMware Blast en lugar del protocolo PCoIP o Microsoft RDP. VMware Blast utiliza HTTPS (HTTP sobre SSL/TLS).

Preparar el servidor de conexión y los servidores de seguridad para HTML Access

Los administradores deben realizar tareas específicas para permitir que los usuarios finales puedan conectarse a aplicaciones y escritorios remotos mediante un navegador web.

Antes de que los usuarios finales puedan conectarse al servidor de conexión o a un servidor de seguridad y acceder a un escritorio remoto, debe instalar el servidor de conexión con el componente HTML Access e instalar los servidores de seguridad.

A continuación, le presentamos una lista de comprobación de las tareas que debe realizar para usar HTML Access:

- 1 Instale el servidor de conexión con la opción HTML Access en el servidor o los servidores que compondrán un grupo replicado de servidores de conexión.

De forma predeterminada, el componente HTML Access ya está seleccionado en el instalador. Para obtener instrucciones sobre la instalación, consulte el documento *Instalación de View*.

Nota Para comprobar si el componente HTML Access está instalado, puede abrir el applet Desinstalar un programa, en el sistema operativo Windows y busque View HTML Access en la lista.

- 2 Si usa servidores de seguridad, instale el servidor de seguridad.

Para obtener instrucciones sobre la instalación, consulte el documento *Instalación de View*.

Importante La versión del servidor de seguridad debe coincidir con la del servidor de conexión.

- 3 Compruebe que cada instancia del servidor de conexión o del servidor de seguridad cuenten con un certificado de seguridad que se pueda verificar completamente con el nombre de host que introdujo en el navegador.

Para obtener más información, consulte *Instalación de View*.

- 4 Para usar una autenticación en dos fases, como autenticaciones RSA SecurID o RADIUS, compruebe que esta función esté habilitada en el servidor de conexión.

Para obtener más información, consulte los temas relacionados con la autenticación en dos fases en el documento sobre *administración de View*.

Importante Si habilita la opción **Ocultar la lista de dominios en la interfaz de usuario del cliente** y selecciona la autenticación de dos fases (RSA SecureID o RADIUS) para la instancia del servidor de conexión, no exija que coincidan los nombres de usuarios de Windows. Si exige que coincidan los nombres de usuarios de Windows, se impide a los usuarios que introduzcan información de dominio en el cuadro de texto del nombre de usuario y siempre se producirá un error al iniciar sesión. Para obtener más información, consulte los temas relacionados con la autenticación en dos fases en el documento sobre *administración de View*.

- 5 Si usa un firewall de terceros, configure las reglas para que permitan el tráfico entrante al puerto TCP 8443 en todos los servidores de seguridad y hosts del servidor de conexión en un grupo replicado y configure una regla para permitir el tráfico entrante (desde los servidores View) al puerto TCP 22443 en los escritorios remotos del centro de datos. Si desea obtener más información, consulte [Reglas de firewall de HTML Access](#).
- 6 Para proporcionar a los usuarios acceso sin autenticar a las aplicaciones publicadas en Horizon Client, debe habilitar esta función en el servidor de conexión. Para obtener más información, consulte los temas relacionados con el acceso sin autenticar en el documento *Administración de View*.

Después de instalar todos los servidores, en Horizon Administrator, verá que la opción **Puerta de enlace segura de Blast** está habilitada en las instancias de los servidores de seguridad y de los servidores de conexión en las que se aplican. Del mismo modo, la opción **URL externa de Blast** se configura automáticamente para usar la puerta de enlace segura de Blast en las instancias de los servidores de seguridad y de los servidores de conexión en las que se aplican. De forma predeterminada, la URL incluye el FQDN de la URL externa del túnel seguro y el número del puerto predeterminado, 8443. La URL debe contener el FQDN y el número de puerto que un sistema cliente puede usar para alcanzar el host del servidor de conexión o el host del servidor de seguridad. Para obtener más información, consulte cómo configurar URL externas en una instancia del servidor de conexión, en la documentación *Instalación de View*.

Nota Puede utilizar HTML Access con VMware Workspace ONE para permitir a los usuarios conectarse a sus escritorios a través de un navegador compatible con HTML5. Si desea obtener información sobre cómo instalar Workspace ONE y configurarlo para su uso con el servidor de conexión, consulte la documentación de Workspace ONE. Para obtener información sobre cómo emparejar el servidor de conexión con un servidor de autenticación SAML, consulte el documento *Administración de View*.

Reglas de firewall de HTML Access

Si desea permitir a los navegadores web cliente que usen HTML Access para establecer conexiones con los servidores de seguridad, las instancias del servidor de conexión de View y los escritorios remotos, los firewalls deben permitir el tráfico de entrada en ciertos puertos TCP.

Las conexiones de HTML Access deben usar HTTPS y no se permiten conexiones HTTP.

De forma predeterminada, cuando instala una instancia del servidor de conexión de View o del servidor de seguridad, se habilita la regla **Servidor de conexión de VMware Horizon View (integrado en Blast)** en el Firewall de Windows, por lo que dicho firewall se configura automáticamente para permitir el tráfico de entrada al puerto TCP 8443.

Tabla 1-1. Reglas de firewall de HTML Access

Origen	Puerto de origen predeterminado	Protocolo	Destino	Puerto de destino predeterminado	Notas
Navegador web cliente	TCP cualquier	HTTPS	Instancia del servidor de conexión de View o del servidor de seguridad	TCP 443	Para establecer la conexión inicial a Horizon, el navegador web de un dispositivo cliente se conecta a una instancia del servidor de conexión de Horizon o del servidor de seguridad en el puerto TCP 443.
Navegador web cliente	TCP cualquier	HTTPS	Puerta de enlace segura de Blast	TCP 8443	Después de establecer la conexión inicial a Horizon, el navegador web en un dispositivo cliente se conecta a la puerta de enlace segura de Blast en el puerto TCP 8443. La puerta de enlace segura de Blast se debe habilitar en una instancia del servidor de conexión de Horizon o del servidor de seguridad para permitir que se produzca esta segunda conexión.
Puerta de enlace segura de Blast	TCP cualquier	HTTPS	agente HTML Access	TCP 22443	Si la puerta de enlace segura de Blast está habilitada, después de que el usuario seleccione un escritorio remoto, dicha puerta de enlace se conecta al agente HTML Access en el puerto TCP 22443 del escritorio. Cuando se instala Horizon Agent, este componente agente está incluido.
Navegador web cliente	TCP cualquier	HTTPS	agente HTML Access	TCP 22443	Si la puerta de enlace segura de Blast no está habilitada, después de que el usuario seleccione un escritorio View, el navegador web del dispositivo cliente establece una conexión directa al agente HTML Access en el puerto TCP 22443 del escritorio. Cuando se instala Horizon Agent, este componente agente está incluido.

Configurar View para eliminar credenciales de la caché

Puede configurar View para eliminar de la caché las credenciales de un usuario cuando este cierre una pestaña que establezca la conexión a una aplicación o escritorio remoto o cuando cierre una pestaña que se conecte a la página de selección de aplicaciones y escritorios, en el cliente HTML Access.

Cuando esta función está deshabilitada (configuración predeterminada), las credenciales se mantienen en la caché.

Nota Si habilita esta función, las credenciales también se eliminan de la caché cuando un usuario actualiza la página de selección de la aplicación y del escritorio o la página de la sesión remota, o ejecuta un comando URI en la pestaña que contiene la sesión remota. Si el servidor presenta un certificado autofirmado, las credenciales se eliminan de la caché cuando un usuario inicie una aplicación o un escritorio remotos y acepte el certificado cuando aparece la advertencia de seguridad.

Requisitos previos

Para usar esta función es necesaria la versión 7.0.2 de Horizon 7 o versiones posteriores.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración global** y haga clic en **Editar** en el panel General.
- 2 Seleccione la casilla **Limpiar credencial al cerrar la pestaña para HTML Access**.
- 3 Haga clic en **Aceptar** para guardar los cambios.

Los cambios se aplicarán de forma inmediata. No es necesario que reinicie el servidor de conexión.

Preparar escritorios, grupos y granjas para HTML Access

Antes de que los usuarios finales puedan acceder a una aplicación o un escritorio remoto, los administradores pueden configurar las opciones de los grupos y las granjas e instalar Horizon Agent en máquinas virtuales del escritorio remoto y hosts RDS en el centro de datos.

El cliente HTML Access es una buena alternativa cuando el software Horizon Client no está instalado en el sistema cliente.

Nota El software Horizon Client ofrece más funciones y mejor rendimiento que el cliente HTML Access. Por ejemplo, con el cliente HTML Access, algunas combinaciones de teclas no funcionan en el escritorio remoto, pero sí lo hacen con Horizon Client.

Requisitos previos

- Compruebe que la infraestructura de vSphere y los componentes de Horizon cumplan con los requisitos del sistema para HTML Access.

Consulte [Requisitos del sistema para HTML Access](#).

- Compruebe que el componente HTML Access esté instalado con el servidor de conexión en el host o los hosts y que el firewall de Windows en las instancias del servidor de conexión y los servidores de seguridad permitan el tráfico entrante en el puerto TCP 8443.

Consulte [Preparar el servidor de conexión y los servidores de seguridad para HTML Access](#).

- Si usa un firewall de terceros, configure una regla para permitir el tráfico entrante desde los servidores Horizon al puerto TCP 22443 en escritorios de Horizon en el centro de datos.

- Compruebe que la máquina virtual que desea usar como origen de escritorio o host RDS tenga instalado el siguiente software: un sistema operativo compatible y VMware Tools.

Para obtener una lista de sistemas operativos compatibles, consulte [Requisitos del sistema para HTML Access](#).

- Familiarícese con los procedimientos para crear grupos y granjas, así como para autorizar usuarios. Consulte los temas sobre la creación de grupos y granjas en *Configurar escritorios y aplicaciones en View*.

- Para verificar que los usuarios finales puedan acceder a la aplicación o al escritorio remotos, compruebe que tenga instalado el software Horizon Client en un sistema cliente. Tiene que probar la conexión usando el software Horizon Client antes de intentar conectarse desde un navegador.

Para obtener instrucciones sobre la instalación de Horizon Client, consulte el sitio de documentación de Horizon Client en https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

- Compruebe que cuenta con uno de los navegadores compatibles para acceder a un escritorio remoto. Consulte [Requisitos del sistema para HTML Access](#).

Procedimiento

- 1 Para los escritorios y las aplicaciones, use Horizon Administrator para crear o editar grupos y granjas y habilite la opción **Permitir HTML Access en los escritorios y las aplicaciones de esta granja** en la configuración de la granja.
- 2 Para grupos de escritorios de sesión única, use Horizon Administrator para crear o editar el grupo de escritorios, por lo que el grupo se podrá usar con HTML Access.

- a Habilitar **HTML Access** en la configuración del grupo de escritorios.

La opción **HTML Access** no aparece en el asistente Agregar grupo de escritorios cuando crea grupos de escritorios RDS. En su lugar, habilite la opción **Permitir HTML Access en escritorios y aplicaciones de esta granja** cuando cree o edite la granja de hosts RDS.

- b En la configuración de los grupos, compruebe que el valor de **Resolución máxima de cualquier monitor** sea **1920x1200** o superior.

- 3 Después de crear los grupos, recomponerlos o actualizarlos para usar Horizon Agent con la opción **HTML Access**, use Horizon Client para iniciar sesión en un escritorio o una aplicación.

Con este paso, antes de intentar usar HTML Access, verifique que el grupo esté trabajando correctamente.

- 4 Abra un navegador compatible e introduzca una URL que lleve a la instancia del servidor de conexión.

Por ejemplo:

```
https://horizon.mycompany.com
```

No olvide introducir **https** en la URL.

- 5 En la página web que aparece, haga clic en **VMware Horizon HTML Access** e inicie sesión con el mismo proceso como lo haría con el software Horizon Client.
- 6 En el escritorio y la página de selección de la aplicación que aparece, haga clic en un icono al que conectarse.

En este momento, puede acceder a una aplicación o un escritorio remotos desde un navegador Web cuando usa un dispositivo cliente que no tiene o no puede tener el software Horizon Client instalado en el sistema operativo.

Pasos siguientes

Para obtener más seguridad, si las directivas de seguridad requieren que el agente Blast del escritorio remoto use un certificado SSL de una entidad de certificación, consulte [Configurar los agentes HTML Access para usar nuevos certificados SSL](#).

Configurar los agentes HTML Access para usar nuevos certificados SSL

Para cumplir las normas de seguridad o de la industria, puede sustituir los certificados SSL predeterminados que genera el agente HTML Access por certificados firmados por una entidad de certificación (CA).

Cuando instala el agente HTML Access en escritorios de View, el servicio del agente HTML Access crea certificados autofirmados y predeterminados. El servicio presenta los certificados predeterminados a navegadores que usan HTML Access para conectarse a View.

Nota En el sistema operativo invitado del escritorio de la máquina virtual, este servicio se denomina VMware Blast.

Para reemplazar los certificados predeterminados por los certificados firmados que obtiene de una CA, debe importar el certificado al almacén de certificados del equipo local Windows en cada escritorio de View. También debe configurar un valor de registro en cada escritorio que permita que el agente HTML Access use el nuevo certificado.

Si reemplaza los certificados predeterminados del agente HTML Access por certificados firmados por una CA, VMware le recomienda que configure un único certificado en cada escritorio. No configure un certificado firmado por una CA en una plantilla o una máquina virtual principal que use para crear un grupo de escritorios, ya que tendría como resultado cientos o miles de escritorios con certificados idénticos.

Procedimiento

1 [Agregar el complemento del certificado a MMC en un escritorio de View](#)

Antes de poder agregar certificados al almacén de certificados del equipo local Windows, debe agregar el complemento de certificados en Microsoft Management Console (MMC) en los escritorios de View donde el agente HTML Access está instalado.

2 [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#)

Para reemplazar un certificado predeterminado del agente HTML Access por un certificado firmado por una CA, debe importar este último al almacén de certificados del equipo local de Windows. Realice este procedimiento en cada escritorio donde el agente HTML Access está instalado.

3 [Importar certificados raíz e intermedio para el agente HTML Access](#)

Si los certificados raíz e intermedio de la cadena de certificados no se importan junto con el certificado SSL ya importado para el agente HTML Access, debe incluirlos en el almacén de certificados del equipo local Windows.

4 [Configurar la huella digital de certificado en el Registro de Windows](#)

Para permitir que HTML Access Agent use un certificado firmado por una entidad de certificación que se importó en el almacén de certificados de Windows, debe configurar la huella digital de certificado en una clave del Registro de Windows. Debe realizar este paso en cada escritorio en el que reemplace el certificado predeterminado por un certificado firmado por una entidad de certificación.

Agregar el complemento del certificado a MMC en un escritorio de View

Antes de poder agregar certificados al almacén de certificados del equipo local Windows, debe agregar el complemento de certificados en Microsoft Management Console (MMC) en los escritorios de View donde el agente HTML Access está instalado.

Requisitos previos

Compruebe que el complemento de certificados y MMC estén disponibles en el sistema operativo invitado de Windows donde está instalado el agente de HTML Access.

Procedimiento

- 1 En el escritorio de View, haga clic en **Inicio** y escriba **mmc.exe**.
- 2 En la ventana **MMC**, diríjase a **Archivo > Agregar o quitar complemento**.
- 3 En la ventana **Agregar o quitar complementos**, seleccione **Certificados** y haga clic en **Agregar**.
- 4 En la ventana **Complemento Certificados**, seleccione **Cuenta de equipo**, haga clic en **Siguiente**, seleccione **Equipo local** y, a continuación, haga clic en **Finalizar**.
- 5 En la ventana **Agregar o quitar complementos**, haga clic en **Aceptar**.

Pasos siguientes

Importe el certificado SSL en el almacén de certificados del equipo local Windows. Consulte [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#).

Importar un certificado para el agente HTML Access al almacén de certificados de Windows

Para reemplazar un certificado predeterminado del agente HTML Access por un certificado firmado por una CA, debe importar este último al almacén de certificados del equipo local de Windows. Realice este procedimiento en cada escritorio donde el agente HTML Access está instalado.

Requisitos previos

- Verifique que el agente HTML Access está instalado en el escritorio de View.
- Verifique que se copió el certificado firmado por una CA en el escritorio.
- Verifique que el complemento Certificado se agregó a MMC. Consulte [Agregar el complemento del certificado a MMC en un escritorio de View](#).

Procedimiento

- 1 En la ventana MMC del escritorio View, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal**.
- 2 En el panel Acciones, diríjase a **Más acciones > Todas las tareas > Importar**.
- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenado el certificado.
- 4 Seleccione el archivo del certificado y haga clic en **Abrir**.
Para visualizar el tipo de archivo del certificado, puede seleccionar su formato en el menú desplegable **Nombre de archivo**.
- 5 Escriba la contraseña de la clave privada que se incluye en el archivo del certificado.
- 6 Seleccione **Marcar esta clave como exportable**.
- 7 Seleccione **Incluir todas las propiedades ampliables**.
- 8 Haga clic en **Siguiente** y en **Finalizar**.

El nuevo certificado aparece en la carpeta **Certificados (equipo local) > Personal > Certificados**.

- 9 Verifique que el nuevo certificado contiene una clave privada.
 - a En la carpeta **Certificados (equipo local) > Personal > Certificados**, haga doble clic en el nuevo certificado.
 - b En la pestaña General del cuadro de diálogo Información del certificado, verifique que aparece la siguiente afirmación: Tiene una clave privada correspondiente a este certificado.

Pasos siguientes

Si es necesario, importe el certificado raíz y los certificados intermedios al almacén de certificados de Windows. Consulte [Importar certificados raíz e intermedio para el agente HTML Access](#).

Configure la clave de registro apropiada con la huella digital del certificado. Consulte [Configurar la huella digital de certificado en el Registro de Windows](#).

Importar certificados raíz e intermedio para el agente HTML Access

Si los certificados raíz e intermedio de la cadena de certificados no se importan junto con el certificado SSL ya importado para el agente HTML Access, debe incluirlos en el almacén de certificados del equipo local Windows.

Procedimiento

- 1 En la consola MMC del escritorio View, expanda el nodo **Certificados (equipo local)** y diríjase a la carpeta **Entidades de certificación raíz de confianza > Certificados**.
 - Si el certificado raíz está en esta carpeta y no existen certificados intermedios en la cadena de certificados, omita este procedimiento.
 - Si el certificado raíz no se encuentra en esta carpeta, comience en el paso 2.
- 2 Haga clic con el botón secundario en la carpeta **Entidades de certificación raíz de confianza > Certificados** y, a continuación, **Todas las tareas > Importar**.
- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenado el certificado CA raíz.
- 4 Seleccione el archivo del certificado CA raíz y haga clic en **Abrir**.
- 5 Haga clic en **Siguiente**, vuelva a hacer clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
- 6 Si el certificado del servidor lo firmó una CA intermedia, importe todos los certificados intermedios de la cadena de certificados al almacén de certificados del equipo local Windows.
 - a Diríjase a la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados**.
 - b Repita del paso 3 al 6 para cada certificado intermedio que se deba importar.

Pasos siguientes

Configure la clave de registro apropiada con la huella digital del certificado. Consulte [Configurar la huella digital de certificado en el Registro de Windows](#).

Configurar la huella digital de certificado en el Registro de Windows

Para permitir que HTML Access Agent use un certificado firmado por una entidad de certificación que se importó en el almacén de certificados de Windows, debe configurar la huella digital de certificado en una clave del Registro de Windows. Debe realizar este paso en cada escritorio en el que reemplace el certificado predeterminado por un certificado firmado por una entidad de certificación.

Requisitos previos

Compruebe que el certificado firmado por una entidad de certificación se importó en el almacén de certificados de Windows. Consulte [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#).

Procedimiento

- 1 En la ventana MMC del escritorio View en el que HTML Access Agent está instalado, diríjase a la carpeta **Certificados (equipo local) > Personal > Certificados**.
- 2 Haga doble clic en el certificado firmado por una entidad de certificación que importó en el almacén de certificados de Windows.
- 3 En el cuadro de diálogo Certificados, haga clic en la pestaña Detalles, desplácese hacia abajo y seleccione el icono **Huella digital**.
- 4 Copie la huella digital seleccionada en un archivo de texto.

Por ejemplo: 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

Nota Cuando copie la huella digital, no incluya el espacio inicial. Si lo pega accidentalmente con la huella digital en la clave del registro (paso 7), es posible que el certificado no se configure correctamente. Este problema se puede producir aunque el espacio inicial no se muestre en el cuadro de texto del valor del registro.

- 5 Inicie el editor del Registro de Windows en el escritorio en el que HTML Access Agent está instalado.
- 6 Diríjase a la clave del registro HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast \Config.
- 7 Modifique el valor SslHash y pegue la huella digital de certificado en el cuadro de texto.
- 8 Reinicie Windows.

Cuando un usuario se conecte a un escritorio a través de HTML Access, HTML Access Agent presenta el certificado firmado en el navegador del usuario.

Configurar los agentes HTML Access para usar conjuntos de cifrado específicos

Puede configurar el agente HTML Access para que use conjuntos de cifrado específicos en lugar de los predeterminados.

De forma predeterminada, el agente HTML Access necesita que las conexiones SSL entrantes usen una encriptación basada en ciertos cifrados para proporcionar una buena protección ante la falsificación y el espionaje telemático de la red. Puede configurar una lista alternativa de cifrados para que use el agente HTML Access. El conjunto de cifrados aceptados se expresa en formato OpenSSL, que se describe en <https://www.openssl.org/docs/manmaster/man1/ciphers.html>.

Procedimiento

- 1 Inicie el editor del Registro de Windows en el escritorio en el que HTML Access Agent está instalado.
- 2 Diríjase a la clave del registro HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast \Config.

- 3 Agregue un nuevo valor de cadena (REG_SZ), SslCiphers, y copie la lista de cifrados en formato OpenSSL en el cuadro de texto.
- 4 Reinicie el servicio VMware Blast para que se apliquen los cambios.

En el sistema operativo invitado Windows, el servicio del agente HTML Access se denomina VMware Blast.

Para volver a usar la lista de cifrados predeterminados, elimine el valor SslCiphers y reinicie el servicio VMware Blast. No elimine simplemente los datos del valor, ya que el agente HTML Access tratará entonces a todos los cifrados como no aceptables, según la definición del formato de la lista de cifrados OpenSSL.

Cuando se inicia el agente HTML Access, este escribe la definición del cifrado en el archivo de registro del servicio VMware Blast. Puede saber la lista de cifrados predeterminada actual si revisa los registros cuando se inicia el servicio VMware Blast sin el valor SslCiphers configurado en el Registro de Windows.

La definición del cifrado predeterminado del agente HTML Access puede cambiar de una versión a la siguiente para ofrecer una mayor seguridad.

Configurar iOS para usar certificados firmados por una entidad de certificación

Para utilizar HTML Access en dispositivos iOS, debe instalar certificados SSL que estén firmados por una entidad de certificación (CA) en lugar de los certificados SSL predeterminados, generados por el servidor de conexión de View o el agente HTML Access.

Para obtener más instrucciones, consulte el artículo sobre cómo configurar Horizon Client para iOS para que confíe en certificados intermedios y raíces en el documento *Instalación de View*.

Actualizar el software de HTML Access

En la mayoría de las versiones de HTML Access, la actualización simplemente implica actualizar los servidores de conexión y View Agent.

Cuando actualice HTML Access, compruebe que la versión correspondiente del servidor de conexión de View esté instalada en todas las instancias de un grupo replicado.

Cuando actualice el servidor de conexión, HTML Access se instala o se actualiza de forma automática.

Nota Para comprobar si el componente HTML Access está instalado, puede abrir el applet Desinstalar un programa del sistema operativo Windows y buscar HTML Access en la lista.

Desinstalar HTML Access del servidor de conexión de View

Para eliminar HTML Access, utilice el mismo método que para desinstalar cualquier otro software de Windows.

Procedimiento

- 1 En los hosts del servidor de conexión de View en los que esté instalado HTML Access, abra el applet Desinstalar un programa que proporciona el Panel de control de Windows.
- 2 Seleccione el programa VMware Horizon 7 HTML Access y haga clic en **Desinstalar**.
- 3 (opcional) En el firewall de Windows de ese host, compruebe que el puerto TCP 8443 ya no permita el tráfico entrante.

Pasos siguientes

No permita el tráfico entrante al puerto TCP 8443 en el firewall de Windows de cualquier servidor de seguridad conectado. En los firewalls de terceros, cambie la reglas para no permitir tráfico entrante al puerto TCP 8443 de todos los servidores de seguridad conectados y este host del servidor de conexión de View (si procede).

Datos recopilados por VMware

Si su compañía participa en el programa de mejora de la experiencia de cliente, VMware recopila datos de ciertos campos de los clientes. Los campos que contienen información personal son anónimos.

VMware recopila datos de los clientes para priorizar la compatibilidad entre el hardware y el software. Si un administrador de Horizon decidió participar en el programa de mejora de la experiencia de cliente, VMware recopila datos anónimos acerca de la implementación para mejorar la respuesta de VMware a los requisitos del cliente. No se recopila ningún dato que identifique a su organización. La información de los clientes se envía primero al servidor de conexión y después a VMware, junto con los datos de los servidores, de los grupos de escritorios y de los escritorios remotos.

Para participar en el programa de mejora de la experiencia de cliente de VMware, el administrador que instala el servidor de conexión puede registrarse mientras se ejecuta el asistente de instalación del servidor de conexión o, también, el administrador puede configurar esta opción en Horizon Administrator después de la instalación.

Tabla 1-2. Datos de los clientes recopilados para el programa de mejora de la experiencia de cliente

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Compañía que desarrolló la aplicación	<client-vendor>	No	VMware
Nombre de producto	<client-product>	No	VMware Horizon HTML Access
Versión del producto del cliente	<client-version>	No	4.5.0-número_compilación

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Arquitectura binaria del cliente	<client-arch>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ navegador ■ arm
Arquitectura nativa del navegador	<browser-arch>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Cadena agente del usuario del navegador	<browser-user-agent>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, like Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Cadena de la versión interna del navegador	<browser-version>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ 7.0.3 (para Safari), ■ 44.0 (para Firefox) ■ 13.10586 (para Edge)
Implementación del núcleo del navegador	<browser-core>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Si los navegadores se ejecutan en un dispositivo portátil	<browser-is-handheld>	No	true

Configurar HTML Access para usuarios finales

2

Es posible cambiar la apariencia de la página web que los usuarios finales verán cuando introduzcan la URL de HTML Access. También puede establecer directivas de grupo que controlen la calidad de la imagen y los puertos utilizados, entre otras opciones.

Este capítulo incluye los siguientes temas:

- [Configurar la página del portal web de VMware Horizon para los usuarios finales](#)
- [Utilizar URI para configurar clientes web de HTML Access](#)
- [Configuración de las directivas de grupo de HTML Access](#)

Configurar la página del portal web de VMware Horizon para los usuarios finales

Puede configurar esta página web para que muestre u oculte el icono para descargar Horizon Client o el icono para conectarse a un escritorio remoto a través de HTML Access. También puede configurar otros vínculos a esta página.

De forma predeterminada, este portal web muestra un icono para descargar e instalar Horizon Client nativo y otro icono para conectarse a través de HTML Access. El vínculo de descarga utilizado se determina a partir de los valores predeterminados definidos en el archivo `portal-links-html-access.properties`.

En algunos casos, sin embargo, es posible que desee que los vínculos dirijan a un servidor web interno o que quiera tener disponibles versiones específicas del cliente en su propio servidor. Puede reconfigurar la página del portal para que dirija a otra URL de descarga modificando el contenido del archivo `portal-links-html-access.properties`. Si ese archivo no está disponible o está vacío y existe el archivo `oslinks.properties`, el archivo `oslinks.properties` se utiliza para determinar el valor de vínculo del archivo de instalador.

El archivo `oslinks.properties` se instala en la carpeta *directorio-de-instalación\VMware\VMware View\Server\broker\webapps\portal\WEB-INF*. Si falta este archivo durante la sesión de HTML Access, el vínculo de descarga redirigirá a los usuarios de forma predeterminada a <https://www.vmware.com/go/viewclients>. El archivo contiene los siguientes valores predeterminados:

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaip1jfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Puede crear vínculos de instalador para sistemas operativos de cliente específicos en el archivo `portal-links-html-access.properties` u `oslinks.properties`. Por ejemplo, si se dirige a la página del portal desde un sistema Mac OS X, aparece el vínculo del instalador Mac OS X nativo. En el caso de los clientes Windows o Linux, puede crear vínculos independientes para instaladores de 32 o 64 bits.

Importante Si actualiza desde el servidor de conexión de View 5.x o una versión anterior y no cuenta con el componente HTML Access instalado y, además, editó previamente la página del portal para que descargue Horizon Client en su propio servidor, estas personalizaciones se podrían ocultar después de instalar el servidor de conexión de View 6.0 o una versión posterior. Con Horizon 6 o una versión posterior, el componente HTML Access se instala automáticamente durante una actualización del servidor de conexión de View.

Si ya instaló el componente HTML Access por separado para View 5.x, se conservan todas las personalizaciones que realizó para la página web. Si no cuenta con el componente HTML Access instalado, se ocultan todas las personalizaciones. Las personalizaciones de las versiones anteriores se encuentran en el archivo `portal-links.properties`, que ya no se utiliza.

Procedimiento

- 1 En el host del servidor de conexión de View, abra el archivo `portal-links-html-access.properties` con un editor de texto.

La ubicación de este archivo es *CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties*. Para los sistemas operativos Windows Server 2008, el directorio *CommonAppDataFolder* es *C:\ProgramData*. Para que aparezca la carpeta *C:\ProgramData* en el Explorador de Windows, debe usar el cuadro de diálogo Opciones de carpeta para mostrar las carpetas ocultas.

Si no existe el archivo `portal-links-html-access.properties` y existe el archivo `oslinks.properties`, abra el archivo `<directorio-de-instalación>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` para modificar las URL para usar los archivos de instalador específicos de descarga.

Nota Las personalizaciones de View 5.x y versiones anteriores se encuentran en el archivo `portal-links.properties`, que está en el mismo directorio `CommonAppDataFolder\VMware\VDM\portal\` que el archivo `portal-links-html-access.properties`.

2 Edite las propiedades de configuración para establecerlas correctamente.

De forma predeterminada, tanto el icono del instalador como el icono de HTML Access están habilitados y un vínculo lleva a la página de descargas del cliente en el sitio web de VMware. Para deshabilitar un icono, lo que supone que se elimine de la página web, configure la propiedad como `false`.

Nota El archivo `oslinks.properties` solo se puede utilizar para configurar los vínculos en los archivos de instalador específicos. No admite las otras opciones enumeradas debajo.

Opción	Configuración de propiedad
Deshabilitar HTML Access	<code>enable.webclient=false</code> Si esta opción aparece como <code>false</code> pero <code>enable.download</code> está configurada como <code>true</code> , se envía al usuario a una página web para que se descargue el instalador de Horizon Client nativo. Si ambas opciones aparecen como <code>false</code> , el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".
Deshabilitar la descarga de Horizon Client	<code>enable.download=false</code> Si esta opción aparece como <code>false</code> pero la opción <code>enable.webclient</code> está configurada como <code>true</code> , se envía al usuario a la página web de inicio de sesión de HTML Access. Si ambas opciones aparecen como <code>false</code> , el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".
Cambiar la URL de la página web para descargar Horizon Client	<code>link.download=https:// url_del_servidor_web</code> Use esta propiedad si piensa crear su propia página web.

Opción	Configuración de propiedad
Crear vínculos para instaladores específicos	<p>Los siguientes ejemplos muestran URL completas, pero puede usar URL relativas si coloca los archivos del instalador en el directorio downloads que se encuentra en el directorio C:\Program Files\VMware\VMware View\Server\broker\webapps\ del servidor de conexión de View, como se describe en el siguiente paso.</p> <ul style="list-style-type: none"> ■ Vínculo general para descargar el instalador: <div>link.download=https://server/downloads</div> ■ Instalador de Windows de 32 bits: <div>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</div> ■ Instalador para Windows de 64 bits: <div>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</div> ■ Instalador de Windows Phone: <div>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</div> ■ Instalador de Linux de 32 bits: <div>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</div> ■ Instalador de Linux de 64 bits: <div>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</div> ■ Instalador para Mac OS X: <div>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</div> ■ Instalador para iOS: <div>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</div> ■ Instalador para Android: <div>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</div> ■ Instalador de Chrome OS: <div>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</div>
Cambiar la URL para el vínculo Ayuda en la página de inicio de sesión	<p>link.help</p> <p>De forma predeterminada, este vínculo lleva a un sistema de ayuda alojado en el sitio web de VMware. El vínculo Ayuda aparece en la parte inferior de la página de inicio de sesión.</p>

- 3 Para hacer que los usuarios se descarguen instaladores de una ubicación diferente al sitio web de VMware, ponga los archivos del instalador en el servidor HTTP correspondiente.

Esta ubicación debe corresponderse con las URL que especificó en el archivo `portal-links-html-access.properties` o el archivo `oslinks.properties` durante el paso anterior. Por ejemplo, para situar los archivos en un directorio `downloads` en el host del servidor de conexión de View, use la siguiente ruta:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Los vínculos a los archivos del instalador pueden usar URL relativas con el formato `/downloads/nombre_archivo_instalador_de_cliente`.

- 4 Reinicie el servicio del componente web de View.

Utilizar URI para configurar clientes web de HTML Access

Con los identificadores uniformes de recursos (URI), puede crear un correo electrónico o una página web con vínculos en los que los usuarios finales hacen clic para iniciar HTML Access Web client, conectarse al servidor de conexión de View y abrir una aplicación o un escritorio específicos con opciones de configuración concretas.

Para simplificar el proceso de conexión a una aplicación o un escritorio remotos, cree vínculos web o de correo electrónico para los usuarios finales. Para ello, deberá crear URI que ofrezcan toda la información (o parte de ella) que se indica a continuación para que los usuarios finales no tengan que proporcionarla:

- Dirección del servidor de conexión de View
- Número de puerto del servidor de conexión de View
- Nombre de usuario de Active Directory
- Nombre de usuario de RSA SecurID o RADIUS (si es distinto al nombre de usuario de Active Directory)
- Nombre de dominio
- Nombre del escritorio o de la aplicación para mostrar
- Acciones (como navegar, restablecer e iniciar o cerrar sesión)

Sintaxis para crear URI para HTML Access

La sintaxis incluye una parte de ruta para especificar el servidor y, de forma opcional, una consulta para especificar un usuario, escritorio o aplicación, así como opciones de configuración o acciones.

Especificación de URI

Use la siguiente sintaxis para crear los URI destinados a iniciar los clientes web de HTML Access:

```
https://authority-part[/?query-part]
```

authority-part

Especifica la dirección del servidor y, de manera opcional, un número de puerto no predeterminado. Los nombres de servidor deben adaptarse a la sintaxis de DNS.

Para especificar un número de puerto, utilice la siguiente sintaxis:

```
server-address:port-number
```

query-part

Especifica las opciones de configuración que se van a utilizar o las acciones que se van a realizar. Las consultas no distinguen entre mayúsculas y minúsculas. Para utilizar varias consultas, utilice el signo et (&) entre ellas. Si se produce un conflicto entre ellas, se utilizará la última consulta de la lista. Utilice la siguiente sintaxis:

```
query1=value1[&query2=value2. ...]
```

Tenga en cuenta las siguientes instrucciones al crear la parte de la consulta:

- Si no usa al menos una de las consultas admitidas, se mostrará la página del portal web de VMware Horizon predeterminada.
- En la parte de la consulta, algunos caracteres especiales no son compatibles y debe usar el formato de codificación URL de la siguiente manera: para el signo almohadilla (#) use **%23**, para el signo porcentaje (%) use **%25**, para el signo et (&) use **%26**, para el signo arroba (@) use **%40** y para la barra diagonal inversa (\) use **%5C**.

Para obtener más información sobre la codificación URL, diríjase a http://www.w3schools.com/tags/ref_urlencode.asp.

- En la parte de la consulta, se debe codificar primero los caracteres que no sean ASCII según UTF-8 [STD63]. A continuación, cada octeto de la secuencia UTF-8 correspondiente se debe codificar con porcentaje para representarse como caracteres URI.

Para obtener información sobre la codificación de caracteres ASCII, consulte la referencia de codificación de URL de <http://www.utf8-chartable.de/>.

Consultas admitidas

En este tema, se incluyen las consultas admitidas para HTML Access Web client. Si crea URI para varios tipos de clientes (por ejemplo, clientes móviles y de escritorio), consulte el documento *Uso de VMware Horizon Client* correspondiente a cada tipo de sistema cliente.

action

Tabla 2-1. Valores que se pueden utilizar con la consulta action

Valor	Descripción
browse	Muestra una lista de las aplicaciones y los escritorios disponibles y alojados en el servidor especificado. No tendrá que especificar un escritorio ni una aplicación al utilizar esta acción.
start-session	Inicia la aplicación o el escritorio especificados. Si no se proporciona ninguna consulta action y se facilita el nombre de la aplicación o el escritorio, start-session es la acción predeterminada.
reset	Cierra y reinicia el escritorio especificado. Se pierden los datos que no se hayan guardado. La acción de reiniciar un escritorio remoto es equivalente a pulsar el botón Reiniciar en un equipo físico. Esta acción no es válida para una aplicación.
logout	Cierra la sesión del usuario en el sistema operativo invitado del escritorio remoto. Esta acción no es válida para una aplicación.
restart	Cierra y vuelve a iniciar el escritorio principal una vez que el usuario confirma la solicitud de operación de reinicio. Esta acción no es válida para una aplicación.

applicationId

El nombre de la aplicación para mostrar. El nombre para mostrar es el que se especifica en Horizon Administrator al crear el grupo de aplicaciones. Si el nombre para mostrar contiene un espacio, el navegador usa %20 para representar el espacio.

args

Especifica los argumentos de la línea de comandos que se agregarán al iniciar una aplicación remota. Utilice la sintaxis `args=value`, en el que *value* es una cadena. Utilice la codificación con porcentajes para los siguientes caracteres:

- Para los dos puntos (:), utilice %3A.
- Para una barra diagonal inversa (\), utilice %5C.
- Para un espacio (), utilice %20.
- Para unas comillas dobles ("), use %22.

Por ejemplo, para especificar el nombre de archivo "My new file.txt" para la aplicación Notepad++, utilice %22My%20new%20file.txt%22.

desktopId

El nombre del escritorio para mostrar. El nombre para mostrar es el que se especifica en View Administrator al crear el grupo de escritorios. Si el nombre para mostrar contiene un espacio, el navegador usa %20 para representar el espacio.

domainName	El nombre de dominio NETBIOS asociado al usuario que se conecta a la aplicación o al escritorio remotos. Por ejemplo, use mycompany en lugar de mycompany.com.
tokenUserName	El nombre de usuario RSA o RADIUS. Utilice esta consulta solo si el nombre de usuario de RSA o RADIUS es diferente al de Active Directory. Si no especifica esta consulta y se necesita la autenticación RSA o RADIUS, se utilizará el nombre de usuario de Windows.
userName	El usuario de Active Directory que se conecta a la aplicación o al escritorio remotos. El nombre de usuario puede tener uno de los formatos siguientes: <ul style="list-style-type: none"> ■ <i>Nombre de usuario</i> ■ <i>nombre de dominio%5Cnombre de usuario</i> ■ nombre principal de usuario (UPN), es decir, <i>nombre de usuario@nombre de dominio</i>
unauthenticatedAccess Enabled	Si esta opción está establecida como true , la función Acceso sin autenticar está habilitada de forma predeterminada. Se inicia HTML Access Web client y aparece una cuenta de un usuario anónimo. Un ejemplo de sintaxis es unauthenticatedAccessEnabled=true .
unauthenticatedAccess Account	Establece la cuenta que se debe utilizar si la función Acceso sin autenticar está habilitada. Si la función Acceso sin autenticar está deshabilitada, esta consulta se ignora. Un ejemplo de sintaxis con la cuenta de usuario anonymous1 es unauthenticatedAccessAccount=anonymous1 .

Ejemplos de URI

Es posible crear botones o vínculos de hipertexto con un URI e incluir estos vínculos en un correo electrónico o en una página web. Los usuarios finales pueden hacer clic en estos vínculos para, por ejemplo, abrir una aplicación o un escritorio remotos con las opciones de inicio que especifique.

Ejemplos de sintaxis de URI

Cada ejemplo de URI aparece con una descripción sobre qué es lo que el usuario final ve después de hacer clic en el vínculo del URI. Las consultas no distinguen entre mayúsculas y minúsculas. Por ejemplo, puede usar **domainName** o **domainname**.

1 `https://horizon.mycompany.com/?domainName=finance&userName=fred`

HTML Access Web client se inicia y se conecta al servidor horizon.mycompany.com. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **fred** y el cuadro de texto **Dominio** se rellena con **finance**. El usuario solo debe proporcionar una contraseña.

2 `https://horizon.mycompany.com/?userName=finance%5Cfred`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **horizon.mycompany.com**. El usuario solo debe proporcionar una contraseña.

3 `https://horizon.mycompany.com/?userName=fred@finance`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **fred@finance**. El usuario solo debe proporcionar una contraseña.

4 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio cuyo nombre para mostrar es **Escritorio primario** y el usuario inicia sesión en el sistema operativo cliente.

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, se inicia la aplicación Bloc de notas.

6 `https://horizon.mycompany.com:7555/?desktopId=Primary%20Desktop`

Este URI tiene el mismo efecto que el ejemplo anterior, excepto que usa el puerto 7555 no predeterminado para el servidor de conexión. (El puerto predeterminado es 443). Dado que se proporciona un identificador del escritorio, este se inicia aunque la acción `start-session` no se incluya en el URI.

7 `https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop`

El URI especifica tanto una aplicación como un escritorio. Cuando especifica una aplicación y un escritorio, solo se inicia este último.

8 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

El cliente web HTML Access se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para restablecer el Escritorio primario.

Nota Esta acción solo está disponible si el administrador de Horizon permite a los usuarios finales restablecer sus equipos.

9 `https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22`

Abre Notepad++ en el servidor `horizon.mycompany.com` y envía el argumento `My new file.txt` al comando que inicia la aplicación. El nombre del archivo aparece entre comillas dobles porque contiene espacios.

10 `https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt`

Abre Notepad++ 12 en el servidor `horizon.mycompany.com` y envía el argumento `a.txt b.txt` al comando que inicia la aplicación. Dado que los argumentos no están entre comillas dobles, un espacio separa los nombres de los archivos y ambos archivos se abren de forma independiente en Notepad++.

Nota Las aplicaciones pueden utilizar los argumentos de la línea de comandos de forma diferente. Por ejemplo, si envía el argumento `a.txt b.txt` a WordPad, este último solo abrirá un archivo, `a.txt`.

11 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para reiniciar el Escritorio primario.

Nota Esta acción solo está disponible si el administrador de Horizon permite a los usuarios finales reiniciar sus equipos.

12 `https://horizon.mycompany.com/?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1`

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com` mediante la cuenta **anonymous_user1**.

Ejemplos de códigos HTML

Si lo desea, puede utilizar los URI para hacer que los botones y los vínculos de hipertexto se incluyan en correos electrónicos o en páginas web. Los siguientes ejemplos muestran cómo usar el URI en el primer ejemplo de URI para codificar un vínculo de hipertexto que aparece como **Test Link** y un botón que aparece como **TestButton**.

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

Configuración de las directivas de grupo de HTML Access

HTML Access usa el protocolo VMware Blast. Puede configurar las directivas de grupo de HTML Access al establecer las directivas de grupo del protocolo VMware Blast.

Para obtener más información, consulte "Configurar directivas para grupos de escritorios y aplicaciones" y "Configuración de la directiva VMware Blast" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Usar una aplicación o un escritorio remotos

3

El cliente proporciona una barra lateral de navegación con botones de la barra de herramientas para que pueda desconectarse fácilmente de una aplicación o un escritorio remotos. También puede hacer clic para enviar la acción equivalente de la combinación de teclas Ctrl+Alt+Supr.

Este capítulo incluye los siguientes temas:

- [Matriz de compatibilidad de funciones](#)
- [Internacionalización](#)
- [Conectarse a una aplicación o escritorio remotos](#)
- [Conectarse a un servidor en el modo Workspace ONE](#)
- [Utilizar la función Acceso sin autenticar para conectarse a aplicaciones remotas](#)
- [Combinaciones de teclas de método abreviado](#)
- [Teclados internacionales](#)
- [Resolución de pantalla](#)
- [Descodificación H.264](#)
- [Establecer la zona horaria](#)
- [Utilizar la barra lateral](#)
- [Utilizar varios monitores](#)
- [Usar la sincronización PPP](#)
- [Sonido](#)
- [Copiar y pegar texto](#)
- [Transferir archivos entre el cliente y un escritorio remoto](#)
- [Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos](#)
- [Cerrar sesión o desconectarse](#)
- [Restablecer un escritorio remoto o aplicaciones remotas](#)
- [Reiniciar un escritorio remoto](#)

Matriz de compatibilidad de funciones

Cuando accede a una aplicación o un escritorio remotos desde el cliente HTML Access basado en el navegador, algunas funciones no están disponibles.

Compatibilidad de funciones para escritorios de máquinas virtuales de usuario único

Tabla 3-1. Funciones admitidas por HTML Access

Función	Escritorio de Windows 7	Escritorio de Windows 8.x	Escritorio de Windows 10	Escritorio de Windows Server 2008 R2	Escritorio de Windows Server 2012 R2	Escritorio de Windows Server 2016
RSA SecurID o RADIUS	X	X	X	X	X	X
Single Sign-On	X	X	X	X	X	X
Protocolo de visualización RDP						
Protocolo de visualización PCoIP						
Protocolo de visualización de VMware Blast	X	X	X	X	X	X
Redireccionamiento USB						
Audio/vídeo en tiempo real (RTAV)	X	X	X	X	X	X
Wyse MMR						
Redireccionamiento multimedia (MMR) de Windows Media						
Impresión virtual						
Impresión según ubicación	X	X	X	X	X	X
Tarjetas inteligentes						
Varios monitores	X	X	X	X	X	X

Para las descripciones de estas funciones y sus limitaciones, consulte el documento acerca de *cómo planificar la arquitectura de View*.

Compatibilidad de funciones para escritorios basados en sesiones y aplicaciones alojadas en hosts RDS

Los hosts RDS son equipos servidores con Servicios de Escritorio remoto de Windows y View Agent instalados. Varios usuarios pueden tener sesiones de escritorio y de aplicaciones en un host RDS al mismo tiempo. Un host RDS puede ser un equipo físico o una máquina virtual.

Nota La siguiente tabla contiene filas únicamente para las funciones que están disponibles en hosts RDS si usa HTML Access. Existen funciones adicionales disponibles si usa Horizon Client instalado de forma nativa, como Horizon Client para Windows.

Tabla 3-2. Funciones compatibles con HTML Access para hosts RDS con View Agent 6.1.1 o posterior, o bien Horizon Agent 7.0 o posterior, instalados

Función	Host RDS con Windows Server 2008 R2	Host RDS con Windows Server 2012 o 2012 R2	Windows Server 2016
RSA SecurID o RADIUS	X	X	Horizon Agent 7.0.2 y posterior
Single Sign-On	X	X	Horizon Agent 7.0.2 y posterior
Protocolo de visualización de VMware Blast	X	X	Horizon Agent 7.0.2 y posterior
Impresión según ubicación	X (solo máquina virtual)	X (solo máquina virtual)	Horizon Agent 7.0.2 y posterior (solo máquina virtual)
Audio/vídeo en tiempo real (RTAV)	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.3 y posterior
Varios monitores (solo para escritorios basados en sesiones)	X	X	X

Para obtener información sobre las ediciones o service pack de cada sistema operativo invitado que son compatibles, consulte la información sobre sistemas operativos compatibles con Horizon Agent en el documento *Instalación de View*.

Internacionalización

La interfaz de usuario y la documentación están disponibles en inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español.

Para obtener más información sobre qué paquetes de idioma debe usar en el sistema cliente, el navegador y el escritorio remoto, consulte [Teclados internacionales](#).

Conectarse a una aplicación o escritorio remotos

Use las credenciales de Active Directory para conectarse a las aplicaciones y escritorios remotos para los que tenga autorización.

Requisitos previos

- Obtenga las credenciales de inicio de sesión, como el nombre de usuario y la contraseña de Active Directory, el nombre de usuario y el código de acceso de RSA SecurID o el nombre de usuario y el código de acceso de la autenticación RADIUS.
- Obtenga el nombre de dominio NETBIOS para iniciar sesión. Por ejemplo, puede usar mycompany en lugar de mycompany.com.

Procedimiento

- 1 Abra el navegador e introduzca la URL de la instancia del servidor de conexión.

En la URL, use **https** y el nombre de dominio completo, por ejemplo: `https://horizon.company.com`.

Las conexiones al servidor de conexión siempre usan SSL. El puerto predeterminado para las conexiones SSL es 443. Si el servidor de conexión no está configurado para utilizar el puerto predeterminado, utilice el formato que se muestra en este ejemplo: **horizon.company.com:1443**.

Aparece el portal web de VMware Horizon. De forma predeterminada, esta página muestra un icono para descargar e instalar Horizon Client nativo y otro icono para conectarse a través de HTML Access.

- 2 (Opcional) Seleccione la casilla de verificación **Hacer clic aquí para omitir esta pantalla y usar siempre HTML Access**.

Su selección se almacena en el almacenamiento local del navegador que esté actualmente en uso. La próxima vez que introduzca la URL de la instancia del servidor de conexión con el mismo tipo de navegador y el mismo equipo cliente, se le dirigirá directamente a la pantalla de inicio de sesión. Si utiliza un tipo de navegador diferente en el mismo equipo cliente o si utiliza el mismo tipo de navegador en un equipo cliente diferente, aparece el portal web de VMware Horizon. Borre la caché del navegador si desea que el portal web de VMware Horizon aparezca.

- 3 Haga clic en el icono **VMware Horizon HTML Access**.

- 4 En el cuadro de diálogo de inicio de sesión, si se le solicita las credenciales RSA SecurID o las credenciales de la autenticación RADIUS, introduzca el nombre de usuario y el código de acceso y, a continuación, haga clic en **Iniciar sesión**.

El código de acceso puede incluir tanto un PIN como el número generado en el token.

- 5 Si se le solicita por segunda vez las credenciales RSA SecurID o las credenciales de autenticación RADIUS, introduzca el siguiente número generado en el token.

No introduzca su PIN ni tampoco el mismo número generado que ya introdujo anteriormente. Si es necesario, espere hasta que se genere un número nuevo.

Este paso solo se solicita cuando introduce de forma errónea el primer código de acceso o cuando las opciones de configuración cambian en el servidor RSA.

6 En el cuadro de diálogo de inicio de sesión, introduzca sus credenciales de inicio de sesión.

- a En el cuadro de texto Nombre de usuario, introduzca su nombre de usuario válido de Active Directory con el formato *nombre de usuario, dominio\nombre de usuario*, o bien *nombre de usuario@dominio*.

Si el cuadro de texto Dominio está deshabilitado, debe utilizar el formato *dominio\nombre de usuario* o bien *nombre de usuario@dominio*.

- b Introduzca la contraseña.
- c (Opcional) Si el cuadro de texto Dominio está habilitado, seleccione un nombre de dominio, si aún no se rellenó correctamente.

Nota Para cancelar el proceso de inicio de sesión, haga clic en **Cancelar** antes de que dicho proceso finalice.

7 (opcional) Si necesita establecer manualmente la zona horaria que se utiliza en la aplicación o el escritorio remotos, haga clic en la barra de herramientas **Configuración** que se encuentra en la esquina superior derecha del escritorio y la pantalla para seleccionar aplicaciones. Desactive la opción **Establecer la zona horaria automáticamente** y seleccione una de las zonas horarias del menú desplegable. Consulte [Establecer la zona horaria](#).

8 (opcional) En la pantalla para seleccionar aplicaciones y escritorios, antes de seleccionar el elemento al que desea acceder, haga clic en la estrella gris que aparece dentro del icono de la aplicación o del escritorio para marcarlos como favoritos.

El icono de la estrella cambia de gris a amarillo. La próxima vez que inicie sesión, puede hacer clic en el icono de la estrella situado en la parte superior derecha de la ventana del navegador para mostrar únicamente los favoritos.

9 Haga clic en el icono de la aplicación o escritorio remotos al que desea acceder.

La aplicación o el escritorio remotos se muestran en el navegador. También está disponible una barra lateral de navegación. Puede hacer clic en la pestaña situada en el lado izquierdo de la ventana del navegador para mostrar la barra lateral. Puede usar esta barra lateral para acceder a otras aplicaciones y escritorios remotos, mostrar la ventana Configuración, copiar y pegar textos, entre otras acciones.

Pasos siguientes

Si, al conectarse a un escritorio o una aplicación, se desconecta y aparece una solicitud que le pide que haga clic en un vínculo para aceptar el certificado de seguridad, puede seleccionar si desea confiar en el certificado. Consulte [Confiar en un certificado raíz autofirmado](#).

Confiar en un certificado raíz autofirmado

En algunos casos, al conectarse a una aplicación o escritorio remotos por primera vez, el navegador le solicitará aceptar el certificado autofirmado usado por el equipo remoto. Debe confiar en el certificado previamente para poder establecer la conexión a la aplicación o escritorio remotos.

La mayoría de los navegadores le ofrecerán la opción de confiar siempre en el certificado autofirmado. Si no elige confiar siempre en el certificado, deberá verificarlo cada vez que reinicie el navegador. Si usa un navegador Safari, debe confiar siempre en el certificado de seguridad para establecer la conexión.

Procedimiento

- 1 Si el navegador presenta una advertencia sobre un certificado que no es de confianza o sobre una conexión que no es privada, examine el certificado para comprobar que coincide con el que usa su empresa.

Es posible que necesite ponerse en contacto con el administrador de Horizon para obtener más ayuda. Por ejemplo, en un navegador Chrome, es necesario que realice el siguiente procedimiento.

- a Haga clic en el icono de bloqueo en la barra de direcciones.
- b Haga clic en el vínculo **Información del certificado**.
- c Compruebe que el certificado coincida con el que usa su empresa.

Es posible que necesite ponerse en contacto con el administrador de Horizon para obtener más ayuda.

- 2 Acepte el certificado de seguridad.

Cada navegador tiene sus propias solicitudes para aceptar un certificado o confiar siempre en él. Por ejemplo, en un navegador Chrome, puede hacer clic en el vínculo **Opciones avanzadas** de la página del navegador y hacer clic en **Acceder a nombre del servidor (sitio no seguro)**.

En un navegador Safari, use el siguiente procedimiento para confiar siempre en el certificado.

- a Haga clic en el botón **Mostrar certificado** cuando aparezca el cuadro de diálogo de un certificado que no es de confianza.
- b Seleccione la casilla **Confiar siempre** y haga clic en **Continuar**.
- c Cuando se le solicite, proporcione su contraseña y haga clic en **Actualizar ajustes**.

Se inicia la aplicación o el escritorio remotos.

Conectarse a un servidor en el modo Workspace ONE

A partir de la versión 7.2 de Horizon 7, un administrador podrá habilitar el modo Workspace ONE en una instancia del servidor de conexión.

Cuando se habilita el modo Workspace ONE, solo podrá conectarse al servidor a través del portal web de Workspace ONE. Se le redirigirá al portal web de Workspace ONE si intenta conectarse al servidor a través de HTML Access. Después de conectarse al servidor a través del portal web de Workspace ONE, solo podrá iniciar aplicaciones y escritorios remotos a través del portal web de Workspace ONE.

Es posible que se produzcan los siguientes problemas cuando está habilitado el modo de Workspace ONE.

- No se puede conectar al servidor a través de HTML Access. Es posible que no pueda comunicarse con el servidor o que vea un mensaje que indica que el servidor espera recibir sus credenciales de inicio de sesión desde otra aplicación o servidor.
- Después de iniciar una aplicación o un escritorio a través del portal web de Workspace ONE, no podrá ver ni iniciar las aplicaciones o escritorios remotos en HTML Access.

Utilizar la función Acceso sin autenticar para conectarse a aplicaciones remotas

Un administrador de Horizon puede utilizar la función Acceso sin autenticar para crear usuarios de acceso sin autenticar y autorizar a dichos usuarios a utilizar las aplicaciones remotas en una instancia del servidor de conexión. Los usuarios de acceso sin autenticar pueden iniciar sesión en el servidor de forma anónima para conectarse a sus aplicaciones remotas.

Requisitos previos

- Realice las tareas administrativas descritas en [Preparar el servidor de conexión y los servidores de seguridad para HTML Access](#).
- Configurar usuarios de acceso sin autenticar en la instancia del servidor de conexión. Si desea obtener más información, consulte el tema sobre cómo proporcionar acceso sin autenticar para aplicaciones publicadas en el documento *Administración de View*.

Procedimiento

- 1 Abra el navegador. Utilice una de las siguientes sintaxis de URI para conectarse a la instancia del servidor de conexión que posee acceso a aplicaciones remotas sin autenticar.
 - `https://authority-part?unauthenticatedAccessEnabled=true`
 - `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

En las anteriores sintaxis de URI, *authority-part* especifica la dirección del servidor y, opcionalmente, un número de puerto no predeterminado. Los nombres de servidor deben adaptarse a una sintaxis de DNS. Para especificar un número de puerto, utilice la siguiente sintaxis: *dirección_de_servidor:número_de_puerto*. La cuenta de usuario de Acceso sin autenticar creada para iniciar sesión de forma anónima es *anonymous_account*.

Las conexiones al servidor de conexión siempre usan SSL. El puerto predeterminado para las conexiones SSL es 443. Si el servidor de conexión no está configurado para utilizar el puerto predeterminado, utilice el formato que se muestra en este ejemplo: **horizon.company.com:1443**.

- 2 (Opcional) Si no se especifica la consulta `unauthenticatedAccessAccount`, seleccione una cuenta de usuario de Acceso sin autenticar en el menú desplegable de **Cuenta de usuario**, si es necesario, y haga clic en **Enviar**.

Si solo una cuenta de usuario de Acceso sin autenticar está disponible, dicha cuenta se selecciona de forma predeterminada.

Se mostrará la ventana de selección de aplicaciones.

- 3 Haga clic en el icono de la aplicación remota a la que desea acceder.

La aplicación remota se muestra en el navegador. También está disponible una barra lateral de navegación. Puede hacer clic en la pestaña situada en el lado izquierdo del navegador para mostrar la barra lateral. Puede usar esta barra lateral para acceder a otras aplicaciones remotas, mostrar la ventana Configuración, copiar y pegar textos, entre otras acciones.

Nota No puede volver a conectarse a las sesiones sin autenticar de aplicaciones. Al desconectarse del cliente, el host RDS cierra la sesión del usuario local de forma automática.

Combinaciones de teclas de método abreviado

Independientemente del idioma que utilice, algunas combinaciones de teclas no se pueden enviar a la aplicación o escritorio remotos.

Los navegadores web permiten que se envíen algunas teclas presionadas y combinaciones de teclas al sistema de destino y al sistema cliente. Para otras teclas y combinaciones, la entrada se procesa únicamente de forma local y no se envía al sistema de destino. Las combinaciones de teclas que funcionan en el sistema dependen del software del explorador, del sistema operativo cliente y de la configuración del idioma.

Nota Si utiliza un equipo Mac, puede asignar la tecla Comando a la tecla Ctrl de Windows cuando use las combinaciones de teclas para seleccionar, copiar y pegar texto. Para habilitar esta función, puede hacer clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y activar **Habilitar Comando-A, Comando-C, Comando-V y Comando-X**. (Esta opción aparece en la ventana Configuración solo si utiliza un equipo Mac.)

Las siguientes teclas y combinaciones del teclado no suelen funcionar en escritorios remotos:

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Tecla Comando
- Alt+Entrar

- **Ctrl+Alt+cualquier_tecla**

Importante Para usar Ctrl+Alt+Supr, use el botón de la barra de herramientas **Enviar Ctrl+Alt+Supr**, situado en la parte superior de la barra lateral.

- Bloq mayús+*tecla_modificadora* (como Alt o Mayús)
- Teclas de funciones, si utiliza un equipo Chromebook
- Combinaciones de teclas de Windows

Las siguientes combinaciones de teclas de Windows no funcionan en los escritorios remotos si habilita la tecla Windows en los escritorios. Para habilitarla, puede hacer clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y activar **Habilitar la tecla Windows para los escritorios**.

Importante Después de activar **Habilitar la tecla Windows para los escritorios**, debe presionar Ctrl+Win (en sistemas Windows), Ctrl+Comando (en sistemas Mac) o Ctrl+Tecla de búsqueda (en sistemas Chromebook) para simular la acción de pulsar la tecla Windows.

Estas combinaciones de teclas no funcionan en aplicaciones remotas proporcionadas por hosts RDS. Funcionan tal y como se describe para los escritorios basados en sesiones y escritorios de usuario único Windows Server 2008 R2 y Windows Server 2012 R2 , proporcionados por un host RDS.

Algunas combinaciones de teclas que funcionan en escritorios remotos con sistemas operativos Windows 8.x o Windows Server 2012 R2 no funcionan en escritorios remotos con sistemas operativos Windows 7, Windows Server 2008 R2 o Windows 10.

Tabla 3-3. Combinaciones de teclas de Windows para escritorios remotos con Windows 10

Teclas	Acción	Limitaciones
Win	Abrir o cerrar Inicio.	
Win+A	Abrir Centro de actividades.	
Win+E	Abrir Explorador de archivos.	
Win+G	Abrir la barra de juegos cuando hay uno abierto.	
Win+H	Abrir el acceso a Compartir.	
Win+I	Abrir el acceso a Configuración.	
Win+K	Abrir la acción rápida Conectar.	
Win+M	Minimizar todas las ventanas.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+S	Abrir Buscar.	
Win+X	Abrir el menú Vínculo rápido .	
Win+, (coma)	Vista temporal del escritorio.	
Win+Pausa	Muestra el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook o Mac no cuentan con la tecla Pausa.

Teclas	Acción	Limitaciones
Win+Mayús+M	Restaurar las ventanas minimizadas en el escritorio.	No funciona en navegadores Safari.
Win+Alt+Num	Abrir el escritorio y la lista de accesos directos de la aplicación anclada en la barra de tareas en la posición indicada por el número.	No funciona en un equipo Chromebook.
Win+Intro	Abrir Narrador.	

Tabla 3-4. Combinaciones de teclas de Windows para escritorios remotos con Windows 8.x y Windows Server 2012 R2

Teclas	Acción	Limitaciones
Win+F1	Abrir Ayuda y soporte técnico de Windows.	No funciona en navegadores Safari.
Win	Mostrar u ocultar la pantalla Inicio.	
Win+B	Llevar el foco al área de notificaciones.	
Win+C	Abrir el panel Accesos.	
Win+D	Mostrar y ocultar el escritorio.	No funciona en navegadores Safari. Solución alternativa: presionar Comando-D en equipos Mac.
Win+E	Abrir Explorador de archivos.	
Win+H	Abrir el acceso a Compartir.	
Win+I	Abrir el acceso a Configuración.	
Win+K	Abrir el acceso a Dispositivos.	
Win+M	Minimizar todas las ventanas.	
Win+Q	Abrir el acceso a Buscar, para realizar búsquedas en cualquier lugar o dentro de la aplicación abierta, si la aplicación admite la búsqueda en ella.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+S	Abrir el acceso a Buscar para realizar búsquedas en Windows y en la Web.	
Win+X	Abrir el menú Vínculo rápido .	
Win+Z	Mostrar los comandos disponibles en la aplicación.	
Win+, (coma)	Mostrar el escritorio durante el tiempo que se mantengan pulsadas las teclas.	Nota No funciona en sistemas operativos Windows 2012 R2.
Win+Pausa	Muestra el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook o Mac no cuentan con la tecla Pausa.
Win+Mayús+M	Restaurar las ventanas minimizadas en el escritorio.	No funciona en navegadores Safari. Solución alternativa: presionar Comando-D en equipos Mac.
Win+Alt+Num	Abrir el escritorio y la lista de accesos directos de la aplicación anclada en la barra de tareas en la posición indicada por el número.	No funciona en un equipo Chromebook.
Win+Flecha arriba	Maximizar la ventana.	No funciona en un equipo Chromebook.

Teclas	Acción	Limitaciones
Win+Flecha abajo	Eliminar la aplicación actual de la pantalla o minimizar la ventana del escritorio.	No funciona en un equipo Chromebook.
Win+Flecha izquierda	Maximizar la ventana de la aplicación o del escritorio en el lado izquierdo de la pantalla.	No funciona en un equipo Chromebook.
Win+Flecha derecha	Maximizar la ventana de la aplicación o del escritorio en el lado derecho de la pantalla.	No funciona en un equipo Chromebook.
Win+Inicio	Minimizar todas las ventanas excepto la del escritorio activo (restaura todas las ventanas cuando se vuelve a pulsar Win+Inicio).	No funciona en navegadores Safari.
Win+Mayús+Flecha arriba	Ampliar la ventana del escritorio hasta la parte de arriba y de abajo de la pantalla.	No funciona en un equipo Chromebook.
Win+Mayús+Flecha abajo	Restaurar la ventana del escritorio de forma vertical, mientras se mantiene el ancho, después de pulsar Win+Mayús+Flecha arriba para ampliar la pantalla, o minimizar la ventana del escritorio activa.	No funciona en un equipo Chromebook.
Win+Intro	Abrir Narrador.	

Tabla 3-5. Combinaciones de teclas de Windows para escritorios remotos con Windows 7 y Windows Server 2008 R2

Teclas	Acción	Limitaciones
Win	Abrir o cerrar el menú Inicio.	
Win+Pausa	Muestra el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook o Mac no cuentan con la tecla Pausa.
Win+D	Mostrar y ocultar el escritorio.	No funciona en navegadores Safari. Solución alternativa: presionar Comando-D en equipos Mac.
Win+M	Minimizar todas las ventanas.	
Win+E	Abrir la carpeta de equipo.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+Flecha arriba	Maximizar la ventana.	No funciona en un equipo Chromebook.
Win+Flecha abajo	Minimizar la ventana.	No funciona en un equipo Chromebook.
Win+Flecha izquierda	Maximizar la ventana de la aplicación o del escritorio en el lado izquierdo de la pantalla.	No funciona en un equipo Chromebook.
Win+Flecha derecha	Maximizar la ventana de la aplicación o del escritorio en el lado derecho de la pantalla.	No funciona en un equipo Chromebook.
Win+Inicio	Minimizar todas las ventanas excepto la del escritorio activo.	No funciona en navegadores Safari.
Win+Mayús+Flecha arriba	Ampliar la ventana del escritorio hasta la parte de arriba y de abajo de la pantalla.	No funciona en un equipo Chromebook.
Win+G	Seleccionar entre los gadgets del escritorio en ejecución.	
Win+U	Abrir el Centro de accesibilidad.	

Teclados internacionales

Cuando utilice configuraciones regionales y teclados que no sean en idioma inglés, debe usar cierta configuración en el sistema cliente, el navegador y el escritorio remoto. Algunos idiomas necesitan que use un IME (editor de métodos de entrada) en el escritorio remoto.

Al tener instalados las configuraciones locales y los métodos de entrada correctos, puede introducir caracteres de los siguientes idiomas: inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español.

Tabla 3-6. Configuración del idioma de entrada necesaria

Idioma	Idioma de entrada en el sistema cliente local	¿IME necesario en el sistema cliente local?	Idioma de entrada y del explorador en el escritorio remoto	¿IME necesario en el escritorio remoto?
Inglés	Inglés	No	Inglés	No
Francés	Francés	No	Francés	No
Alemán	Alemán	No	Alemán	No
Chino (simplificado)	Chino (simplificado)	Modo de entrada inglés	Chino (simplificado)	Sí
Chino (tradicional)	Chino (tradicional)	Modo de entrada inglés	Chino (tradicional)	Sí
Japonés	Japonés	Modo de entrada inglés	Japonés	Sí
Coreano	Coreano	Modo de entrada inglés	Coreano	Sí
Español	Español	No	Español	No

Resolución de pantalla

Si Horizon Administrator configura un escritorio remoto con la cantidad correcta de RAM de vídeo, el cliente web puede cambiar el tamaño de un escritorio remoto para adaptarlo al tamaño de la ventana del navegador. La configuración predeterminada es 36 MB de RAM de vídeo, que es una cantidad bastante superior al mínimo requerido de 16 MB si no usa aplicaciones 3D.

Si usa un navegador o un dispositivo Chrome que tenga una resolución con alta densidad de píxeles, como un Macbook con Retina Display o un Google Chromebook Pixel, puede configurar la aplicación o el escritorio remotos para que usen dicha resolución. Active la opción **Modo de alta resolución** en la ventana Configuración, que se encuentra en la barra lateral. (Esta opción solo aparece en la ventana Configuración si utiliza una pantalla de alta resolución o una pantalla normal con una escala superior al 100 %.)

Para usar la función de procesamiento 3D, debe asignar suficiente VRAM en cada escritorio remoto.

- La función de gráficos acelerados por software, disponible con vSphere 5.0 o versiones posteriores, le permite utilizar aplicaciones 3D como, por ejemplo, los temas de Aero de Windows o Google Earth. Para utilizar estas funciones se necesitan entre 64 MB y 128 MB de VRAM.
- La función de gráficos acelerados por hardware compartida (vSGA), disponible con vSphere 5.1 o versiones posteriores, le permite utilizar aplicaciones 3D para actividades multimedia, de diseño y de modelado. Para utilizar esta función se necesitan entre 64 MB y 512 MB de VRAM. La cantidad predeterminada son 96 MB.
- La función de gráficos acelerados por el hardware dedicada (vDGA), disponible en vSphere 5.5 o versiones posteriores, asigna una GPU (unidad de procesamiento gráfico) física única en un host ESXi para una máquina virtual única. Use esta función si necesita gráficos de estación de trabajo acelerados por hardware de alta gama. Para utilizar esta función se necesitan entre 64 MB y 512 MB de VRAM. La cantidad predeterminada son 96 MB.

Cuando el procesamiento 3D está habilitado, el número máximo de monitores es 1 y la resolución máxima es 3840 x 2160.

De forma similar, si usa un navegador en un dispositivo que tenga una resolución con alta densidad de píxeles, como un Macbook con Retina Display o un Google Chromebook Pixel, debe asignar suficiente VRAM para cada escritorio remoto.

Importante El cálculo de la cantidad de VRAM que necesita para el protocolo de visualización VMware Blast es similar al cálculo de la cantidad de VRAM necesaria para el protocolo de visualización PCoIP. Para obtener más instrucciones, consulte la sección "Tamaño de RAM para configuraciones de monitores específicas al utilizar PCoIP", que se encuentra dentro del tema "Cómo calcular los requisitos de memoria para escritorios virtuales", en el documento *Planificación de la arquitectura de View*.

Descodificación H.264

Si utiliza un navegador Chrome, puede permitir la descodificación H.264 en el cliente HTML Access para las sesiones de aplicaciones y escritorios remotos.

Cuando permite la descodificación H.264, el cliente HTML Access usa la descodificación H.264 si el agente la admite. Si el agente no admite la descodificación H.264, el cliente HTML Access usa la descodificación JPEG/PNG.

Si está conectado a una aplicación o escritorio remotos, puede permitir la descodificación H.264 al activar la opción **Permitir la descodificación H.264** en la ventana Configuración, que se encuentra en la barra lateral. Debe desconectarse y volver a conectarse a la aplicación o escritorio remotos para que se aplique la nueva configuración.

Si no está conectado a una aplicación o escritorio remotos, puede hacer clic en el botón de la barra de herramientas **Configuración**, situado en la esquina superior derecha de la ventana de selección de aplicaciones y escritorios y activar la opción **Permitir la descodificación H.264** en la ventana Configuración. Se aplicará la nueva configuración en todas las sesiones que se conecten después de realizar los cambios.

Establecer la zona horaria

La zona horaria utilizada en una aplicación o escritorio remotos se establece automáticamente en la zona horaria de su máquina local. Sin embargo, al utilizar el cliente HTML Access, puede que necesite establecer manualmente la zona horaria si no se puede determinar correctamente debido a algunas directivas de horario de verano.

Para establecer manualmente la información de zona horaria correcta que se debe utilizar antes de conectarse a una aplicación o escritorio remotos, haga clic en el botón de la barra de herramientas **Configuración** que se encuentra en la esquina superior derecha de la pantalla de selección de aplicaciones y el escritorio. Desactive la opción **Establecer la zona horaria automáticamente** en la ventana Configuración y seleccione una de las zonas horarias del menú desplegable.

El valor que seleccione se guardará como su zona horaria preferida al conectarse a una aplicación o escritorio remotos.

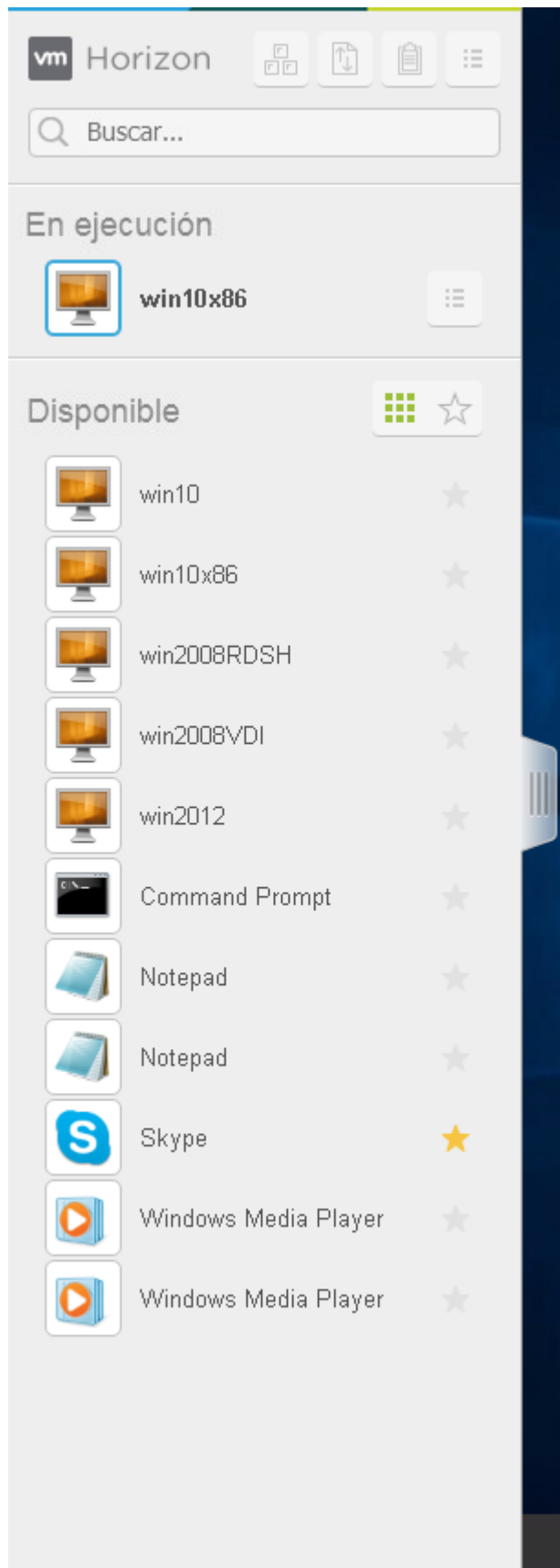
Si ya está conectado a una aplicación o escritorio remotos, vuelva a la pantalla de selección de aplicaciones y el escritorio para cambiar la configuración de zona horaria actual. La opción **Establecer la zona horaria automáticamente** no está disponible en la ventana Configuración a la que se puede acceder desde la barra lateral.

Utilizar la barra lateral

Una vez que se conecte a una aplicación alojada o un escritorio remoto, puede utilizar la barra lateral para iniciar otras aplicaciones y otros escritorios, cambiar de aplicaciones y escritorios en ejecución, así como llevar a cabo otras acciones.

Cuando acceda a una aplicación o un escritorio remotos, la barra lateral se mostrará en la parte izquierda de la pantalla. Haga clic en la pestaña de la barra lateral para mostrar u ocultar la barra lateral. También puede deslizar la pestaña hacia arriba y hacia abajo.

Figura 3-1. Barra lateral que se muestra al iniciar una aplicación o un escritorio remotos



Haga clic en la flecha de ampliación situada junto a una aplicación en ejecución para mostrar la lista de documentos abiertos en dicha aplicación. Sin embargo, debe tener en cuenta que si, por ejemplo, tiene dos documentos Excel abiertos en programas Excel independientes alojados en dos servidores diferentes, la aplicación Excel se incluirá dos veces en la lista **En ejecución** de la barra lateral.

En la barra lateral puede llevar a cabo varias acciones.

Tabla 3-7. Acciones de la barra lateral

Acción	Procedimiento
Mostrar la barra lateral	Cuando tenga una aplicación o un escritorio remotos abiertos, haga clic en la pestaña de la barra lateral. Cuando la barra lateral esté abierta, podrá seguir realizando acciones en la ventana del escritorio o de la aplicación.
Ocultar la barra lateral	Haga clic en la pestaña de la barra lateral.
Iniciar una aplicación o un escritorio remotos	Haga clic en el nombre de una aplicación o un escritorio de la sección Disponible de la barra lateral. Los escritorios aparecen primero en la lista.
Buscar una aplicación o un escritorio remotos	<ul style="list-style-type: none"> ■ Haga clic en el cuadro Buscar y escriba el nombre de la aplicación o del escritorio. ■ Para iniciar una aplicación o un escritorio, haga clic en el nombre de la aplicación o del escritorio en los resultados de la búsqueda. ■ Para volver a la vista inicial de la barra lateral, toque la X del cuadro de búsqueda.
Crear una lista de aplicaciones y escritorios favoritos	Haga clic en la estrella de color gris situada junto al nombre del escritorio o de la aplicación de la lista Disponible de la barra lateral. A continuación, puede hacer clic en el botón Mostrar favoritos de la barra de herramientas (icono de estrella) situado junto a Disponible para mostrar una lista que contenga solo los favoritos.
Cambiar de aplicaciones o escritorios	Haga clic en el nombre del escritorio o en el nombre del archivo de la aplicación en la lista En ejecución de la barra lateral.
Abrir el panel Copiar y pegar	Haga clic en el botón Copiar y pegar situado en la parte superior de la barra lateral. Utilice este botón para copiar texto de aplicaciones y copiar texto en ellas en su sistema cliente local. Si desea obtener más información, consulte Copiar y pegar texto . En Safari para iOS, este botón no está disponible porque la función de copiar y pegar no es compatible.
Abrir la ventana Transferencia de archivos	Haga clic el botón Transferencia de archivos situado en la parte superior de la barra lateral para descargar archivos del escritorio remoto o cargarlos a él. Para obtener más información, consulte Descargar archivos de un escritorio en el cliente y Cargar archivos del cliente a un escritorio .
Habilitar Comando-A, Comando-C, Comando-V y Comando-X	Esta opción aparece en la ventana Configuración solo si utiliza un equipo Mac. Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración . Cuando esta función está habilitada, la tecla Comando del equipo Mac se asigna a la tecla Ctrl en la aplicación o el escritorio remotos de Windows. Por ejemplo, al pulsar Comando-A en un teclado de Mac, se obtendrá el mismo efecto que al pulsar Ctrl+A en la aplicación o el escritorio remotos de Windows.

Acción	Procedimiento
Cerrar un escritorio en ejecución	<p>Haga clic en el botón Abrir menú situado junto al nombre del escritorio de la lista En ejecución de la barra lateral y seleccione la acción que desee:</p> <ul style="list-style-type: none"> ■ Seleccione Cerrar para desconectarse del escritorio sin cerrar sesión en el sistema operativo. Sin embargo, debe tener en cuenta que View Administrator puede configurar el escritorio para cerrar sesión de forma automática cuando se desconecte. En ese caso, los cambios que no se hayan guardado en las aplicaciones abiertas se perderán. ■ Seleccione Cerrar sesión para cerrar sesión en el sistema operativo y desconectarse del escritorio. Los cambios que no se hayan guardado en las aplicaciones abiertas se perderán.
Cerrar una aplicación en ejecución	<p>Haga clic en la X situada junto al nombre del archivo en el nombre de la aplicación de la lista En ejecución de la barra lateral. Haga clic en la X situada junto al nombre de la aplicación para salir de ella y cerrar todos los archivos abiertos de dicha aplicación. Se le solicitará que guarde los cambios realizados en los archivos.</p>
Restablecer un escritorio	<p>Haga clic en el botón Abrir menú situado junto al nombre del escritorio de la lista En ejecución de la barra lateral y seleccione Restablecer. Los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardar. Solo puede restablecer un escritorio si el administrador habilitó esta función.</p>
Reiniciar un escritorio	<p>Haga clic en el botón Abrir menú situado junto al nombre del escritorio de la lista En ejecución de la barra lateral y seleccione Reiniciar. El sistema operativo del escritorio normalmente le pide que guarde los datos que no haya guardado antes de reiniciar. Solo puede reiniciar un escritorio si el administrador habilitó esta función.</p>
Restablecer todas las aplicaciones en ejecución	<p>Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración y Restablecer todas las aplicaciones en ejecución. Los cambios que no se hayan guardado se perderán.</p>
Utilizar combinaciones de teclas que incluyan la tecla Windows	<p>Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Habilitar la tecla Windows para los escritorios. Si desea obtener más información, consulte Combinaciones de teclas de método abreviado.</p>
Enviar Ctrl+Alt+Supr al área de trabajo actual	<p>Haga clic en el botón Enviar Ctrl+Alt+Supr de la barra de herramientas situado en la parte superior de la barra lateral.</p>
Desconectarse del servidor	<p>Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral o en el logotipo de Horizon situado en la parte superior de la barra lateral y seleccione Cerrar sesión.</p>
Utilizar el modo de alta resolución en equipos con una pantalla de alta resolución (por ejemplo, un Macbook Pro con pantalla Retina)	<p>Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Modo de alta resolución.</p>
Permitir la decodificación H.264	<p>(Solo Chrome) Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Permitir la decodificación H.264. Si desea obtener más información, consulte Decodificación H.264.</p>
Utilizar varios monitores	<p>(Versión 55 de Chrome o posteriores) Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración de pantalla. Para obtener más información, consulte Utilizar varios monitores</p>

Acción	Procedimiento
Mostrar u ocultar el teclado en pantalla	(Solo Safari para iOS) Haga clic en el icono de teclado situado en la parte superior de la barra lateral. También puede mostrar u ocultar el teclado en pantalla. Para ello, toque la pantalla con tres dedos.
Mostrar temas de ayuda	Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral o en el logotipo de Horizon situado en la parte superior de la barra lateral y seleccione Ayuda .
Mostrar el cuadro Acerca de VMware Horizon	Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral o bien en el logotipo de Horizon situado en la parte superior de la barra lateral y seleccione Acerca de .

Utilizar varios monitores

Puede usar varios monitores en HTML Access Web client para mostrar una ventana del escritorio remoto con un navegador Chrome (versión 55 o posteriores).

Puede agregar hasta un monitor adicional a su monitor principal para mostrar la ventana actual del escritorio remoto al que está conectado. Por ejemplo, si dispone de tres monitores, puede especificar que la ventana del escritorio remoto solo aparezca en dos de esos monitores. Se deben seleccionar monitores adyacentes para la configuración de varios monitores. Los monitores pueden estar colocados uno junto al otro o bien apilados de forma vertical.

A partir de la versión 4.5 de HTML Access Web client, la sincronización PPP por dispositivo se aplica cuando se habilita la función de varios monitores. Si utiliza dos monitores que tienen diferentes configuraciones PPP, la configuración PPP del agente HTML Access se establece con el mismo valor PPP del monitor del equipo cliente que se usó para iniciar la sesión de HTML Access Web client.

Procedimiento

- 1 Inicie Horizon Client e inicie sesión en un servidor.
- 2 En la ventana de selección de aplicaciones y escritorios, haga clic en el icono del escritorio remoto al que desea acceder.
- 3 Para mostrar la barra lateral, haga clic en la pestaña de la barra lateral.
- 4 Haga clic en el botón **Abrir menú** de la barra de herramientas situado en la parte superior de la barra lateral y seleccione **Configuración de pantalla**.
- 5 En el cuadro de diálogo Configuración de pantalla, haga clic en **Agregar pantalla**.

Nota Si la ventana del navegador Selector de pantallas no aparece, agregue la dirección FQDN del servidor Horizon en la sección Excepciones de elementos emergentes de la ventana **Configuración de contenido** de su navegador.

- 6 Arrastre la ventana Selector de pantallas para que aparezca en la pantalla del otro monitor que desea utilizar.

El mensaje de la ventana del navegador Selector de pantallas cambiará y se agregará un icono gris rectangular.

- 7 En la ventana del navegador Selector de pantallas, haga clic en el icono del monitor **+** para confirmar que desea utilizar la pantalla del monitor actual.

El mensaje Esperando otras pantallas aparecerá en la pantalla del monitor actual y el icono gris de monitor de la ventana Configuración de pantalla de la pantalla principal cambiará a verde.

- 8 Haga clic en **Aceptar** en la ventana Configuración de pantalla una vez que agregue las pantallas del monitor que desee utilizar para la sesión.

Si la ventana Configuración de pantalla desaparece, el mensaje Esperando otras pantallas se borrará de la pantalla del monitor que no sea el principal y se mostrará en la ventana del escritorio remoto.

- 9 Para salir del modo de varios monitores, pulse Esc y haga clic en **Sí** en el cuadro de diálogo **Cerrar el modo de pantallas múltiples** para confirmar.

Nota Cada vez que tenga que utilizar la tecla Esc en el escritorio remoto, abra la barra lateral, haga clic en el botón **Abrir menú** de la barra de herramientas situado en la parte superior de la barra lateral y seleccione **Enviar ESC**.

Usar la sincronización PPP

La función de sincronización PPP asegura que la configuración PPP del escritorio remoto coincide con la configuración PPP del equipo cliente en las nuevas sesiones remotas. Cuando inicia una nueva sesión, Horizon Agent establece los valores PPP en el escritorio remoto para que coincida con el valor PPP del equipo cliente.

La función Sincronización PPP no puede cambiar la configuración PPP para las sesiones remotas activas. Si vuelve a conectarse a una sesión remota existente, la función de escala de pantalla ajusta la aplicación o escritorio remotos de forma apropiada.

La función Sincronización PPP se habilita si la opción Modo de alta resolución está deshabilitada en la ventana Configuración. A partir de la versión 4.5 de HTML Access, si un administrador deshabilita la opción de directiva de grupo **Sincronización PPP** de Horizon Agent, la función de sincronización de PPP se puede deshabilitar, pero no la función de Ajuste de escala de la pantalla. Debe cerrar sesión e iniciarla de nuevo para que se realicen los cambios en la configuración. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para utilizar la función Sincronización PPP, es necesario Windows 7 o versiones posteriores en los escritorios de una sesión única, Windows Server 2008 R2 o versiones posteriores para escritorios publicados y aplicaciones en hosts RDS, Horizon Agent 7.0.2 o versiones posteriores y HTML Access 4.4 o versiones posteriores.

A continuación le mostramos algunos consejos para usar la función Sincronización PPP:

- Si cambia la configuración PPP en el equipo cliente, deberá cerrar sesión y volverla a iniciar para que Horizon Client reconozca la nueva configuración PPP. Este requisito se aplica aunque el equipo cliente ejecute Windows 10.

- Si inicia una sesión remota en un equipo cliente que tenga una configuración PPP de más del 100% y utiliza la misma sesión en otro equipo cliente que tenga una configuración PPP diferente de más del 100%, debe cerrar sesión y volver a iniciarla en el segundo equipo cliente para hacer que la sincronización PPP funcione en dicho equipo.
- Aunque los equipos con Windows 10 Windows 8.x admitan distintas configuraciones PPP en los distintos monitores, la función Sincronización PPP utiliza el valor PPP que se configuró en el monitor del equipo cliente en el que se encuentra el navegador web que se utilizó para iniciar la sesión de cliente de HTML Access. HTML Access no admite diferentes configuraciones PPP en monitores diferentes.
- Si un administrador cambia el valor configurado para la directiva de grupo **Sincronización PPP** para Horizon Agent, debe cerrar sesión y volver a iniciarla para que se aplique la nueva configuración.
- Si desea sincronizar con otro monitor utilizando otra configuración PPP, debe cerrar sesión en el escritorio o la aplicación remotos, arrastrar al otro monitor el navegador web utilizado para iniciar la sesión de cliente de HTML Access y volver a iniciar sesión en la aplicación o el escritorio remotos para que las configuraciones PPP del sistema cliente y la aplicación o el escritorio remotos coincidan.

Sonido

Puede reproducir sonidos en las aplicaciones y los escritorios remotos, pero se aplican algunas limitaciones.

De forma predeterminada, la reproducción de sonidos está habilitada para las aplicaciones y los escritorios remotos, aunque View Administrator puede establecer una directiva para deshabilitar la reproducción de sonidos.

Tenga en cuenta las siguientes instrucciones:

- Para subir el volumen, use el control de sonido en el sistema cliente, no el control de sonido en la aplicación o escritorio remotos.
- De forma ocasional, se puede perder la sincronización del sonido con el vídeo.
- En condiciones de tráfico de red intenso o si los navegadores realizan un gran número de tareas (E/S), es posible que la calidad del sonido disminuya. En este sentido, algunos navegadores trabajan mejor que otros.

Copiar y pegar texto

Es posible realizar operaciones de copiado y pegado en las aplicaciones y los escritorios remotos. View Administrator puede establecer esta función para que sea posible realizar estas operaciones desde su sistema cliente a una aplicación o un escritorio remotos, así como desde una aplicación o un escritorio remotos a su sistema cliente, o ninguna o ambas posibilidades.

Los administradores configuran la posibilidad de copiar y pegar utilizando las directivas de grupo que pertenecen a View Agent o a Horizon Agent en los escritorios remotos. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#). Los administradores también pueden usar directivas de grupo para restringir los formatos del portapapeles durante operaciones de copiado y pegado. Debido a que HTML Access admite únicamente la transferencia de texto en el portapapeles, solo los filtros de texto funcionan con el cliente HTML Access. Para obtener más información sobre cómo usar las directivas de grupo para filtrar formatos del portapapeles, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Puede copiar hasta 1 MB de texto, incluidos los caracteres Unicode que no sean ASCII. Puede copiar texto de su sistema cliente a una aplicación o escritorio remotos, o viceversa, pero el texto pegado será texto sin formato.

No puede copiar y pegar gráficos. Tampoco puede copiar y pegar archivos entre un escritorio remoto y el sistema de archivos de su equipo cliente.

Nota La función para copiar y pegar no es compatible con iOS Safari.

Usar la función de copiar y pegar

Para copiar y pegar texto, debe usar el botón **Copiar y pegar** situado en la parte superior de la barra lateral.

Este procedimiento describe cómo usar la ventana Copiar y pegar para copiar texto desde el sistema cliente a una aplicación remota o cómo copiar texto desde una aplicación remota al sistema cliente local. Sin embargo, si copia y pega texto entre escritorios y aplicaciones remotas, puede realizar la acción como lo hace habitualmente y no es necesario usar la ventana Copiar y Pegar.

La ventana Copiar y pegar, que puede abrir con el botón situado en la parte superior de la barra lateral HTML Access, es necesaria únicamente para sincronizar el Portapapeles del sistema local con el Portapapeles del equipo remoto.

El texto en la ventana Copiar y pegar muestra uno de los siguientes mensajes para indicar en qué dirección el usuario puede copiar y pegar contenido.

- Use este panel para copiar y pegar contenido entre el cliente local y la aplicación o el escritorio remotos.
- Use el panel para copiar y pegar contenido desde el cliente local a la aplicación o el escritorio remotos.
- Use el panel para copiar y pegar contenido desde la aplicación o el escritorio remotos al cliente local.

Requisitos previos

Si utiliza un equipo Mac, compruebe que tiene habilitada la opción para asignar la tecla Comando a la tecla Ctrl de Windows cuando use las combinaciones de teclas para seleccionar, copiar y pegar texto. Haga clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y active **Habilitar Comando-A, Comando-C, Comando-V y Comando-X**. (Esta opción aparece en la ventana Configuración solo si utiliza un equipo Mac.)

El View Administrator debe mantener la directiva predeterminada en funcionamiento, lo que permite a los usuarios copiar desde sistemas cliente y pegar a aplicaciones y escritorios remotos, o bien debe configurar otra directiva que permita el copiado y el pegado. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#).

Procedimiento

- ◆ Siga estos pasos para copiar texto desde el sistema cliente a la aplicación o el escritorio remoto:
 - a Copie el texto en la aplicación cliente local.
 - b En el navegador, haga clic en la pestaña de la barra lateral de HTML Access para abrirla y, a continuación, haga clic en **Copiar y pegar**, en la parte superior de la barra lateral.

Aparece la ventana Copiar y pegar. Si el texto copiado anteriormente ya aparece en la ventana, este texto se reemplazará cuando pegue el nuevo texto copiado.
 - c Pulse Ctrl+V (o Comando-V en equipos Mac) para pegar el texto dentro de la ventana Copiar y pegar.

Aparece brevemente el siguiente mensaje: "Portapapeles remoto sincronizado."
 - d Haga clic en la aplicación remota en la que desea pegar el texto y pulse Ctrl+V.

El texto se pega en la aplicación remota.
- ◆ Siga estos pasos para copiar texto desde la aplicación o el escritorio remotos al sistema cliente:
 - a Copie el texto en la aplicación remota.
 - b En el navegador, haga clic en la pestaña de la barra lateral de HTML Access para abrirla y, a continuación, haga clic en **Copiar y pegar**, en la parte superior de la barra lateral.

La ventana Copiar y pegar aparece con el texto ya pegado. Aparece brevemente el siguiente mensaje: "Portapapeles remoto sincronizado".
 - c Haga clic en la ventana Copiar y pegar y pulse Ctrl+C (o Comando-C en equipos Mac) para volverlo a pegar.

Al realizar esta acción no se seleccionará el texto y tampoco lo puede seleccionar usted mismo. Aparece brevemente el siguiente mensaje: "Copiado del panel del portapapeles".
 - d En el sistema cliente, haga clic donde desee pegar el texto y pulse Ctrl+V.

El texto se pega en la aplicación del sistema cliente.

Transferir archivos entre el cliente y un escritorio remoto

Con la función de transferencia de archivos, puede transferir (cargar y descargar) archivos entre el cliente y un escritorio remoto. No se admite la transferencia de archivos entre las aplicaciones.

El administrador de Horizon puede configurar la capacidad de permitir, prohibir o permitir solo en una dirección la transferencia de archivos al modificar la configuración de la directiva de grupo **Configurar la transferencia de archivos** del protocolo de VMware Blast. La opción predeterminada es únicamente la carga. Si el valor **Deshabilitar tanto cargar como descargar** está seleccionado en la opción de la directiva de grupo **Configurar la transferencia de archivos** para el protocolo VMware Blast, el botón **Transferencia de archivos** está deshabilitado. Si el valor **Solo carga de archivos habilitada** está seleccionado, solo se muestra la pestaña **Cargar** en la ventana de diálogo **Transferir archivos**. Si el valor **Solo descarga de archivos habilitada** está seleccionado, solo se muestra la pestaña **Descargar** en la ventana de diálogo **Transferir archivos**. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#).

Puede descargar un archivo que tenga como máximo 500 MB de tamaño y cargar un archivo de hasta 2 GB de tamaño. En Internet Explorer 11 de 32 bits, es posible que se produzca un error al descargar un archivo con un tamaño superior a 300 MB. Para solucionar este problema, ejecute Internet Explorer 11 en modo de 64 bits.

No puede descargar o cargar carpetas ni archivos que tengan un tamaño cero.

Safari en iOS y Safari 8 no permiten cargar ni descargar. Safari 9 y sus versiones posteriores no admiten la descarga.

Si la transferencia de archivos está en curso en una sesión de escritorio, el usuario abre una conexión en un segundo escritorio y se muestra una advertencia de seguridad (esto puede suceder si no se instaló ningún certificado válido, por ejemplo), si ignora esta advertencia y continúa con el proceso de conexión del segundo escritorio, se anulará la transferencia de archivos en la primera sesión del escritorio. Este es un comportamiento previsto.

Nota La capacidad de descarga se ve afectada por la configuración de la directiva de grupo del redireccionamiento del portapapeles. Si el redireccionamiento del portapapeles está deshabilitado del servidor al cliente, la descarga de archivos también lo estará.

Descargar archivos de un escritorio en el cliente

Con Horizon Client puede descargar archivos en el equipo cliente desde un escritorio remoto.

Procedimiento

- 1 Haga clic en el icono de transferencia de archivos situado en la parte superior de la barra lateral.
Se abrirá la ventana **Transferir archivos**.
- 2 Haga clic en **Descargar**.
- 3 Seleccione uno o varios archivos en el escritorio remoto.
- 4 Pulse Ctrl+C para iniciar la descarga.

- 5 Tras completarse la descarga, haga clic en el icono de descarga para guardar los archivos en el equipo cliente.

Cargar archivos del cliente a un escritorio

Horizon Client le permite cargar archivos desde el equipo cliente a un escritorio remoto.

Procedimiento

- 1 Haga clic en el icono de transferencia de archivos situado en la parte superior de la barra lateral. Se abrirá la ventana **Transferir archivos**.
- 2 Haga clic en **Cargar**.
- 3 Arrastre y suelte los archivos dentro de la ventana **Transferir archivos** y haga clic en **Elegir archivos** para seleccionarlos.

Los archivos seleccionados se cargan en la carpeta Documentos.

Con Internet Explorer 11 y Chrome en ChromeBook, si arrastra y suelta carpetas, archivos de tamaño cero o superiores a 2 GB, se le mostrará un mensaje de error esperado. Después de descartar el mensaje de error, ya no podrá arrastrar ni soltar archivos que se puedan transferir.

Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos

Con la función Audio/vídeo en tiempo real, puede usar el micrófono o la cámara web del equipo cliente en una aplicación o un escritorio remotos. Esta función es compatible con las aplicaciones de conferencias estándares y las aplicaciones de vídeo basadas en el explorador. Además, admite entrada de audio analógica, dispositivos de audio USB y cámaras web estándar.

La función Audio/vídeo en tiempo real solo es compatible en Chrome, Microsoft Edge y Firefox. La resolución de vídeo predeterminada es 320 x 240. La configuración Audio/vídeo en tiempo real predeterminada funciona correctamente con la mayoría de aplicaciones de audio y de cámaras web. Para obtener más información sobre cómo cambiar la configuración Audio/vídeo en tiempo real, consulte "Configurar la directiva de grupo de Audio/vídeo en tiempo real" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Cuando una aplicación o un escritorio remotos estén conectados al micrófono o a la cámara web del equipo cliente, antes de que la aplicación o el escritorio remotos puedan usar la cámara web o el micrófono, el navegador pedirá permiso. No todos los navegadores tienen el mismo comportamiento.

- Microsoft Edge le pedirá permiso en cada ocasión. No es posible cambiar este comportamiento. Si desea obtener más información, consulte <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>.
- Firefox le pedirá permiso en cada ocasión. Es posible cambiar este comportamiento. Si desea obtener más información, consulte <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>.

- Chrome le pedirá permiso la primera vez. Si permite que se use el dispositivo, Chrome no le volverá a pedir permiso.

Cuando un escritorio remoto está conectado al micrófono o la cámara web de un equipo cliente, aparece un icono de cada dispositivo en la parte superior de la barra lateral. También aparece un signo de interrogación rojo sobre el icono del dispositivo en la barra lateral para indicar la solicitud de permiso. Si permite que se use un dispositivo, desaparece este signo. Si rechaza una solicitud de permiso, desaparece el icono del dispositivo.

Si se usa la función Audio/vídeo en tiempo real en una sesión de aplicación o escritorio remotos, abre una conexión a una segunda aplicación o un segundo escritorio, y si aparece una advertencia de seguridad (por ejemplo, si no se instaló un certificado válido), si ignora esta advertencia y continúa con el proceso de conexión del segundo escritorio, esta función dejará de funcionar en la primera sesión.

Cerrar sesión o desconectarse

Con algunas configuraciones, si se desconecta desde un escritorio remoto sin cerrar sesión, las aplicaciones de dicho escritorio permanecerán abiertas. También se puede desconectar desde un servidor y dejar las aplicaciones remotas en ejecución.

Procedimiento

- ◆ Cerrar sesión en el servidor y desconectarse desde el escritorio (pero sin cerrar sesión en él) o salir de la aplicación alojada en el host.

Opción	Acción
En la pantalla para seleccionar la aplicación y el escritorio, antes de conectarse a una aplicación o escritorio remotos	Haga clic en el botón Cerrar sesión de la barra de herramientas situado en la esquina superior derecha de la pantalla.
En la barra lateral, cuando se conecta a una aplicación o escritorio remotos	Haga clic en el botón Cerrar sesión de la barra de herramientas situado en la parte superior de la barra lateral.

- ◆ Cerrar una aplicación remota.

Opción	Acción
Desde la aplicación	Salga de la aplicación con el procedimiento habitual, por ejemplo, haciendo clic en el botón X (Cerrar) en la esquina de la ventana de la aplicación.
En la barra lateral	Haga clic en la X que aparece junto al nombre del archivo en la lista En ejecución de la barra lateral.

- ◆ Cerrar sesión o desconectarse desde un escritorio remoto.

Opción	Acción
Desde el SO de escritorio	Para cerrar sesión, utilice el menú Inicio de Windows para cerrar sesión.
En la barra lateral	<p>Para cerrar sesión y desconectarse, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio en la lista En ejecución de la barra lateral y seleccione Cerrar sesión. Los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardar.</p> <p>Para desconectarse sin cerrar sesión, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio en la lista En ejecución y seleccione Cerrar.</p> <p>Nota El View Administrator puede configurar el escritorio para cerrar sesión de forma automática cuando se desconecte. En ese caso, se cerrarán todas las aplicaciones abiertas en el escritorio.</p>
Con un URI	Para cerrar sesión, utilice el siguiente URI: <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=logoff</code> .

Restablecer un escritorio remoto o aplicaciones remotas

Puede que tenga que restablecer un escritorio remoto si el sistema operativo del escritorio deja de responder y no se soluciona el problema reiniciando el escritorio remoto. Al restablecer las aplicaciones remotas, se sale de todas las aplicaciones abiertas.

La acción de restablecer un escritorio remoto es equivalente a pulsar el botón Restablecer en un equipo físico para forzar su restablecimiento. Los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardarse.

Restablecer las aplicaciones remotas es equivalente a salir de todas las aplicaciones sin guardar. Se cierran todas las aplicaciones abiertas, incluso las que proceden de diferentes granjas de servidores RDS.

Solo puede restablecer un escritorio remoto si un administrador de Horizon ha habilitado la función de restablecimiento de escritorio para dicho escritorio.

Para obtener información sobre cómo habilitar la función de restablecimiento de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- ◆ Utilizar el comando **Restablecer**.

Opción	Acción
Restablecer aplicaciones remotas desde la pantalla de selección de aplicaciones	Desde el escritorio y la pantalla de selección de aplicaciones, antes de conectarse a un escritorio o una aplicación remotos, para restablecer todas las aplicaciones remotas que se estén ejecutando, haga clic en el botón de la barra de herramientas Configuración , que se encuentra en la esquina superior derecha de la pantalla, y haga clic en Restablecer .
Restablecer un escritorio remoto desde la barra lateral	Si se conecta a un escritorio remoto, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio en la lista En ejecución de la barra lateral y seleccione Restablecer .
Restablecer aplicaciones remotas desde la barra lateral	Para restablecer todas las aplicaciones en ejecución, haga clic en el botón Abrir ventana Configuración de la barra de herramientas, situado en la parte superior de la barra lateral y, a continuación, en Restablecer .
Restablecer un escritorio remoto utilizando un URI	Para restablecer un escritorio remoto, utilice el URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> .

Cuando restablezca un escritorio remoto, el sistema operativo del escritorio remoto se reinicia y Horizon Client desconecta y cierra la sesión del escritorio. Cuando restablece aplicaciones remotas, se sale de las aplicaciones.

Pasos siguientes

Espere un periodo de tiempo apropiado para iniciar el sistema antes de intentar volver a conectarse a la aplicación o el escritorio remoto.

Reiniciar un escritorio remoto

Es posible que tenga que reiniciar un escritorio remoto si el sistema operativo del escritorio deja de responder. Reiniciar un escritorio remoto es el equivalente del comando de reinicio del sistema operativo Windows. El sistema operativo del escritorio normalmente le pide que guarde los datos que no haya guardado antes de reiniciar.

Puede reiniciar un escritorio remoto solo si un administrador de Horizon ha habilitado la función de reinicio de escritorio para dicho escritorio.

Para obtener información sobre cómo habilitar la función de reinicio de escritorio, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- ◆ Utilice el comando **Reiniciar**.

Opción	Acción
En la barra lateral	Cuando esté conectado a un escritorio remoto, haga clic en la barra de herramientas Abrir menú que se encuentra junto al nombre del escritorio en la lista En ejecución de la barra lateral y seleccione Reiniciar .
Usar un URI	Para reiniciar un escritorio, utilice el URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart</code> .

Se reinicia el sistema operativo del escritorio remoto y Horizon Client se desconecta y cierra la sesión del escritorio.

Pasos siguientes

Espere un periodo de tiempo apropiado para que se inicie el sistema antes de intentar volver a conectarse al escritorio remoto.

Si no se soluciona el problema reiniciando el escritorio remoto, puede que tenga que restablecer el escritorio remoto. Consulte [Restablecer un escritorio remoto o aplicaciones remotas](#).