

Planificación de la arquitectura de Horizon 7

MARZO DE 2020

VMware Horizon 7 7.12



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 © 2009-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Planificación de la arquitectura de Horizon 7 6

1 Introducción a Horizon 7 7

Ventajas de utilizar Horizon 7 7

Funciones de Horizon 7 10

Cómo se coordinan los componentes 13

Dispositivos cliente 13

Servidor de conexión de Horizon 14

Horizon Client 15

Portal web del usuario de VMware Horizon 15

Horizon Agent 16

Horizon Administrator 16

View Composer 16

vCenter Server 17

Integración y personalización Horizon 7 17

2 Planificar una experiencia de usuario satisfactoria 24

Matriz de compatibilidad de funciones para Horizon Agent 24

Elegir un protocolo de visualización 25

VMware Blast Extreme 25

PCoIP 30

Microsoft RDP 32

Utilizar aplicaciones publicadas 32

Usar Horizon Persona Management para conservar datos y configuraciones de los usuarios 33

Usar dispositivos USB con aplicaciones y escritorios remotos 35

Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos 36

Utilizar aplicaciones de gráficos 3D 36

Transmisión de multimedia a un escritorio remoto 37

Imprimir desde un escritorio remoto 38

Utilizar single sign-on para iniciar sesión 38

Resolución de pantalla y monitores 39

3 Administrar grupos de aplicaciones y escritorios desde una ubicación centralizada 42

Ventajas de los grupos de escritorios 42

Ventajas de los grupos de aplicaciones 43

Reducir y administrar requisitos de almacenamiento 44

Administrar almacenamiento con vSphere 45

Utilizar VMware vSAN para almacenamiento de alto rendimiento y administración basada en directivas	47
Usar Virtual Volumes con el almacenamiento situado en máquinas virtuales y la administración basada en directivas	49
Reducir requisitos de almacenamiento con Composer	50
Reducir requisitos de almacenamiento con clones instantáneos	52
Aprovisionamiento de aplicaciones	55
Implementar aplicaciones individuales mediante un host RDS	55
Implementar aplicaciones y actualizaciones del sistema con View Composer	56
Implementar aplicaciones y actualizaciones del sistema con clones instantáneos	57
Administrar las aplicaciones VMware ThinApp en Horizon Administrator	57
Implementar y administrar aplicaciones mediante App Volumes	58
Utilizar procesos existentes o VMware Mirage para el aprovisionamiento de aplicaciones	58
Utilizar GPO de Active Directory para administrar usuarios y escritorios	59

4 Elementos de diseño de la arquitectura y directrices de planificación para implementaciones de escritorios remotos

Requisitos de máquina virtual para escritorios remotos	62
Planificación basada en tipos de trabajadores	62
Estimar los requisitos de memoria para escritorios de máquinas virtuales	63
Estimar los requisitos de CPU para escritorios de máquinas virtuales	66
Elegir el tamaño adecuado del disco del sistema	67
Nodo de Horizon 7ESXi	68
Grupos de escritorios para tipos específicos de trabajo	69
Grupos de trabajadores con tareas específicas	71
Grupos para trabajadores del conocimiento y usuarios avanzados	73
Grupos de usuarios de pantalla completa	74
Configuración de la máquina virtual del escritorio	75
Configuración de la máquina virtual del host RDS	76
Configuración de máquinas virtuales de vCenter Server y View Composer	77
Máximos del servidor de conexión de Horizon y configuración de máquinas virtuales	79
Clústeres de vSphere	82
Requisitos de almacenamiento y ancho de banda	84
Ejemplo de almacenamiento compartido	85
Consideraciones de ancho de banda de almacenamiento	88
Consideraciones de ancho de banda	89
Resultados de la prueba de rendimiento de View Composer	91
Compatibilidad WAN	93
Bloques de creación de Horizon 7	95
Pods de Horizon 7	96
Descripción general de Arquitectura de Cloud Pod	98
Ventajas de utilizar varios servidores vCenter Server en un pod	99

5 Planificar las funciones de seguridad 103

- Comprender el funcionamiento de las conexiones cliente 103
 - Conexiones de clientes mediante puertas de enlace seguras de Blast y PCoIP 104
 - Conexiones de túnel de cliente con Microsoft RDP 105
 - Conexiones directas del cliente 106
- Elegir un método de autenticación de usuarios 106
 - Autenticación de Active Directory 107
 - Uso de la autenticación en dos fases 108
 - Autenticación con tarjeta inteligente 109
 - Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows 109
- Restringir el acceso a escritorios remotos 111
- Utilizar configuraciones de directivas de grupo para asegurar aplicaciones y escritorios remotos 112
- Usar Directivas de Smart 113
- Implementar procedimientos recomendados para proteger sistemas de cliente 113
- Asignar funciones de administrador 114
- Preparar el uso de un servidor de seguridad 114
 - Prácticas recomendadas para las implementaciones de servidores de seguridad 115
 - Topologías de servidores de seguridad 115
 - Firewall para servidores de seguridad basados en zonas DMZ 117
- Comprender los protocolos de comunicaciones 121
 - Servidor de puerta de enlace segura de View 124
 - Puerta de enlace segura de Blast 125
 - Puerta de enlace segura de PCoIP 126
 - LDAP de View 126
 - Horizon Messaging 127
 - Reglas de firewall para el servidor de conexión de Horizon 127
 - Reglas del firewall para Horizon Agent o View Agent 128
 - Reglas del firewall para Active Directory 130

6 Descripción general de los pasos para configurar un entorno de Horizon 7 131

Planificación de la arquitectura de Horizon 7

Planificación de la arquitectura de Horizon 7 es una introducción a VMware Horizon™ 7 que incluye una descripción de sus principales características y opciones de implementación, y una descripción general de la configuración típica de los componentes en un entorno de producción.

En esta guía, se da respuesta a las preguntas siguientes:

- ¿Resuelve el producto los problemas que es necesario resolver?
- ¿Sería factible y económicamente rentable implementar esta solución en su empresa?

No todas las funciones y características de VMware Horizon 7 están disponibles en todas las ediciones. Si desea obtener más información sobre los conjuntos de funciones de cada edición, consulte <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Para ayudarle a proteger la instalación, en esta guía también se comentan características de seguridad.

Público al que se dirige

Esta información se dirige a arquitectos, administradores y responsables de la toma de decisiones de TI, así como a otras personas que necesiten familiarizarse con los componentes y las posibilidades de este producto. Con esta información, los arquitectos y planificadores pueden determinar si Horizon 7 satisface las necesidades de su empresa para proporcionar de manera eficiente y segura aplicaciones y escritorios de Windows a sus usuarios finales. La arquitectura de ejemplo ayuda a los planificadores a conocer los requisitos de hardware y los trabajos de configuración necesarios para implementaciones a gran escala.

Introducción a Horizon 7

1

Con Horizon 7, los departamentos de TI pueden ejecutar aplicaciones y escritorios remotos en el centro de datos y entregar estas aplicaciones y escritorios a los empleados como un servicio administrado. Los usuarios finales reciben un entorno familiar y personalizado al que pueden acceder desde cualquier número de dispositivos en cualquier lugar de toda la empresa o desde el hogar. Los administradores obtienen control centralizado, eficiencia y seguridad al tener los datos de los escritorios en el centro de datos.

Este capítulo incluye los siguientes temas:

- [Ventajas de utilizar Horizon 7](#)
- [Funciones de Horizon 7](#)
- [Cómo se coordinan los componentes](#)
- [Integración y personalización Horizon 7](#)

Ventajas de utilizar Horizon 7

Entre las ventajas de administrar escritorios con Horizon 7, se incluyen mayor fiabilidad, seguridad, independencia del hardware y comodidad.

Fiabilidad y seguridad

Los escritorios y las aplicaciones se pueden centralizar mediante la integración con VMware vSphere® y la virtualización de recursos de servidor, almacenamiento y conexión de red. Colocar sistemas operativos y aplicaciones de escritorio en un servidor del centro de datos ofrece las siguientes ventajas:

- El acceso a los datos se puede restringir fácilmente. Se puede evitar la copia de datos confidenciales a un equipo doméstico de un empleado remoto.
- La compatibilidad con RADIUS ofrece flexibilidad al elegir entre proveedores de autenticación de doble factor. Entre los proveedores compatibles, se incluyen RSA SecureID, VASCO DIGIPASS, SMS Passcode y SafeNet.

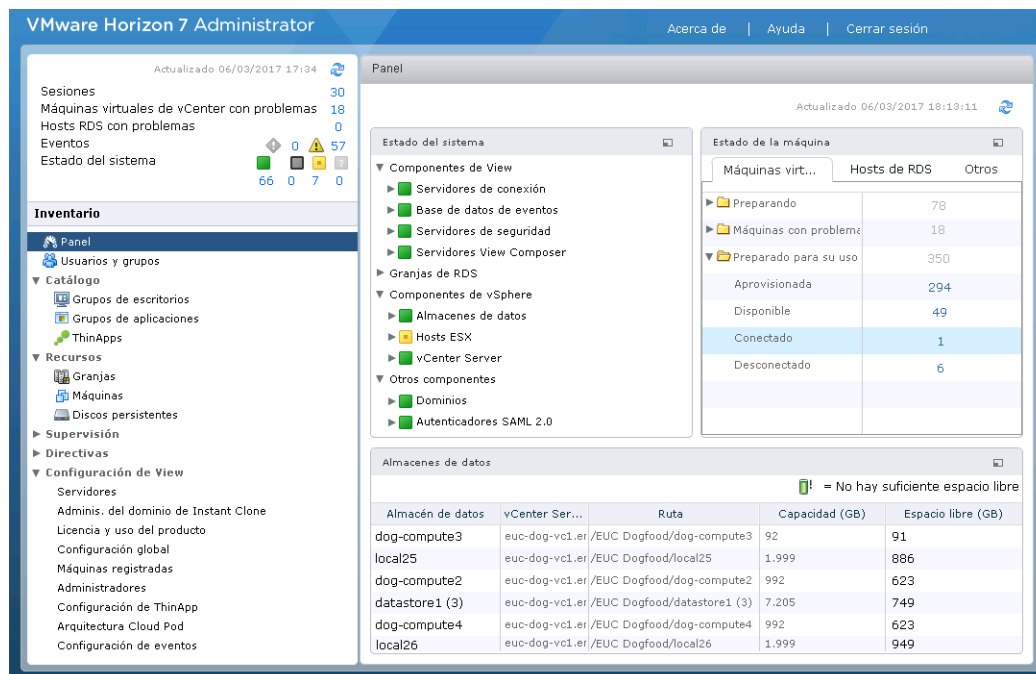
- La integración con VMware Identity Manager significa que los usuarios finales podrán acceder bajo demanda a escritorios remotos mediante el mismo catálogo de aplicaciones basadas en la web que utilizan para acceder a aplicaciones SaaS, web y Windows. Dentro de un escritorio remoto, los usuarios también pueden utilizar este almacén de aplicaciones personalizadas para acceder a aplicaciones.
- La posibilidad de aprovisionar los escritorios remotos con cuentas de Active Directory creadas previamente permite cumplir los requisitos de los entornos bloqueados de Active Directory que tengan directivas de acceso de solo lectura.
- Las copias de seguridad de los datos se pueden programar sin tener en cuenta cuándo se podrían apagar los sistemas de los usuarios finales.
- Las aplicaciones y escritorios remotos alojados en centros de datos no experimentarán ningún tiempo de inactividad o será muy pequeño. Las máquinas virtuales pueden residir en clústeres de alta disponibilidad de servidores VMware.

Los escritorios virtuales también se pueden conectar a sistemas back-end físicos y a hosts Microsoft Remote Desktop Services (RDS).

Comodidad

La consola de administración unificada se ha creado para que sea escalable, por lo que incluso las implementaciones más grandes de Horizon 7 se pueden administrar con eficiencia desde una única interfaz de administración. Los asistentes y paneles de control mejoran el flujo de trabajo y facilitan el análisis para buscar detalles o cambiar configuraciones. [Figura 1-1. Consola de administración que muestra la vista del panel de control](#) es un ejemplo de interfaz de usuario basada en navegador para Horizon Administrator.

Figura 1-1. Consola de administración que muestra la vista del panel de control



Otras características que aumentan la comodidad son los protocolos de visualización remota de VMware, PCoIP (PC over IP) y Blast Extreme. Estos protocolos de visualización proporcionan al usuario final una experiencia igual a la de utilizar un PC físico:

- En redes LAN, la visualización es más rápida y suave que las visualizaciones remotas tradicionales.
- En redes WAN, los protocolos de visualización pueden compensar el aumento de la latencia o la disminución del ancho de banda, lo que asegura el rendimiento para los usuarios finales independientemente de las condiciones de la red.

Facilidad de administración

El aprovisionamiento de escritorios y aplicaciones para usuarios finales es un proceso rápido. Nadie tiene que instalar aplicaciones una por una en cada uno de los equipos físicos del usuario final. Los usuarios finales se conectan a una aplicación publicada o a un escritorio remoto completo con aplicaciones. Los usuarios finales pueden acceder a su mismo escritorio remoto o aplicación desde varios dispositivos en distintas ubicaciones.

El uso de VMware vSphere para alojar escritorios virtuales y servidores de host RDS ofrece las siguientes ventajas:

- Se reducen las tareas administrativas y las rutinas de administración. Los administradores pueden aplicar revisiones y actualizar aplicaciones y sistemas operativos sin tocar el equipo físico del usuario.
- La integración con VMware Identity Manager significa que los administradores de TI pueden utilizar la interfaz de administración de VMware Identity Manager basada en la web para supervisar las autorizaciones de grupos y usuarios para acceder a escritorios remotos.
- La integración con VMware App Volumes, un sistema de entrega de aplicaciones en tiempo real, permite a las empresas entregar y administrar aplicaciones a gran escala. App Volumes se puede utilizar para vincular aplicaciones a usuarios, grupos o equipos de destino, incluso si los usuarios han iniciado la sesión en sus escritorios. También es posible aprovisionar, entregar, actualizar y retirar aplicaciones en tiempo real.
- Horizon Persona Management permite administrar escritorios virtuales y físicos de forma centralizada, incluidos perfiles de usuario, autorizaciones para aplicaciones, directivas, rendimiento y otras opciones. Implemente Persona Management en los usuarios de escritorios físicos antes de convertirlos en escritorios virtuales.
- Con VMware User Environment Manager, los usuarios finales obtienen un escritorio Windows personalizado adaptado a la situación del usuario, lo que significa que el acceso a los recursos de TI necesarios se basa en aspectos como los derechos de usuario, el dispositivo y la ubicación.
- Se simplifica la administración del almacenamiento. VMware vSphere permite virtualizar volúmenes y sistemas de archivos para evitar la administración de dispositivos de almacenamiento independientes.
- vSphere 6.0 y las versiones posteriores permiten el uso de Virtual Volumes (VVols). Esta función asigna directamente discos virtuales y sus derivados, clonaciones, snapshots y réplicas a objetos,

denominados volúmenes virtuales, de un sistema de almacenamiento. Esta asignación permite a vSphere trasladar al sistema de almacenamiento operaciones de almacenamiento intensivas, como snapshots, clonación y replicación. Por ejemplo, con Virtual Volumes, una operación de clonación que antes tardaba una hora se puede ahora solo tarda unos minutos.

- vSphere 5.5 Update 1 y las versiones posteriores permiten utilizar vSAN, que virtualiza los discos físicos de estado sólido y las unidades de disco duro disponibles en hosts ESXi™ en un único almacén de datos compartido por todos los hosts de un clúster. Se especifica solo un almacén de datos al crear un grupo de escritorios y los distintos componentes, como archivos de máquina virtual, réplicas y archivos del sistema operativo, se colocan en discos SSD o unidades de disco duro, según corresponda.

Los requisitos de almacenamiento de la máquina virtual, como la capacidad, el rendimiento y la disponibilidad, se administran en forma de perfiles de directivas predeterminados, que se crean automáticamente al crear un grupo de escritorios.

- El acelerador de almacenamiento de Horizon 7 reduce considerablemente la carga de almacenamiento de operaciones de E/S por segundo (IOPS) y permite que se produzcan inicios de sesión de usuarios finales a mayor escala sin necesidad de ninguna tecnología de matriz de almacenamiento especial.
- Si los escritorios remotos utilizan el formato de disco para eficiencia del espacio disponible en vSphere 5.1 y versiones posteriores, el espacio ocupado por los datos antiguos o borrados dentro de un sistema operativo invitado se recupera automáticamente mediante un proceso de limpieza y reducción.

Independencia del hardware

Las aplicaciones publicadas y los escritorios remotos son independientes del hardware. Por ejemplo, como un escritorio remoto se ejecuta en un servidor del centro de datos y solo se accede a él desde un dispositivo cliente, un escritorio remoto puede usar un sistema operativo que no sea compatible con el hardware del dispositivo cliente.

Los escritorios remotos se ejecutan en equipos PC, Mac, clientes ligeros, equipos PC reconvertidos en clientes ligeros, tabletas y teléfonos. Las aplicaciones publicadas se ejecutan en un subconjunto de estos dispositivos. Trimestralmente, se agrega compatibilidad con nuevos dispositivos.

Si se utiliza la característica HTML Access, los usuarios finales pueden abrir una aplicación o un escritorio remoto dentro de un navegador, sin tener que instalar ninguna aplicación en el dispositivo o sistema cliente.

Funciones de Horizon 7

Las funciones incluidas en Horizon 7 proporcionan usabilidad, seguridad, control centralizado y escalabilidad.

Las siguientes funciones proporcionan al usuario final una experiencia familiar:

- En determinados dispositivos cliente, imprimir desde un escritorio virtual en cualquier impresora local o de red definida en el dispositivo cliente. Esta función de impresora virtual resuelve problemas de compatibilidad y no requiere instalar controladores de impresora adicionales en una máquina virtual.
- En la mayoría de los dispositivos cliente, se utiliza la función de impresión basada en la ubicación para asignar impresoras que se encuentren físicamente cerca del cliente. La impresión basada en la ubicación requiere instalar controladores de impresora en la máquina virtual.
- El redireccionamiento de la impresora local está diseñado para los siguientes escenarios de uso:
 - Impresoras conectadas directamente a puertos serie o USB del cliente
 - Impresoras especializadas, como impresoras de códigos de barras o de etiquetas conectadas al equipo cliente
 - Impresoras de red en una red remota que no se puedan direccionar desde la sesión virtual.
- Usar varios monitores. Con los protocolos de visualización PCoIP y Blast Extreme, la compatibilidad con varios monitores significa que se puede ajustar la rotación y la resolución de la pantalla de forma independiente para cada monitor.
- Acceder a dispositivos USB y a otros periféricos conectados al dispositivo local que muestra el escritorio virtual.

Se pueden especificar los tipos de dispositivos USB a los que se permite que se conecten los usuarios finales. En el caso de dispositivos compuestos que contengan varios tipos de dispositivos, como un dispositivo de entrada de vídeo y un dispositivo de almacenamiento, se puede dividir el dispositivo de manera que uno de ellos (por ejemplo, el dispositivo de entrada de vídeo) pueda conectar, pero el otro no (por ejemplo, el de almacenamiento).

- Use Horizon Persona Management para conservar los datos y las configuraciones de los usuarios entre sesiones, incluso después de actualizar o recomponer escritorios. Persona Management tiene la capacidad de replicar perfiles de usuario en un almacén de perfiles remoto (recurso compartido CIFS) a intervalos configurables.

También se puede utilizar una versión independiente de Persona Management en equipos físicos y máquinas virtuales que Horizon 7 no administre.

Horizon 7 ofrece las siguientes funciones de seguridad, entre otras:

- Usar autenticación de doble factor para iniciar la sesión, como RSA SecurID o RADIUS (Remote Authentication Dial-In User Service), o tarjetas inteligentes.
- Usar cuentas de Active Directory creadas previamente al aprovisionar aplicaciones y escritorios remotos en entornos que tengan directivas de acceso de solo lectura para Active Directory.
- Usar túneles SSL/TLS para asegurar que todas las conexiones estén completamente cifradas.
- Usar VMware High Availability para asegurar la conmutación por error automática.

Las funciones de escalabilidad dependen de la plataforma de virtualización de VMware para administrar tanto escritorios como servidores.

- Integrar con VMware vSphere para conseguir densidades económicamente rentables, altos niveles de disponibilidad y control de asignación de recursos avanzado para aplicaciones y escritorios remotos.
- Utilice el acelerador de almacenamiento de Horizon 7 para admitir inicios de sesión de usuarios a mayor escala con los mismos recursos de almacenamiento. Este acelerador de almacenamiento utiliza funciones de la plataforma vSphere 5 para crear una caché de memoria de hosts de lecturas de bloques comunes.
- Configure el servidor de conexión de Horizon para que actúe como agente en las conexiones entre los usuarios finales y las aplicaciones y escritorios remotos a los que tienen autorización para acceder.
- Usar View Composer para crear rápidamente imágenes de escritorio que compartan discos virtuales con una imagen principal. Al utilizar clones vinculados de esta manera, se ahorra espacio de disco y se simplifica la administración de revisiones y actualizaciones del sistema operativo.
- Usar la función Clon instantáneo, introducida en Horizon 7, para crear rápidamente imágenes de escritorios que compartan discos virtuales y memoria con una imagen principal. Los clones instantáneos no solo tienen la eficiencia de espacio de los clones vinculados de View Composer, sino que eliminan la necesidad de actualizar, recomponer y reequilibrar, simplificando aún más la administración de revisiones y actualizaciones del sistema operativo. Los clones instantáneos eliminan por completo el intervalo de mantenimiento de los escritorios.

Las siguientes funciones proporcionan administración y gestión centralizadas:

- Usar Microsoft Active Directory para administrar el acceso a aplicaciones y escritorios remotos y administrar directivas.
- Usar Persona Management para simplificar la migración de escritorios físicos a virtuales.
- Usar la consola de administración basada en web para administrar aplicaciones y escritorios remotos desde cualquier ubicación.
- Usar Horizon Administrator para distribuir y administrar aplicaciones empaquetadas con VMware ThinApp™.
- Usar una plantilla, o imagen maestra, para crear y aprovisionar grupos de escritorios rápidamente.
- Enviar actualizaciones y revisiones a escritorios virtuales, sin afectar a la configuración, datos y preferencias del usuario.
- Integrar con VMware Identity Manager de manera que los usuarios finales puedan acceder a escritorios remotos a través del portal del usuario en la web, así como usar VMware Identity Manager desde un navegador dentro de un escritorio remoto.
- Integrar con Mirage™ y Horizon FLEX™ para administrar escritorios de máquinas virtuales instaladas localmente e implementar y actualizar aplicaciones en clones completos de escritorios remotos dedicados sin sobrescribir aplicaciones instaladas por los usuarios.

Los usuarios finales abren Horizon Client para visualizar sus aplicaciones y escritorios remotos. Los dispositivos cliente utilizan el software de cliente ligero de Horizon 7 y se pueden configurar de manera que la única aplicación que los usuarios puedan iniciar directamente en el dispositivo sea el cliente ligero de Horizon 7. La reconversión de un PC heredado en un escritorio de cliente ligero puede alargar la vida del hardware entre tres y cinco años. Por ejemplo, al utilizar Horizon 7 en un escritorio ligero, se puede utilizar un sistema operativo más nuevo, como Windows 8.x, en hardware de escritorio más antiguo.

Si se utiliza la característica HTML Access, los usuarios finales pueden abrir un escritorio remoto dentro de un navegador, sin tener que instalar ninguna aplicación cliente en el dispositivo o sistema cliente.

Servidor de conexión de Horizon

Este servicio de software actúa como agente para las conexiones de clientes. El servidor de conexión de Horizon autentica a los usuarios a través de Windows Active Directory y envía la solicitud a la máquina virtual, el equipo físico o el host Microsoft RDS correspondientes.

El servidor de conexión ofrece las siguientes posibilidades de administración:

- Autenticar usuarios
- Autorizar usuarios a grupos y escritorios específicos
- Asignar aplicaciones empaquetadas con VMware ThinApp a grupos y usuarios específicos
- Administrar sesiones de aplicaciones y escritorios remotos
- Establecer conexiones seguras entre usuarios y aplicaciones y escritorios remotos
- Habilitar single sign-on
- Configurar y aplicar directivas

Dentro del firewall corporativo, se instala y configura un grupo de dos o más instancias del servidor de conexión. Los datos de configuración se almacenan en un directorio LDAP integrado y se replican entre los miembros del grupo.

Fuera del firewall corporativo, en la zona DMZ, se puede instalar y configurar el servidor de conexión como servidor de seguridad, o bien instalar un dispositivo de Unified Access Gateway. Los servidores de seguridad y los dispositivos de Unified Access Gateway de la zona DMZ se comunican con los servidores de conexión dentro del firewall corporativo. Los servidores de seguridad y los dispositivos de Unified Access Gateway aseguran que el único tráfico de aplicaciones y escritorios remotos que puede entrar al centro de datos corporativo sea el tráfico en nombre de un usuario autenticado correctamente. Los usuarios solo pueden acceder a los recursos para los que tengan autorización.

Los servidores de seguridad ofrecen un subconjunto de funciones y no necesitan estar en un dominio de Active Directory. El servidor de conexión se instala en un servidor Windows Server 2008 R2 o Windows Server 2012 R2, preferiblemente en una máquina virtual de VMware. Para obtener más información sobre los dispositivos de Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Importante Es posible crear una configuración de Horizon 7 que no utilice el servidor de conexión. Si se instala el complemento Horizon 7 Agent Direct Connect en un escritorio de máquina virtual remoto, el cliente se puede conectar directamente a la máquina virtual. Todas las funciones de escritorio remoto, incluyendo PCoIP, HTML Access, RDP, el redireccionamiento USB y la administración de sesiones, funcionan de la misma manera, como si el usuario se conectara a través del servidor de conexión. Para obtener más información, consulte *Horizon 7 Administración del complemento Agent Direct-Connection*.

Horizon Client

El software de cliente para acceder a aplicaciones y escritorios remotos se puede ejecutar en una tableta, un teléfono, un PC o portátil Windows, Linux o Mac, un cliente ligero y otros equipos.

Después de iniciar la sesión, los usuarios pueden seleccionar de una lista las aplicaciones y escritorios remotos que están autorizados a utilizar. La autorización puede requerir credenciales de Active Directory, UPN, PIN de tarjeta inteligente, RSA SecurID u otro token de autenticación de doble factor.

El administrador puede configurar Horizon Client para permitir que los usuarios finales seleccionen un protocolo de visualización. Los protocolos incluyen PCoIP, Blast Extreme y Microsoft RDP para escritorios remotos. La velocidad y calidad de visualización de PCoIP y Blast Extreme son prácticamente iguales a las de un PC físico.

Las funciones dependen de qué Horizon Client se utilice. Esta guía se centra en Horizon Client para Windows. En esta guía, no se describen con detalle los siguientes tipos de cliente:

- Detalles sobre Horizon Client para tabletas, clientes Linux y clientes Mac. Consulte la documentación de Horizon Client en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.
- Detalles sobre el HTML Access Web client, que permite abrir un escritorio remoto dentro de un navegador. No se instala ninguna aplicación Horizon Client en el dispositivo o sistema cliente. Consulte la documentación de Horizon Client en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.
- Diversos clientes ligeros y cero de terceros, disponibles solo a través de partners certificados.
- View Open Client, que es compatible con el programa de certificación de partners de VMware. View Open Client no es una aplicación cliente oficial y no es compatible como tal.

Portal web del usuario de VMware Horizon

Desde un navegador web de un dispositivo cliente, los usuarios finales se pueden conectar a aplicaciones y escritorios remotos a través del navegador, iniciar automáticamente Horizon Client si está instalado o descargar el instalador de Horizon Client.

Al abrir un navegador e introducir la dirección URL de una instancia de Horizon Connection Server, la página web que aparecerá contiene vínculos al [sitio de descargas de VMware](#) para descargar Horizon Client. No obstante, los vínculos de la página web se pueden configurar. Por ejemplo, se pueden configurar los vínculos para que se dirijan a un servidor web interno o limitar las versiones del cliente disponibles en su propio servidor de conexión.

Si se usa la función HTML Access, la página web muestra también un vínculo para acceder a aplicaciones y escritorios remotos dentro de un navegador compatible. Con esta función, no se instala ninguna aplicación Horizon Client en el dispositivo o sistema cliente. Para obtener más información, consulte la Horizon Client documentación en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Horizon Agent

El servicio Horizon Agent se instala en todos los hosts Microsoft RDS, máquinas virtuales y sistemas físicos que se utilicen como orígenes de aplicaciones y escritorios remotos. En las máquinas virtuales, este agente se comunica con Horizon Client para proporcionar funciones, como la supervisión de la conexión, la impresión virtual, Horizon Persona Management y el acceso a dispositivos USB conectados de forma local.

Si el origen del escritorio es una máquina virtual, se instala primero el servicio Horizon Agent en esa máquina virtual y, a continuación, se usa la máquina virtual como plantilla o como máquina virtual principal de clones vinculados o instantáneos. Al crear un grupo desde esta máquina virtual, el agente se instala automáticamente en todos los escritorios remotos.

El agente se puede instalar con la opción de single sign-on. Si se usa Single Sign-On, los usuarios solo deben iniciar sesión al conectarse al servidor de conexión de Horizon y no se les vuelve a pedir que lo hagan de nuevo para conectarse a una aplicación o escritorio remotos.

Horizon Administrator

Esta aplicación basada en la Web permite a los administradores configurar el servidor de conexión de Horizon, implementar y administrar aplicaciones y escritorios remotos, controlar la autenticación de usuarios y solucionar problemas de los usuarios finales.

Al instalar una instancia del servidor de conexión, se instala también la aplicación Horizon Administrator. Esta aplicación permite a los administradores gestionar instancias del servidor de conexión desde cualquier lugar sin tener que instalar ninguna aplicación en el equipo local.

View Composer

Este servicio de software se puede instalar en una instancia de vCenter Server que administre máquinas virtuales o en un servidor independiente. A continuación, View Composer podrá crear un grupo de clones vinculados desde una máquina virtual principal especificada. Esta estrategia reduce los costes de almacenamiento hasta un 90%.

Cada clon vinculado actúa como un escritorio independiente, con una dirección IP y un nombre de host únicos y, sin embargo, requiere un espacio de almacenamiento significativamente menor porque comparte una imagen de base con la máquina principal. Como los grupos de escritorios de clones vinculados comparten una imagen de base, se pueden implementar rápidamente actualizaciones y revisiones actualizando solo la máquina virtual principal. La configuración, las aplicaciones y los datos del usuario no se ven afectados.

View Composer también se puede utilizar para crear granjas automatizadas de hosts Microsoft RDS de clones vinculados, que proporcionan aplicaciones publicadas a los usuarios finales.

Aunque View Composer se puede instalar en su propio host de servidor, un servicio View Composer solo puede operar con una instancia de vCenter Server. De forma similar, una instancia de vCenter Server solo se puede asociar a un servicio View Composer.

Importante View Composer es un componente opcional. Si se prevé aprovisionar clones instantáneos, no es necesario instalar View Composer.

vCenter Server

Este servicio actúa como administrador central de servidores VMware ESXi conectados en una red. vCenter Server proporciona el punto central para configurar, aprovisionar y administrar máquinas virtuales del centro de datos.

Además de utilizar estas máquinas virtuales como orígenes para grupos de escritorios de máquinas virtuales, estas se pueden usar para alojar los componentes del servidor de Horizon 7, incluyendo instancias de Horizon Connection Server, servidores de Active Directory, hosts Microsoft RDS e instancias de vCenter Server.

View Composer se puede instalar en el mismo servidor que vCenter Server o en uno diferente. A continuación, vCenter Server administra la asignación de las máquinas virtuales a los servidores físicos y al almacenamiento y administra la asignación de recursos de memoria y CPU a las máquinas virtuales.

vCenter Server se puede instalar como dispositivo virtual de VMware o instalar vCenter Server en un servidor Windows Server 2008 R2 o un servidor Windows Server 2012 R2, preferiblemente en una máquina virtual de VMware.

Integración y personalización Horizon 7

Para aumentar la efectividad de Horizon 7 en su organización, se pueden usar varias interfaces para integrar Horizon 7 con aplicaciones externas o para crear scripts de administración que se pueden ejecutar desde la línea de comandos o por lotes.

Integración con otros componentes

Horizon 7 se integra a estos productos de VMware.

VMware Cloud on AWS

VMware Cloud on AWS le permite crear centros de datos de vSphere en Amazon Web Services. Estos centros de datos incluyen vCenter Server para administrar su centro de datos, vSAN para el almacenamiento y VMware NSX para las redes. Puede conectar un centro de datos en las instalaciones al SDDC de su nube y administrarlos desde una única interfaz de vSphere Client. Con su cuenta de AWS conectada, puede acceder a servicios de AWS, como EC2 y S3, desde máquinas virtuales de su SDDC. Para obtener más información, consulte la VMware Cloud on AWS documentación en <https://docs.vmware.com/es/VMware-Cloud-on-AWS/index.html>.

A partir de la versión 7.5 de Horizon 7, puede implementar clones completos de Horizon 7 en VMware Cloud on AWS. Por ejemplo, puede implementar un entorno de Horizon 7 que use la Arquitectura Cloud Pod en las instancias de VMware Cloud on AWS y los centros de datos en las instalaciones. Esto permite que Horizon 7 se ejecute fácilmente en un entorno de nube híbrida y subcontratar a VMware la administración de la infraestructura de SDDC.

VMware Identity Manager

Se puede integrar VMware Identity Manager con Horizon 7 para proporcionar a usuarios finales y administradores de TI las siguientes ventajas:

- Los usuarios finales pueden acceder bajo demanda a aplicaciones y escritorios remotos a través del mismo portal de la web que utilizan para acceder a aplicaciones de Windows, SaaS y web, con la misma comodidad de single sign-on.

La función True SSO permite que los usuarios que se autenticuen mediante tarjeta inteligente o autenticación de doble factor accedan a sus aplicaciones y escritorios remotos sin tener que proporcionar credenciales de Active Directory.

- Los usuarios finales pueden acceder a VMware Identity Manager en la web desde dentro de un escritorio remoto para utilizar las aplicaciones que necesiten.
- Si se utiliza también HTML Access, los usuarios finales pueden abrir un escritorio remoto dentro de un navegador, sin tener que instalar ninguna aplicación cliente en el dispositivo o sistema cliente.
- Los administradores de TI pueden utilizar la consola de administración basada en la web de VMware Identity Manager para supervisar las autorizaciones de usuarios y grupos para los escritorios remotos.

VMware Mirage y Horizon FLEX

Es posible utilizar Mirage y Horizon FLEX para implementar y actualizar aplicaciones en clones completos de escritorios remotos dedicados sin sobrescribir datos ni aplicaciones instaladas por el usuario.

Mirage ofrece una solución de escritorios virtuales sin conexión mejor que la función de modo local incluida anteriormente en Horizon 7. Mirage incluye las siguientes funciones de seguridad y administración para escritorios sin conexión.

- Cifra la máquina virtual instalada localmente e impide que los usuarios modifiquen configuraciones de la máquina virtual que afecten a la integridad del contenedor seguro.
- Proporciona directivas, incluyendo la caducidad, disponibles en VMware Fusion™ Professional y VMware® Player Plus™, comparables a las directivas proporcionadas en la función de modo local anterior. Fusion Pro y Player Plus se incluyen en Mirage.
- Elimina la necesidad de que los usuarios inicien o salgan de la sesión en sus escritorios para recibir actualizaciones.
- Permite a los administradores utilizar la función de superposición de capas de Mirage, las funciones de copia de seguridad y el portal de archivos.

VMware App Volumes

VMware App Volumes es un sistema integrado y unificado de administración de usuarios y de distribución de aplicaciones para Horizon 7 y otros entornos virtuales. Las aplicaciones y los datos administrados por App Volumes se guardan en archivos VMDK o VHD denominados AppStacks, que se adjuntan a cada sesión de usuario de Windows al iniciar sesión o al reiniciar. Esta estrategia asegura que el usuario reciba los datos y aplicaciones más actuales. App Volumes proporciona también un contenedor diferente para configuraciones y aplicaciones persistentes instaladas por el usuario denominado volumen de escritura, que se carga también al iniciar sesión o al reiniciar. Los perfiles de usuario y la configuración de directivas también se pueden administrar mediante la plataforma App Volumes.

VMware User Environment Manager

La función Directivas de Smart se puede utilizar para crear directivas que controlen el comportamiento del redireccionamiento USB, impresión virtual, redireccionamiento del portapapeles, redireccionamiento de unidades del cliente y funciones de protocolo de visualización PCoIP en escritorios remotos específicos. User Environment Manager permite que el personal de TI controle qué configuraciones pueden personalizar los usuarios y asigna también configuraciones de entorno tales como redes e impresoras específicas de la ubicación. La función Directivas de Smart permite crear directivas que solo tengan efecto si se cumplen determinadas condiciones.

Por ejemplo, puede configurar una directiva que deshabilite la función del redireccionamiento de unidades cliente si un usuario se conecta a un escritorio remoto desde un lugar que no se encuentre dentro de la red corporativa.

VMware Unified Access Gateway

Unified Access Gateway funciona como una puerta de enlace segura para usuarios que deseen acceder a aplicaciones y escritorios remotos desde fuera del firewall corporativo. Unified Access Gateway es un dispositivo que se instala en una zona desmilitarizada (DMZ). Use Unified Access Gateway para garantizar que el único tráfico que entra al centro de datos corporativo lo hace en nombre de usuarios correctamente autenticados. Puede usar dispositivos de Unified Access Gateway en lugar de servidores de seguridad de Horizon 7. Para obtener más información, consulte la documentación de Unified Access Gateway.

Integración con el software de videoconferencia más habitual

Puede usar estos software de videoconferencia y de llamadas con Horizon 7.

Redireccionamiento URL de Flash

Al enviar el contenido Flash directamente desde Adobe Media Server a endpoints cliente, disminuye la carga en el host ESXi del centro de datos y se elimina el enrutamiento adicional de dicho centro, además de reducir el ancho de banda necesario para transmitir vídeos al mismo tiempo en directo a varios endpoints cliente.

La función de redireccionamiento URL de Flash usa un JavaScript que el administrador de una página web incrustó en la misma. Cuando un usuario del escritorio virtual haga clic en el vínculo URL designado desde una página web, JavaScript intercepta y realiza un redireccionamiento de ShockWave File (SWF) desde la sesión del escritorio virtual al endpoint cliente. A continuación, el endpoint abre un VMware Flash Projector local fuera de la sesión del escritorio virtual y reproduce la secuencia de medios de forma local.

Nota Con Redireccionamiento URL de Flash, la transmisión multidifusión o unidifusión se redirecciona a los dispositivos cliente que puedan estar fuera del firewall de su organización. Los clientes deben tener acceso al servidor Adobe Web que aloja el archivo ShockWave Flash (SWF) que inicia las transmisiones multidifusión o unidifusión. Si es necesario, configure el firewall para abrir los puertos apropiados para permitir que los dispositivos cliente accedan a este servidor.

Esta función está disponible solo en algunos tipos de clientes. Para saber si es compatible con un tipo de cliente concreto, consulte la matriz de compatibilidad de funciones en el documento "Uso de VMware Horizon Client" para el tipo específico de dispositivo de cliente móvil o de escritorio. Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Microsoft Lync 2013

Es posible usar un cliente Microsoft Lync 2013 en escritorios remotos para participar en llamadas de comunicaciones unificadas (UC), de VoIP (voz sobre IP) y videollamadas con dispositivos de audio y vídeo USB certificados por Lync. Ya no es necesario un teléfono IP dedicado.

Esta arquitectura requiere la instalación de un cliente Microsoft Lync 2013 en el escritorio remoto y un complemento VDI de Microsoft Lync en el endpoint Windows 7 u 8 cliente. Los usuarios pueden usar el cliente Microsoft Lync 2013 para las funciones de presencia, de mensajería instantánea, de conferencias web y de Microsoft Office.

Cuando se produce una videollamada o una llamada VoIP de Lync, el complemento Lync VDI descarga todos los elementos multimedia procesados en el servidor del centro de datos al endpoint cliente y codifica todo este contenido en códecs de vídeo y de audio optimizados para Lync. Esta arquitectura optimizada es altamente escalable, con ella se reduce el uso de ancho de banda de red y proporciona una entrega multimedia punto a punto con compatibilidad para vídeo y VoIP de alta calidad y a tiempo real. Para obtener más información, consulte el documento técnico de VMware Horizon 6 y Microsoft Lync 2013 disponible en <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf>.

Nota Aún no se admite la grabación de audio. Esta integración solo es compatible con el protocolo de visualización PCoIP o Blast Extreme.

Skype Empresarial

Un usuario final puede realizar llamadas de voz o videollamadas con una buena calidad si cuenta con Skype Empresarial en un escritorio virtual. Esto no afectará de forma negativa la infraestructura virtual ni sobrecargará la red. Todos los procesos multimedia tienen lugar en el equipo cliente, en lugar de en el escritorio virtual, cuando se realizan llamadas de voz o videollamadas de Skype.

El software Virtualization Pack para Skype Empresarial se instala de forma predeterminada como parte de los instaladores de Horizon Client para Windows (4.6 y versiones posteriores), Horizon Client para Linux (4.6 y versiones posteriores) y Horizon Client para Mac (4.7 y versiones posteriores). Un administrador de Horizon también debe instalar la función VMware Virtualization Pack para Skype Empresarial en el escritorio virtual

durante la instalación de Horizon Agent. Para obtener más información, consulte el documento *Configurar escritorios virtuales en Horizon 7*. Para configurar Skype Empresarial, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Integración de Horizon 7 con software de información empresarial

El servidor de conexión de Horizon se puede configurar para que registre los eventos en una base de datos Microsoft SQL Server u Oracle.

- Acciones del usuario final como inicios de sesión e inicios de sesiones de escritorio remoto.
- Acciones de administrador como agregar autorizaciones y crear grupos de escritorios.
- Alertas que informan de errores y fallos del sistema.
- Muestreo estadístico, como el registro del número máximo de usuarios en un período de 24 horas.

Para acceder a la base de datos y efectuar análisis, se pueden utilizar sistemas de elaboración de informes de inteligencia empresarial como Crystal Reports, IBM Cognos, MicroStrategy 9 y Oracle Enterprise Performance Management System.

Para obtener más información, consulte el documento *Integración de Horizon 7*.

Alternativamente, se pueden generar eventos de Horizon 7 en formato syslog para que los programas de software de análisis puedan acceder a los datos de los eventos. Si habilita el registro de eventos basados en archivo, los eventos se acumulan en un archivo de registro local. Si se especifica un recurso compartido de archivo, los archivos de registro se mueven a ese recurso. Para obtener más información, consulte el documento *Instalación de Horizon 7*.

Utilizar los cmdlets Horizon PowerCLI para crear scripts de administración

Puede usar los cmdlets de Horizon PowerCLI con VMware PowerCLI. Utilice los cmdlets de Horizon PowerCLI para realizar varias tareas de administración en los componentes de Horizon.

Para obtener más información sobre los cmdlets de Horizon PowerCLI, lea la *referencia sobre cmdlets de VMware PowerCLI*.

Si desea obtener información sobre las especificaciones de la API para crear funciones y scripts avanzados con el fin de utilizarlos con Horizon PowerCLI, consulte la referencia de la API en el [Centro para desarrolladores de VMware](#).

Para obtener más información sobre los scripts de ejemplo que puede utilizar para crear sus propios scripts de Horizon PowerCLI, consulte la [comunidad de Horizon PowerCLI en GitHub](#).

Los cmdlets de Horizon PowerCLI se pueden utilizar para realizar diversas tareas administrativas en componentes de Horizon 7.

- Crear y actualizar grupos de escritorios.

- Configurar varias etiquetas de red para expandir enormemente el número de direcciones IP asignadas a las máquinas virtuales de un grupo.
- Agregar recursos de base de datos a una máquina virtual completa o un grupo de clones vinculados.
- Realizar operaciones de reequilibrado, actualización o recomposición en escritorios de clones vinculados.
- Realizar un muestreo del uso de determinados escritorios o grupos de escritorios a lo largo del tiempo.
- Consultar la base de datos de eventos.
- Consultar el estado de los servicios.

Modificar datos de configuración de LDAP en Horizon 7

Cuando se usa Horizon Administrator para modificar la configuración de Horizon 7, se actualizan los datos de LDAP correspondientes en el repositorio. El servidor de conexión de Horizon almacena su información de configuración en un repositorio compatible con LDAP. Por ejemplo, si se agrega un grupo de escritorios, el servidor de conexión almacena información acerca de usuarios, grupos de usuarios y autorizaciones en LDAP.

Es posible utilizar herramientas de línea de comandos de VMware y Microsoft para exportar e importar datos de configuración de LDAP en archivos con formato LDAP Data Interchange Format (LDIF) desde y en Horizon 7. Estos comandos son para administradores avanzados que deseen usar scripts para actualizar datos de configuración sin usar Horizon Administrator ni Horizon PowerCLI.

Los archivos LDIF se pueden utilizar para realizar determinadas tareas.

- Se puede enviar datos de configuración entre instancias del servidor de conexión.
- Se puede definir un gran número de objetos de Horizon 7, como grupos de escritorios, y agregarlos a las instancias del servidor de conexión sin utilizar Horizon Administrator ni Horizon PowerCLI.
- Se puede hacer una copia de seguridad de una configuración para restaurar el estado de una instancia del servidor de conexión.

Para obtener más información, consulte el documento *Integración de Horizon 7*.

Usar el comando vdmadmin

La interfaz de línea de comandos `vdmadmin` se puede utilizar para realizar diversas tareas de administración en una instancia del servidor de conexión. `vdmadmin` se puede utilizar para realizar tareas de administración que no se puedan hacer desde la interfaz de usuario de Horizon Administrator o que se tengan que ejecutar automáticamente desde scripts.

Para obtener más información, consulte el documento *Administración de Horizon 7*.

Planificar una experiencia de usuario satisfactoria

2

Horizon 7 proporciona el entorno de escritorio personalizado con el que el usuario final está familiarizado y que espera encontrar. Por ejemplo, en algunos sistemas cliente, los usuarios finales pueden acceder a dispositivos USB y de otro tipo conectados al equipo local, enviar documentos a las impresoras que este equipo pueda detectar, autenticarse con tarjetas inteligentes y usar varios monitores.

Horizon 7 incluye muchas funciones que puede que desee poner a disposición de sus usuarios finales. Antes de decidir qué funciones utilizar, debe conocer las limitaciones y restricciones de cada una de ellas.

Este capítulo incluye los siguientes temas:

- [Matriz de compatibilidad de funciones para Horizon Agent](#)
- [Elegir un protocolo de visualización](#)
- [Utilizar aplicaciones publicadas](#)
- [Usar Horizon Persona Management para conservar datos y configuraciones de los usuarios](#)
- [Usar dispositivos USB con aplicaciones y escritorios remotos](#)
- [Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos](#)
- [Utilizar aplicaciones de gráficos 3D](#)
- [Transmisión de multimedia a un escritorio remoto](#)
- [Imprimir desde un escritorio remoto](#)
- [Utilizar single sign-on para iniciar sesión](#)
- [Resolución de pantalla y monitores](#)

Matriz de compatibilidad de funciones para Horizon Agent

Al planificar el protocolo de visualización y las funciones que estarán disponibles para el usuario final, utilice la siguiente información para determinar qué sistemas operativos agente (aplicaciones y escritorio remoto) son compatibles con cada función.

Los tipos y ediciones de los sistemas operativos compatibles dependen de la versión de Windows. Para obtener una lista actualizada de los sistemas operativos Windows 10 compatibles, consulte el artículo <http://kb.vmware.com/kb/2149393> de la base de conocimientos (KB) de VMware. Para sistemas operativos Windows que no sean Windows 10, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150295>.

Para consultar una lista de funciones de experiencia remota específicas que se admiten en los sistemas operativos Windows en los que Horizon Agent está instalado, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150305>.

Nota Para obtener información sobre las funciones compatibles con distintos tipos de dispositivos cliente, consulte la documentación de Horizon Client en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Además, varios partners de VMware ofrecen dispositivos de cliente ligero y cero para implementaciones de Horizon 7. Las funciones que están disponibles para cada dispositivo de cliente ligero o cero están determinadas por el proveedor, el modelo y la configuración que la empresa decida utilizar. Para obtener más información acerca de los proveedores y los modelos de estos dispositivos de cliente ligero y cero, consulte la [Guía de compatibilidad de VMware](#) en el sitio web.

Elegir un protocolo de visualización

Un protocolo de visualización proporciona a los usuarios finales una interfaz gráfica para una aplicación o escritorio remoto que resida en el centro de datos. En función del tipo de dispositivo cliente que se tenga, se podrá elegir entre Blast Extreme y PCoIP (PC-over-IP), proporcionados por VMware, o Microsoft RDP (Remote Desktop Protocol).

Se pueden establecer directivas para controlar el protocolo que se usa o permitir que los usuarios finales lo elijan al iniciar sesión en un escritorio.

Nota En algunos tipos de clientes, no se utiliza el protocolo de visualización remota RDP ni el protocolo PCoIP. Por ejemplo, si se utiliza el cliente de HTML Access, disponible con la función HTML Access, se usa el protocolo de Blast Extreme en lugar de PCoIP o RDP. De manera similar, si se utiliza un escritorio remoto Linux, se usa Blast Extreme.

VMware Blast Extreme

Optimizado para la nube móvil, VMware Blast Extreme admite el rango más amplio de dispositivos cliente que son compatibles con H.264. De los protocolos de visualización, VMware Blast ofrece el menor consumo de CPU para obtener una mayor duración de la batería de los dispositivos móviles. VMware Blast Extreme puede compensar un aumento en la latencia o una reducción en el ancho de banda y puede aprovechar los transportes de redes UDP y TCP.

El protocolo de visualización VMware Blast se puede usar para las aplicaciones publicadas y para los escritorios remotos que usan máquinas virtuales o escritorios de sesión compartida en un host RDS. El host RDS puede ser un equipo físico o una máquina virtual. El protocolo de visualización VMware Blast no funciona en máquinas físicas de usuario único, excepto en la edición Enterprise de Windows 10 RS4 y compilaciones posteriores.

Nota No se admiten aplicaciones de películas y TV en las máquina físicas con Windows 10 RS4.

Funciones de VMware Blast Extreme

Las funciones clave de VMware Blast Extreme incluyen las siguientes:

- Los usuarios que se encuentran fuera del firewall corporativo pueden utilizar este protocolo con la red privada virtual (VPN) corporativa. También pueden establecer conexiones seguras y cifradas con un servidor de seguridad o dispositivo de Access Point de la red perimetral (DMZ) corporativa.
- El cifrado de 128 bits de Estándar de cifrado avanzado (AES) es compatible y se activa de forma predeterminada, pero puede cambiarlo a AES-256.
- Las conexiones desde todos los tipos de dispositivos cliente.
- Controles de optimización para reducir el uso del ancho de banda en las redes LAN y WAN.
- Los contadores de rendimiento mostrados mediante PerfMon en agentes de Windows proporcionan una representación exacta del estado actual del sistema que también se actualiza a un ritmo constante para lo siguiente:
 - Sesión de Blast
 - Imágenes
 - Audio
 - CDR
 - USB: Los contadores de USB que aparecen cuando utiliza PerfMon en agentes de Windows son válidos si el tráfico USB está configurado para utilizar VMware Virtual Channel (VVC).
 - Skype Empresarial: Los contadores son solo para controlar el tráfico.
 - Portapapeles
 - RTAV
 - Funciones de redireccionamiento del escáner y del puerto serie
 - Impresión virtual
 - MMR HTML5
 - Windows Media (MMR): Los contadores de rendimiento aparecen solo si se configuró esta función para que use VMware Virtual Channel (VVC).
- Continuidad de red durante una pérdida de red momentánea en clientes Windows.
- Las pantallas virtuales admiten color de 32 bits.

- Compatible con fuentes ClearType.
- Redirección de audio con ajuste de calidad de audio dinámico para LAN y WAN.
- Audio y vídeo en tiempo real para usar cámaras web y micrófonos en algunos tipos de cliente.
- Opción de copiar y pegar texto (y también imágenes en algunos clientes) entre el sistema operativo cliente y una aplicación publicada o escritorio remoto. En otros tipos de cliente, solo se puede copiar texto sin formato. No es posible copiar y pegar objetos del sistema, como carpetas y archivos, de un sistema a otro.
- En algunos tipos de cliente, se pueden utilizar varios monitores. En algunos casos, puede usar hasta cuatro monitores con una resolución de hasta 2560 x 1600 en cada uno o tres monitores con una resolución de 4K (3840 x 2160) para escritorios remotos de Windows 7 en los que se deshabilite Aero. También son compatibles las opciones de autoajustar y rotar la pantalla.

Al habilitar la función 3D, se admiten hasta dos monitores con una resolución de hasta 1920 x 1200 o un único monitor con una resolución de 4K (3840 x 2160).

- En algunos tipos de cliente, se admite el redireccionamiento USB.
- El redireccionamiento MMR se admite en algunos sistemas operativos cliente Windows y en algunos sistemas operativos de escritorio remoto (con Horizon Agent instalado).
- Las conexiones a equipos físicos sin monitores son compatibles con las tarjetas gráficas NVIDIA. Para obtener un mejor rendimiento, utilice una tarjeta gráfica que admita la codificación H.264.

Si tiene una GPU discreta adicional y una GPU integrada, es posible que se utilice el sistema operativo predeterminado para la GPU integrada. Para solucionar este problema, puede deshabilitar o eliminar el dispositivo en el Administrador de dispositivos. Si el problema persiste, puede instalar el controlador de gráficos WDDM para la GPU integrada o deshabilitar la GPU integrada en la BIOS del sistema. Consulte la documentación del sistema sobre cómo deshabilitar la GPU integrada.

Precaución Al deshabilitar la GPU integrada, es posible que se pierda el acceso a determinadas funciones como, por ejemplo, el acceso de la consola a la configuración del BIOS o al cargador de arranque NT.

- El códec Blast mejora el rendimiento de Adaptive y de los codificadores H.264 en el uso de escritorios al mostrar fuentes e imágenes más nítidas, y funciona como un códec de vídeo con detección de movimiento, vectores de movimiento y macrobloques interpredecibles. Se admite en los siguientes entornos y está deshabilitado de forma predeterminada:
 - Agentes Windows y Linux. Para habilitar el códec:
 - En agentes Windows, establezca la clave de registro: HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1
 - En agentes Linux, establezca RemoteDisplay.allowBlastCodec=TRUE en /etc/vmware/config
 - Deshabilite H.264 en la configuración del cliente Windows, Linux y MacOS. Esta función no es compatible con los clientes móviles ni con Web Client.

- Un conmutador de codificador dinámico permite alternar entre un codificador optimizado de vídeo (H.264 4:2:0 o H.264 4:4:4) y un codificador optimizado de texto (códec Blast o Adaptive). Este conmutador ayuda a mostrar vídeos y textos nítidos con un uso de ancho de banda reducido. Para usar esta función, habilite el conmutador del codificador:
 - En agentes Windows, establezca la clave de registro HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1
 - En agentes Linux, establezca RemoteDisplay.allowSwitchEncoder=TRUE en `\etc\vmware\config`
 - Habilite el códec Blast, que está deshabilitado de forma predeterminada. Si el códec Blast no está habilitado, el codificador del conmutador utilizará Adaptive para la codificación optimizada de texto.
 - Habilite H.264 en la configuración del cliente Windows, Linux o MacOS. Esta función no es compatible con los clientes móviles ni con Web Client.

Nota El conmutador de codificador solo utiliza software H.264 y no admite gráficos acelerados por hardware.

Para obtener más información sobre los dispositivos cliente que admiten funciones específicas de VMware Blast Extreme, diríjase a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Wake-on-LAN

Wake-on-LAN se admite en máquinas físicas con la edición Enterprise de Windows 10 RS4 y compilaciones posteriores. Esta función permite a los usuarios reactivar máquinas físicas cuando se conectan con Horizon Connection Server. La función Wake-on-LAN tiene estos requisitos previos:

- Wake-on-LAN (WoL) solo se admite en entornos IPv4.
- La máquina física debe estar configurada para reactivarse al recibir paquetes de Wake-on-LAN si la función Wake-on-LAN está habilitada en la configuración de la BIOS y de la tarjeta de red.
- Se debe utilizar el puerto de destino 9 para los paquetes de WoL procedentes del servidor de conexión.
- Los paquetes de WoL son paquetes de difusión orientados a direcciones IP que deben ser capaces de llegar a Horizon Agent cuando se envían desde Horizon Connection Server. Wake-on-LAN funciona en los siguientes casos:
 - El servidor de conexión y Horizon Agent en la máquina física están en la misma subred dentro de un entorno LAN.
 - Todos los enrutadores entre el servidor de conexión y Horizon Agent están configurados para permitir los paquetes de difusión orientados a direcciones IP en la subred de destino de la máquina física que desea reactivar.

Nota La función Wake-on-LAN no es compatible con grupos de asignaciones flotantes de un agente Windows 10 físico. El paquete de WoL solo se envía a grupos de asignaciones dedicados con la autorización de un usuario en particular.

Configuración recomendada para los sistemas operativos invitados

Se recomienda 1 GB o más de RAM y una CPU dual para reproducir en alta definición, en modo de pantalla completa, o bien vídeos de 720p o con un formato superior. Si desea utilizar Virtual Dedicated Graphics Acceleration para aplicaciones con gráficos avanzados, como aplicaciones CAD, necesita 4 GB de RAM.

Requisitos de calidad de vídeo

Vídeo con formato de 480p

Puede reproducir vídeo con una resolución nativa de 480p o inferior si el escritorio remoto tiene una única CPU virtual. Si desea reproducir el vídeo en Flash de alta definición o en modo de pantalla completa, el escritorio requiere una CPU virtual dual. Incluso con un escritorio que tenga doble CPU virtual, es posible que el vídeo con formato de 360p que se reproduce en modo de pantalla completa se retrase con respecto al audio, sobre todo en el caso de clientes Windows.

Vídeo con formato de 720p

Puede reproducir vídeo de 720p en resoluciones nativas si el escritorio remoto tiene una CPU virtual doble. El rendimiento puede verse afectado si reproduce vídeos en 720p en alta definición o en modo de pantalla completa.

Vídeo con formato de 1080p

Si el escritorio remoto tiene una CPU virtual doble, puede reproducir vídeo con formato de 1080p, aunque es posible que el reproductor deba ajustarse a una ventana más pequeña.

Procesamiento 3D

Puede configurar escritorios remotos para que utilicen gráficos de aceleración de hardware o software. La función de gráficos de aceleración de software le permite ejecutar aplicaciones de OpenGL 2.1 y DirectX9 sin necesidad de una unidad de procesamiento de gráficos (GPU) física. Las funciones de gráficos de aceleración de hardware permiten que las máquinas virtuales compartan sus GPU (unidades de procesamiento gráfico) físicas en un host de vSphere, o bien dediquen una GPU física a un único escritorio virtual.

Para las aplicaciones 3D, se admiten hasta dos monitores y la resolución de pantalla máxima es 1920 x 1200. El sistema operativo invitado en los escritorios remotos debe ser Windows 7 o posterior.

Para obtener más información sobre las funciones 3D, consulte [Utilizar aplicaciones de gráficos 3D](#).

Requisitos de hardware para los sistemas cliente

Para obtener más información sobre los requisitos de memoria y de procesamiento para el tipo específico de escritorio o dispositivo móvil cliente, acceda a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

PCoIP

PCoIP (PC over IP) ofrece una experiencia de escritorio optimizada para enviar una aplicación publicada o un entorno de escritorio remoto completo, con aplicaciones, imágenes y contenido de audio y vídeo, a un amplio grupo de usuarios a través la red LAN o WAN. PCoIP puede compensar el aumento de la latencia o la disminución del ancho de banda para garantizar que el rendimiento de los usuarios finales sea productivo independientemente de las condiciones de la red.

El protocolo de visualización PCoIP se puede utilizar con aplicaciones publicadas y escritorios remotos que usen máquinas virtuales, máquinas físicas que contengan tarjetas de host Teradici o escritorios de sesión compartida en un host RDS.

Funciones de PCoIP

Entre las funciones principales del protocolo PCoIP se incluyen las siguientes:

- Los usuarios que se encuentran fuera del firewall corporativo pueden utilizar este protocolo con la red privada virtual (VPN) de su compañía. También pueden establecer conexiones seguras y cifradas con un servidor de seguridad o dispositivo de Access Point de la red perimetral (DMZ) corporativa.
- El cifrado de 128 bits de Estándar de cifrado avanzado (AES) es compatible y se activa de forma predeterminada, pero puede cambiarlo a AES-256.
- Las conexiones desde todos los tipos de dispositivos cliente.
- Controles de optimización para reducir el uso del ancho de banda en las redes LAN y WAN.
- Las pantallas virtuales admiten color de 32 bits.
- Compatible con fuentes ClearType.
- Redirección de audio con ajuste de calidad de audio dinámico para LAN y WAN.
- Audio y vídeo en tiempo real para usar cámaras web y micrófonos en algunos tipos de cliente.
- Opción de copiar y pegar texto (y también imágenes en algunos clientes) entre el sistema operativo cliente y una aplicación publicada o escritorio remoto. En otros tipos de cliente, solo se puede copiar texto sin formato. No es posible copiar y pegar objetos del sistema, como carpetas y archivos, de un sistema a otro.
- En algunos tipos de cliente, se pueden utilizar varios monitores. En algunos casos, puede usar hasta 4 monitores con una resolución de hasta 2560 x 1600 en cada uno o 3 monitores con una resolución de 4K (3840 x 2160) para escritorios remotos de Windows 7 en los que se deshabilite Aero. También son compatibles las opciones de autoajustar y rotar la pantalla.

Al habilitar la función 3D, se admiten hasta 2 monitores con una resolución de hasta 1920 x 1200 o un único monitor con una resolución de 4K (3840 x 2160).

- En algunos tipos de cliente, se admite el redireccionamiento USB.
- El redireccionamiento MMR es compatible con algunos sistemas operativos cliente Windows y algunos sistemas operativos de escritorio remoto (que tengan instalado Horizon Agent).

Para obtener información sobre los sistemas operativos de escritorio compatibles con funciones específicas de PCoIP, consulte [Matriz de compatibilidad de funciones para Horizon Agent](#).

Acceda a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html> para obtener información sobre los dispositivos cliente compatibles con funciones específicas de PCoIP.

Configuración recomendada para los sistemas operativos invitados

Se recomienda 1 GB o más de RAM y una CPU dual para reproducir en alta definición, modo en pantalla completa, o bien vídeos de 720p o con un formato superior. Si desea utilizar Virtual Dedicated Graphics Acceleration para aplicaciones con gráficos avanzados, como aplicaciones CAD, necesita 4 GB de RAM.

Requisitos de calidad de vídeo

Vídeo con formato de 480p

Puede reproducir vídeo con una resolución nativa de 480p o inferior si el escritorio remoto tiene una única CPU virtual. Si desea reproducir el vídeo en Flash de alta definición o en modo de pantalla completa, el escritorio requiere una CPU virtual dual. Incluso con un escritorio que tenga doble CPU virtual, es posible que el vídeo con formato de 360p que se reproduce en modo de pantalla completa se retrase con respecto al audio, sobre todo en el caso de clientes Windows.

Vídeo con formato de 720p

Puede reproducir vídeo de 720p en resoluciones nativas si el escritorio remoto tiene una CPU virtual doble. El rendimiento puede verse afectado si reproduce vídeos en 720p en alta definición o en modo de pantalla completa.

Vídeo con formato de 1080p

Si el escritorio remoto tiene una CPU virtual doble, puede reproducir vídeo con formato de 1080p, aunque es posible que el reproductor deba ajustarse a una ventana más pequeña.

Procesamiento 3D

Puede configurar escritorios remotos para que utilicen gráficos de aceleración de hardware o software. La función de gráficos de aceleración de software le permite ejecutar aplicaciones de OpenGL 2.1 y DirectX9 sin necesidad de una unidad de procesamiento de gráficos (GPU) física. Las funciones de gráficos de aceleración de hardware permiten que las máquinas virtuales compartan sus GPU (unidades de procesamiento gráfico) físicas en un host de vSphere o bien dediquen una GPU física a un único escritorio de máquina virtual.

Para las aplicaciones 3D, se admiten hasta 2 monitores y la resolución de pantalla máxima es 1920 x 1200. El sistema operativo invitado en los escritorios remotos debe ser Windows 7 o posterior.

Para obtener más información sobre las funciones 3D, consulte [Utilizar aplicaciones de gráficos 3D](#).

Requisitos de hardware para los sistemas cliente

Para obtener información sobre los requisitos del procesador y la memoria, consulte el tipo de escritorio o dispositivo cliente móvil específico en el documento "Uso de VMware Horizon Client". Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Microsoft RDP

El Protocolo de escritorios remotos es el mismo protocolo multicanal que muchos usuarios ya utilizan para acceder al equipo de trabajo desde el equipo personal. La conexión a Escritorio remoto de Microsoft (RDC) usa RDP para enviar datos.

Microsoft RDP es un protocolo de visualización compatible con los escritorios remotos que usan máquinas virtuales, equipos físicos o escritorios de sesión compartida en un host RDS. (Únicamente los protocolos de visualización VMware Blast y PCoIP se admiten en las aplicaciones publicadas). Microsoft RDP proporciona las siguientes funciones:

- RDP 7 es compatible con varios monitores de confianza, admitiendo hasta 16 monitores.
- Puede copiar y pegar texto y objetos del sistema como carpetas y archivos entre el sistema local y el escritorio remoto.
- Las pantallas virtuales admiten color de 32 bits.
- RDP admite el cifrado de 128 bits.
- Los usuarios que se encuentren fuera del firewall empresarial pueden usar este protocolo con la red privada virtual (VPN) de su compañía o pueden establecer conexiones cifradas y seguras al servidor de seguridad de View en la DMZ empresarial.

Para admitir las conexiones TLSv1.1 y TLSv1.2 en Windows 7 y Windows Server 2008 R2, debe aplicar la revisión de Microsoft KB3080079.

Requisitos de hardware para los sistemas cliente

Para obtener más información sobre los requisitos del sistema y del procesador, consulte el documento "Uso de VMware Horizon Client" para el tipo específico de sistema cliente. Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Nota Los dispositivos cliente móviles 3.x únicamente usan el protocolo de visualización PCoIP. Los dispositivos cliente móviles 4.x solo usan el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast.

Utilizar aplicaciones publicadas

También puede utilizar Horizon Client para acceder de forma segura a las aplicaciones publicadas basadas en Windows, además de acceder a los escritorios remotos.

Con esta función, después de iniciar Horizon Client e iniciar sesión en un servidor de Horizon 7, los usuarios ven todas las aplicaciones publicadas para las que tienen autorización, además de los escritorios remotos. Al seleccionar una aplicación, se abre una ventana para dicha aplicación en el dispositivo cliente local, con la misma apariencia y comportamiento que si estuviera instalada localmente.

Por ejemplo, en un equipo cliente Windows, si se minimiza la ventana de la aplicación, permanece un elemento para esa aplicación en la barra de tareas, con la misma apariencia que si estuviera instalada en el equipo Windows local. También se puede crear un acceso directo para la aplicación que aparecerá en el escritorio del cliente, al igual que los accesos directos de las aplicaciones instaladas localmente.

Es preferible implementar aplicaciones publicadas de esta manera a implementar escritorios remotos completos cuando se dan las siguientes condiciones:

- Si una aplicación se configura con una arquitectura de varios niveles, en la que los componentes funcionan mejor si se encuentran geográficamente cerca unos de otros, el uso de aplicaciones publicadas es una buena solución.

Por ejemplo, cuando un usuario necesita acceder a una base de datos de forma remota, si se necesitan transmitir grandes cantidades de datos a través de la WAN, el rendimiento se suele ver afectado. Gracias a las aplicaciones publicadas, todas las partes de la aplicación se pueden encontrar en el mismo centro de datos que la base de datos, por lo que el tráfico está aislado y solo se envían las actualizaciones de pantalla a través de la WAN.

- Desde un dispositivo móvil, es más fácil acceder a una aplicación individual que abrir un escritorio remoto de Windows y, a continuación, acceder a la aplicación.

Para utilizar esta función, las aplicaciones se instalan en un host Microsoft RDS. A este respecto, las aplicaciones publicadas de Horizon 7 funcionan de forma similar a otras soluciones de aplicaciones remotas. Las aplicaciones publicadas de Horizon 7 se distribuyen mediante el protocolo de visualización Blast Extreme o el protocolo de visualización PCoIP para optimizar la experiencia del usuario.

Usar Horizon Persona Management para conservar datos y configuraciones de los usuarios

Puede utilizar Horizon Persona Management con escritorios remotos, equipos físicos y máquinas virtuales no administradas por Horizon 7. Persona Management conserva los cambios realizados por los usuarios en sus perfiles. Los perfiles de usuario incluyen diversa información generada por los usuarios.

- Configuraciones de escritorio y datos específicos del usuario que permiten que la apariencia del escritorio sea la misma, independientemente del escritorio en el que inicie la sesión el usuario.
- Configuraciones y datos de las aplicaciones. Por ejemplo, estas configuraciones permiten a las aplicaciones recordar las preferencias y posiciones de la barra de herramientas.
- Entradas del registro configuradas por aplicaciones del usuario.

Para posibilitar estas funciones, Persona Management necesita un espacio de almacenamiento en un recurso compartido CIFS igual o mayor que el tamaño del perfil local del usuario.

Minimizar los tiempos de inicio y cierre de sesión

Persona Management minimiza el tiempo que se necesita para iniciar y cerrar la sesión en los escritorios. De forma predeterminada, durante el inicio de sesión, Horizon 7 descarga solo los archivos necesarios para Windows, como los archivos del registro. Horizon 7 lee los cambios realizados en el perfil del escritorio remoto y los copia al repositorio remoto a intervalos regulares.

Persona Management evita tener que hacer cambios en Active Directory para disponer de un perfil administrado. Para configurar Persona Management, se especifica un repositorio central, sin cambiar las propiedades del usuario en Active Directory. Este repositorio central permite administrar el perfil de un usuario en un entorno sin afectar a las máquinas físicas en las que los usuarios puedan también iniciar la sesión.

Con Persona Management, si se aprovisionan escritorios con aplicaciones de VMware ThinApp, los datos del entorno de pruebas de ThinApp también se pueden almacenar en el perfil del usuario. Estos datos pueden trasladarse en itinerancia junto con el usuario, pero no afectan significativamente a los tiempos de inicio de sesión. Esta estrategia proporciona una mayor protección frente a los daños o la pérdida de datos.

Opciones de configuración

Es posible configurar personas de Horizon 7 en varios niveles: un único escritorio remoto, un grupo de escritorios, un OU o todos los escritorios remotos de la implementación. También se puede utilizar una versión independiente de Persona Management en equipos físicos y máquinas virtuales que Horizon 7 no administre.

Al instalar directivas de grupo (GPO) se dispone de un control granular de los archivos y carpetas a incluir en una persona. Es posible especificar si se incluye o no la carpeta de configuración local, los archivos que se cargarán al iniciar sesión, los archivos que se descargarán después de que el usuario inicie la sesión y los archivos dentro de la identidad de un usuario que se administrarán mediante la función de perfiles de itinerancia de Windows en lugar de hacerlo mediante Persona Management.

Al igual que en los perfiles de itinerancia de Windows, es posible configurar el redireccionamiento de carpetas. Es posible redirigir a un recurso compartido de red las siguientes carpetas.

Contactos	Mis documentos	Guardar juegos
Cookies	Mi música	Búsquedas
Escritorio	Mis imágenes	Menú Inicio
Descargas	Mis vídeos	Elementos de inicio
Favoritos	Entorno de red	Plantillas
Historial	Entorno de impresoras	Archivos temporales de Internet
Vínculos	Elementos recientes	

Limitaciones

Persona Management tiene las siguientes limitaciones y restricciones:

- Esta función no es compatible con grupos de escritorios de clones instantáneos.
- Es necesario tener una licencia de Horizon 7 que incluya el componente Persona Management.
- Persona Management requiere un recurso compartido CIFS (Sistema de archivos de Internet común).
- Esta función no es compatible con el uso de discos persistentes en grupos de escritorios de clones vinculados de Windows 10.

Usar dispositivos USB con aplicaciones y escritorios remotos

Los administradores pueden configurar que se puedan usar los dispositivos USB, como unidades de memoria flash, cámaras, dispositivos VoIP (voz sobre IP) e impresoras, desde un escritorio virtual. Esta función se denomina redireccionamiento USB. Un escritorio virtual puede admitir hasta 255 dispositivos USB.

También puede redireccionar algunos dispositivos USB conectados localmente para usarlos en aplicaciones y escritorios publicados. Para obtener más información sobre los tipos específicos de dispositivos que se admiten, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Cuando use esta función en grupos de escritorios que se implementan en máquinas de usuario único, la mayoría de los dispositivos USB que están conectados al sistema cliente están disponibles en el escritorio remoto. Incluso puede conectar un iPad y administrarlo desde un escritorio remoto. Por ejemplo, puede sincronizar el iPad con el iTunes que está instalado en el escritorio remoto. En algunos dispositivos cliente, como los equipos Windows y Mac, los dispositivos USB aparecen en un menú de Horizon Client. Este menú permite conectar y desconectar los dispositivos.

En la mayoría de los casos, no puede usar un dispositivo USB en el sistema cliente y en el escritorio remoto al mismo tiempo. Solo se pueden compartir algunos tipos de dispositivos USB entre el escritorio remoto y el equipo local. Estos dispositivos incluyen lectores de tarjetas inteligentes y dispositivos de interfaz humana, como teclados y dispositivos señaladores.

Los administradores pueden especificar los tipos de dispositivos USB a los que los usuarios finales pueden conectarse. En los dispositivos compuestos que contengan varios tipos de dispositivos, como un dispositivo de entrada de vídeo y uno de almacenamiento, en algunos sistemas cliente, los administradores pueden dividir el dispositivo, de forma que se permita un dispositivo (por ejemplo, el de entrada de vídeo) pero el otro no (por ejemplo, el de almacenamiento).

La función Redireccionamiento USB solo está disponible en algunos tipos de clientes. Para saber si un cliente concreto admite la función, consulte la matriz de compatibilidad de funciones en el documento de instalación y configuración de Horizon Client de ese cliente.

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

Con la función Audio/vídeo en tiempo real, puede utilizar el micrófono o la cámara web del sistema cliente local en un escritorio remoto o aplicación publicada. Audio/vídeo en tiempo real es compatible con las aplicaciones de vídeo basadas en el navegador y las aplicaciones de conferencia estándar. Admite la entrada de audio analógico, dispositivos USB de audio y cámaras web estándar.

Los usuarios finales pueden ejecutar Skype, WebEx, Google Hangouts y otras aplicaciones de conferencias en los escritorios remotos. Esta función redirecciona los datos de audio y vídeo a la máquina agente con un ancho de banda inferior al que se puede alcanzar utilizando un redireccionamiento USB. Con la función Audio/vídeo en tiempo real, la entrada de audio y las imágenes de la cámara web se codifican en el sistema cliente y, a continuación, se envían a la máquina cliente. En la máquina agente, una cámara virtual y un micrófono virtual pueden descodificar y reproducir la transmisión que puede usar la aplicación externa.

No es necesaria una configuración especial, aunque los administradores pueden establecer claves de registro y directivas de grupo del lado del agente para configurar la velocidad de fotogramas y la resolución de imágenes, o desactivar la función. De forma predeterminada, la resolución es de 320 x 240 píxeles en 15 fotogramas por segundo. Si es necesario, los administradores pueden utilizar las opciones de configuración del lado del cliente para configurar un dispositivo de audio o una cámara web preferida.

Nota Esta función está disponible solo en algunos tipos de clientes. Para saber si un tipo de cliente concreto admite la función, consulte la matriz de compatibilidad de funciones en el documento de instalación y configuración del tipo específico de dispositivo de cliente móvil o de escritorio.

Utilizar aplicaciones de gráficos 3D

Las funciones de gráficos con aceleración por hardware y software disponibles con el protocolo de visualización Blast Extreme o PCoIP permiten que los usuarios de escritorios remotos ejecuten aplicaciones 3D como Google Earth, aplicaciones CAD y otras aplicaciones que hacen un uso intensivo de gráficos.

NVIDIA GRID vGPU (aceleración por hardware GPU compartido)

Esta función, disponible con vSphere 6.0 y versiones posteriores, permite compartir una GPU (unidad de procesamiento de gráficos) física en un host ESXi entre máquinas virtuales. Esta función se utiliza si se necesita utilizar gráficos de estación de trabajo con aceleración por hardware de alta gama.

GPU AMD multiusuario con vDGA

Esta función, disponible con vSphere 6.0 y versiones posteriores, permite que varias máquinas virtuales compartan una GPU AMD haciendo que la GPU aparezca como varios dispositivos PCI de paso. Esta función ofrece perfiles 3D con aceleración por hardware flexibles, que van desde trabajadores que realizan tareas ligeras con gráficos 3D hasta usuarios avanzados de gráficos de estación de trabajo.

**Aceleración Virtual
Dedicated Graphics
Acceleration (vDGA)**

Esta función, disponible con vSphere 5.5 Update 2 y versiones posteriores, dedica una sola GPU física de un host ESXi a una única máquina virtual. Esta función se utiliza si se necesita utilizar gráficos de estación de trabajo con aceleración por hardware de alta gama.

Nota Algunas tarjetas Intel vDGA requieren una versión específica de vSphere 6. Consulte la lista de compatibilidad de hardware de VMware en <http://www.vmware.com/resources/compatibility/search.php>. Además, en el caso de Intel vDGA, se utiliza la GPU integrada de Intel en lugar de GPU discretas, como ocurre con otros proveedores.

**Aceleración Virtual
Shared Graphics
Acceleration (vSGA)**

Esta función, disponible con vSphere 5.5 Update 2 y versiones posteriores, permite que varias máquinas virtuales compartan GPU físicas de hosts ESXi. Se pueden utilizar aplicaciones 3D para diseño, modelado y multimedia.

Soft 3D

Los gráficos con aceleración por software, disponibles con vSphere 5.5 Update 2 y versiones posteriores, permiten ejecutar aplicaciones DirectX 9 y OpenGL 2.1 sin necesidad de una GPU física. Esta función se utiliza para aplicaciones 3D menos exigentes, como los temas Aero de Windows, Microsoft Office 2010 y Google Earth.

NVIDIA GRID vGPU y vDGA ya se admiten en aplicaciones publicadas que se ejecutan en hosts Microsoft RDS.

Importante Para obtener más información sobre las diversas opciones y requisitos del procesamiento 3D, consulte el [documento técnico de VMware](#) sobre gráficos, la [Guía de implementación de NVIDIA GRID vGPU para VMware Horizon 6.1](#) y la [guía de usuario de GPU virtual de NVIDIA GRID](#).

Transmisión de multimedia a un escritorio remoto

La función Windows Media MMR (redireccionamiento multimedia), para escritorios y clientes Windows 7 y Windows 8/8.1, permite la reproducción con la fidelidad original en equipos cliente Windows al transmitir archivos multimedia a un escritorio remoto.

Con el redireccionamiento multimedia (MMR), la transmisión multimedia se procesa, es decir, se descodifica, en el sistema cliente Windows. El sistema cliente reproduce el contenido multimedia, por lo que se descarga la demanda en el host ESXi. Son compatibles los formatos de medios compatibles con Windows Media Player; por ejemplo: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 y 9; WMA; AVI; ACE; MP3; WAV.

Nota Se debe agregar el puerto MMR como una excepción al software de firewall. El puerto predeterminado para MMR es el 9427.

Imprimir desde un escritorio remoto

La función de impresión virtual permite a los usuarios finales de algunos sistemas cliente utilizar impresoras locales o de red desde un escritorio remoto sin que sea necesario que los controladores de impresión estén instalados en el sistema operativo del escritorio remoto. La función de impresión basada en la ubicación permite asignar escritorios remotos a la impresora más cercana al dispositivo cliente endpoint.

En la impresión virtual, después de agregar una impresora a un equipo cliente local, la impresora se agrega automáticamente a la lista de impresoras disponibles del escritorio remoto. No necesita realizar ningún tipo de configuración. En cada impresora disponible en esta función, puede configurar las preferencias relativas a la compresión de datos, la calidad de la impresión, la impresión a doble cara, el color, etc. Los usuarios con privilegios de administrador pueden instalar controladores de impresión en el escritorio remoto sin crear un conflicto con el componente de impresión virtual.

El redireccionamiento de la impresora local está diseñado para los siguientes escenarios de uso:

- Impresoras conectadas directamente a puertos serie o USB del dispositivo cliente
- Impresoras especializadas, como impresoras de códigos de barras o de etiquetas conectadas al equipo cliente
- Impresoras de red en una red remota que no se puedan direccionar desde la sesión virtual.

Para enviar tareas de impresión a una impresora USB, se puede utilizar la función de redireccionamiento USB o la función de impresión virtual.

La función de impresión basada en la ubicación permite que las organizaciones de TI asignen escritorios remotos a la impresora más cercana al dispositivo cliente endpoint. Por ejemplo, si un médico se desplaza de una sala a otra de un hospital, cada vez que imprime un documento, este se envía a la impresora más próxima. Para utilizar esta función, es necesario que los controladores adecuados estén instalados en el escritorio remoto.

Nota Estas funciones de impresión solo están disponibles en algunos tipos de clientes. Para saber si un tipo de cliente concreto admite la función de impresión, consulte la matriz de compatibilidad de funciones en la guía de instalación y configuración del tipo específico de dispositivo de cliente móvil o de escritorio. Acceda a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Utilizar single sign-on para iniciar sesión

La función single sign-on (SSO) permite que los usuarios finales solo tengan que introducir sus credenciales de inicio de sesión de Active Directory una vez.

Si no se utiliza la función single sign-on, los usuarios finales deberán iniciar sesión dos veces. Primero, se les solicitarán las credenciales de Active Directory para iniciar sesión en el servidor de conexión de Horizon y, a continuación, que inicien sesión en sus escritorios remotos. Si se utilizan también tarjetas inteligentes, los usuarios finales deberán iniciar sesión tres veces, porque también deberán hacerlo cuando el lector de tarjetas inteligentes les solicite un PIN.

En escritorios remotos, esta función incluye una biblioteca de vínculo dinámico de proveedores de credenciales.

True SSO

Con la función True SSO, ya no es necesario que los usuarios proporcionen las credenciales de Active Directory. Después de que los usuarios inicien la sesión en VMware Identity Manager mediante algún método distinto a AD (por ejemplo, autenticación RSA SecurID o RADIUS), no se les pide que introduzcan también credenciales de Active Directory para utilizar una aplicación o un escritorio remotos.

Si un usuario se autentica mediante tarjetas inteligentes o credenciales de Active Directory, la función True SSO no es necesaria, pero se puede configurar True SSO para que se use incluso en este caso. Entonces se ignorarán todas las credenciales de AD proporcionadas por el usuario y se usará True SSO.

True SSO funciona generando un certificado único y con una validez corta para el proceso de inicio de sesión de Windows. Para generar certificados de validez corta en nombre del usuario, es necesario configurar una entidad de certificación, si aún no se tiene una, y un servidor de inscripción de certificados. Para instalar el servidor de inscripción, se ejecuta el instalador del servidor de conexión y se selecciona la opción Servidor de inscripción.

True SSO separa la autenticación (validación de la identidad de un usuario) del acceso (como el acceso a una aplicación o escritorio de Windows). Las credenciales de usuario se aseguran mediante un certificado digital. No se almacena ni transfiere ninguna contraseña en el centro de datos. Para obtener más información, consulte el documento *Administración de Horizon 7*.

Resolución de pantalla y monitores

Puede ampliar un escritorio remoto a varios monitores. Si cuenta con un monitor de alta resolución, puede ver la aplicación o el escritorio remotos en alta resolución.

Para visualizar un escritorio remoto en varios monitores, se puede seleccionar el modo de visualización Todos los monitores. Si utiliza el modo Todos los monitores y hace clic en el botón Minimizar, al maximizar la ventana, esta volverá a dicho modo. De forma similar, si utiliza el modo Pantalla completa y minimiza la ventana, cuando la maximice, esta volverá a dicho modo en uno de los monitores.

Usar todos los monitores con una configuración de varios monitores

Independientemente del protocolo de visualización, puede usar varios monitores con un escritorio remoto. Si configuró Horizon Client para que use todos los monitores, al maximizar la ventana de una aplicación se ampliará a pantalla completa solo en el monitor en el que se encuentra.

Horizon Client es compatible con las siguientes configuraciones del monitor:

- Si utiliza dos monitores, no es necesario que se encuentren en el mismo modo. Por ejemplo, si usa un portátil conectado a un monitor externo, este puede presentar una orientación vertical u horizontal.

- Los monitores pueden estar colocados uno al lado del otro, o bien apilados de dos en dos o en vertical solo si utiliza dos monitores y la altura total es inferior a 4096 píxeles.
- Para usar la función de procesamiento 3D, debe utilizar los protocolos de visualización VMware Blast o PCoIP. Puede utilizar hasta dos monitores con una resolución máxima de 1920x1200. Con una resolución de 4K (3840x2160) solo se admite un monitor.
- Gracias a los protocolos de visualización VMware Blast o PCoIP, se admite una resolución de pantalla de escritorio remoto de 4K (3840 x 2160). El número de pantallas 4K que se admite depende de la versión de hardware de la máquina virtual de escritorio y la versión de Windows.

Versión de hardware	Versión de Windows	Número de pantallas 4K admitidas
10 (compatible con ESXi 5.5.x)	7, 8, 8.x, 10	1
11 (compatible con ESXi 6.0)	7 (funciones de representación 3D y Windows Aero deshabilitadas)	3
11	7 (función de representación 3D habilitada)	1
11	8, 8.x, 10	1
13 o 14	7, 8, 8.x, 10 (función de representación 3D habilitada)	1
13 o 14	7, 8, 8.x, 10	4

- Si utiliza Microsoft RDP 7, el número máximo de monitores que puede usar para mostrar un escritorio remoto es 16.
- Si utiliza el protocolo de visualización Microsoft RDP, debe tener instalada en el escritorio remoto la versión 6.0 de la Conexión a Escritorio remoto (RDC) de Microsoft o una posterior.

Usar un monitor en una configuración de varios monitores

Si dispone de varios monitores pero desea que Horizon Client use únicamente uno de ellos, puede seleccionar que una ventana del escritorio remoto se inicie en otro modo que no sea Todos los monitores. De forma predeterminada, la ventana se abre en el monitor principal. Para obtener más información, consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.

Uso del modo de alta resolución

En algunos tipos de clientes, si usa el protocolo de visualización VMware Blast o PCoIP, Horizon Client también admite resoluciones muy elevadas para aquellos sistemas cliente con pantallas de alta resolución. La opción para habilitar el modo de alta resolución aparece únicamente si el sistema cliente es compatible con pantallas de alta resolución.

La codificación de hardware se habilita de forma predeterminada tras configurar vGPU en la máquina virtual. La codificación de hardware está habilitada para todas las configuraciones de varios monitores excepto para los perfiles de vGPU que utilicen menos de 1GB de memoria de vídeo, que usarán el decodificador de software debido a las restricciones de memoria NVENC. Consulte *NVENC requiere al menos 1 GB de búfer de fotogramas* en <https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vmware/index.html>

Administrar grupos de aplicaciones y escritorios desde una ubicación centralizada

3

Es posible crear grupos de escritorios que incluyan un escritorio remoto, cientos o miles de ellos. Como origen de escritorios, se pueden utilizar máquinas virtuales, máquinas físicas y hosts de Windows Remote Desktop Services (RDS). Se puede crear una máquina virtual como imagen de base y que Horizon 7 genere un grupo de escritorios remotos a partir de ella. También se pueden crear grupos de aplicaciones que proporcionen acceso remoto a las aplicaciones a los usuarios.

Este capítulo incluye los siguientes temas:

- [Ventajas de los grupos de escritorios](#)
- [Ventajas de los grupos de aplicaciones](#)
- [Reducir y administrar requisitos de almacenamiento](#)
- [Aprovisionamiento de aplicaciones](#)
- [Utilizar GPO de Active Directory para administrar usuarios y escritorios](#)

Ventajas de los grupos de escritorios

Horizon 7 ofrece la capacidad de crear y aprovisionar grupos de escritorios como base de la administración centralizada.

Los grupos de escritorios remotos se crean a partir de una de las siguientes fuentes:

- Un sistema físico, como un equipo de escritorio físico.
- Una máquina virtual alojada en un host ESXi y administrada por vCenter Server
- Una máquina virtual que se ejecute sobre una plataforma de virtualización que no sea vCenter Server y que sea compatible con Horizon Agent.
- Un escritorio basado en sesiones en un host RDS. Para obtener más información sobre cómo crear grupos de escritorios desde un host RDS, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Si utiliza una máquina virtual vSphere como origen de escritorios, puede automatizar el proceso de crear tantos escritorios virtuales idénticos como necesite. Puede establecer un número mínimo y máximo de escritorios virtuales para que se generen para el grupo. Establecer estos parámetros garantiza disponer siempre de suficientes escritorios remotos disponibles para su uso inmediato, pero no tantos que se usen en exceso los recursos disponibles.

Utilizar grupos para administrar escritorios le permite aplicar ajustes o implementar aplicaciones en todos los escritorios remotos de un grupo. En los siguientes ejemplos, se muestran algunos de los ajustes disponibles:

- Especifique qué protocolo de visualización remota debe usarse como predeterminado para el escritorio remoto y si se permite a los usuarios finales invalidar el protocolo predeterminado.
- En el caso de máquinas virtuales de clones completos o de máquinas virtuales de clones vinculados de View Composer, especifique si se debe apagar la máquina virtual cuando no se esté utilizando y si debe eliminarse por completo. Las máquinas virtuales de clones instantáneos siempre están encendidas.
- En el caso de las máquinas virtuales de clones vinculados de View Composer, puede especificar si se debe usar una especificación de personalización Microsoft Sysprep o QuickPrep desde VMware. Sysprep genera un SID y GUID únicos para cada máquina virtual del grupo. Los clones instantáneos requieren una especificación de personalización diferente, denominada ClonePrep, desde VMware.

También puede especificar cómo se asignan a los usuarios los escritorios de un grupo.

Grupos de asignación dedicada

Cada uno de los usuarios se asigna a un escritorio remoto determinado y vuelve en cada inicio de sesión al mismo escritorio. Los grupos de asignación dedicada requieren un escritorio por cada usuario. Por ejemplo, para un grupo de 100 usuarios se necesita un grupo de 100 escritorios.

Grupos de asignación flotante

El uso de grupos de asignación flotante también le permite crear un grupo de escritorios que puedan utilizar turnos de usuarios. Por ejemplo, un grupo de 100 escritorios podría ser utilizado por 300 usuarios si estos trabajasen en grupos de 100 usuarios por turno. El escritorio remoto se elimina de manera opcional y se vuelve a crear después de cada uso, lo que ofrece un entorno altamente controlado.

Ventajas de los grupos de aplicaciones

En los grupos de aplicaciones, usted da a los usuarios acceso a las aplicaciones que se ejecutan en los servidores de un centro de datos en lugar de en sus dispositivos o equipos personales.

Los grupos de aplicaciones ofrecen varias ventajas importantes:

- **Accesibilidad**
Los usuarios pueden acceder a las aplicaciones desde cualquier lugar de la red. También puede configurar el acceso seguro a la red.
- **Independencia de los dispositivos**

Con los grupos de aplicaciones, puede ofrecer compatibilidad con un rango de dispositivos cliente, como smartphones, tablets, portátiles, clientes ligeros y equipos personales. Los dispositivos cliente pueden ejecutar varios sistemas operativos, como Windows, iOS, Mac OS o Android.

- **Control de acceso**

Puede conceder o retirar el acceso a las aplicaciones para un usuario o grupo de usuarios de forma rápida y sencilla.

- **Implementación acelerada**

Con los grupos de aplicaciones, se puede acelerar la implementación de las aplicaciones porque solo se implementan aplicaciones en los servidores de un centro de datos y cada servidor admite varios usuarios.

- **Facilidad de administración**

Administrar software implementado en dispositivos y equipos cliente requiere por lo general una cantidad considerable de recursos. Las tareas de administración incluyen la implementación, la configuración, el mantenimiento, el soporte y las actualizaciones. Con los grupos de aplicaciones, puede simplificar la administración de software en una empresa porque el software se ejecuta en servidores de un centro de datos, lo que requiere menos copias instaladas.

- **Seguridad y cumplimiento normativo**

Con los grupos de aplicaciones, puede mejorar la seguridad porque las aplicaciones y sus datos asociados están ubicados de forma centralizada en un centro de datos. Los datos centralizados pueden gestionar problemas de seguridad y cumplimiento normativo.

- **Costo reducido**

Dependiendo de los acuerdos de licencia de software, puede que sea más rentable alojar las aplicaciones en un centro de datos. Otros factores, entre los que se incluyen una implementación acelerada y una mejor administración, también pueden reducir el costo del software en una empresa.

Reducir y administrar requisitos de almacenamiento

Implementar escritorios en máquinas virtuales administradas por vCenter Server proporciona la eficiencia de almacenamiento que solo estaba disponible previamente para servidores virtualizados. El uso de clones instantáneos o de clones vinculados de Composer como máquinas de escritorios aumenta el ahorro de almacenamiento porque todas las máquinas virtuales de un grupo comparten un disco virtual con una imagen de base.

- **Administrar almacenamiento con vSphere**

vSphere le permite virtualizar volúmenes de discos y sistemas de archivos para que pueda administrar y configurar almacenamiento sin tener que valorar dónde se almacenan físicamente los datos.

- **Utilizar VMware vSAN para almacenamiento de alto rendimiento y administración basada en directivas**

VMware vSAN es un nivel de almacenamiento definido por software, disponible con vSphere 5.5 Update 2 o una versión posterior, que virtualiza los discos de almacenamiento físicos y locales disponibles en un clúster de hosts de vSphere. Especifique solo un almacén de datos cuando cree un grupo de escritorios automatizado o una granja automatizada, y los distintos componentes, como los archivos de la máquina virtual, las réplicas, los datos de usuario y los archivos del sistema operativo, se ubican en los discos de la unidad de estado sólido (SSD) o los discos duro de conexión directa (HDD).

- **Usar Virtual Volumes con el almacenamiento situado en máquinas virtuales y la administración basada en directivas**

Con Virtual Volumes (VVols), disponible con vSphere 6.0 o una versión posterior, una máquina virtual individual, no un almacén de datos, pasa a ser una unidad de administración del almacenamiento. El hardware de almacenamiento obtiene más control sobre la administración, el diseño y el contenido del disco virtual.

- **Reducir requisitos de almacenamiento con Composer**

Como Composer crea imágenes de escritorio que comparten discos virtuales con una imagen de base, puede reducir entre un 50 y un 90 por ciento la capacidad de almacenamiento necesaria.

- **Reducir requisitos de almacenamiento con clones instantáneos**

La función de clones instantáneos usa la tecnología vSphere vmFork (disponible con vSphere 6.0 U1 y versiones posteriores) para poner en modo inactivo una imagen base que se está ejecutando, o una máquina virtual principal y crear y personalizar rápidamente un grupo de escritorios virtuales.

Administrar almacenamiento con vSphere

vSphere le permite virtualizar volúmenes de discos y sistemas de archivos para que pueda administrar y configurar almacenamiento sin tener que valorar dónde se almacenan físicamente los datos.

Las matrices Fibre Channel SAN, iSCSI SAN y NAS son tecnologías de almacenamiento muy utilizadas que se basan en vSphere para satisfacer las necesidades de almacenamiento de los distintos centros de datos. Las matrices de almacenamiento están conectadas a los grupos de servidores a través de redes de área de almacenamiento y compartidas entre dichos grupos. Esta disposición permite la adición de recursos de almacenamiento y proporciona más flexibilidad para aprovisionarlos a máquinas virtuales.

Funciones compatibles con vSphere 5.5 Update 2 o versiones posteriores

vSphere 5.5 Update 2 y las versiones posteriores permiten utilizar vSAN, que virtualiza los discos físicos de estado sólido y las unidades de disco duro disponibles en hosts ESXi en un único almacén de datos compartido por todos los hosts de un clúster. vSAN proporciona almacenamiento de alto rendimiento con administración basada en directivas, para que así especifique solo un almacén de datos cuando cree un grupo de escritorios, y los distintos componentes, como archivos de máquina virtual, réplicas, datos de usuario y archivos del sistema operativo, se ubiquen en los correspondientes discos SSD (unidades de estado sólido) o HDD (unidades de disco duro) de conexión directa.

vSAN también le permite administrar el rendimiento y el almacenamiento de la máquina virtual a través de los perfiles de directivas de almacenamiento. Si la directiva se vuelve incompatible por un fallo de red, disco o host, o por cambios en la carga de trabajo, vSAN volverá a configurar los datos de las máquinas virtuales afectadas y optimizará el uso de recursos en el clúster. Puede implementar un grupo de escritorios en un clúster que contenga hasta 20 hosts ESXi.

Además de respaldar funciones de VMware que requieren almacenamiento compartido, como HA, vMotion y DRS, vSAN elimina la necesidad de contar con un almacenamiento compartido externo y simplifica la configuración de almacenamiento y las actividades de aprovisionamiento de las máquinas virtuales.

Importante La función vSAN disponible con vSphere 6.0 y versiones posteriores contiene muchas mejoras de rendimiento. Con vSphere 6.0, esta función también tiene una mayor compatibilidad de hardware (HCL). Para obtener más información sobre vSAN en vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware vSAN*.

Nota vSAN es compatible con la función de acelerador de almacenamiento de View, pero no con la función de formato de disco de espacio eficiente, que recupera espacio de disco mediante la reducción y el borrado de discos.

Con vSphere 5.5 Update 2 o una versión posterior, puede usar las siguientes funciones:

- Con la función de acelerador de almacenamiento de View, puede configurar hosts ESXi para almacenar datos del disco de la máquina virtual.

Usar el almacenamiento de caché de lectura basada en el contenido (CBRC) puede reducir las operaciones de E/S por segundo y mejorar el rendimiento durante el arranque simultáneo de máquinas virtuales, cuando muchas máquinas se inician y ejecutan análisis antivirus al mismo tiempo. En lugar de leer todo el SO desde el sistema de almacenamiento una y otra vez, un host puede leer bloques de datos comunes desde la caché.
- Si los escritorios remotos utilizan el formato de disco para eficiencia del espacio disponible en vSphere 5.1 y versiones posteriores, el espacio ocupado por los datos antiguos o borrados dentro de un sistema operativo invitado se recupera automáticamente mediante un proceso de limpieza y reducción.
- Los discos de réplica deben almacenarse en almacenes de datos VMFS5 o posteriores, o bien en almacenes de datos NFS. Si almacena réplicas en una versión de VMFS anterior a VMFS5, un clúster puede tener como máximo ocho hosts. Los discos de SO y los discos persistentes se pueden almacenar en almacenes de datos NFS o VMFS.

Funciones compatibles con vSphere 6.0 o versiones posteriores

vSphere 6.0 y las versiones posteriores permiten el uso de Virtual Volumes (VVols). Esta función asigna directamente discos virtuales y sus derivados, clonaciones, snapshots y réplicas a objetos, denominados volúmenes virtuales, de un sistema de almacenamiento. Esta asignación permite a vSphere descargar al sistema de almacenamiento operaciones de almacenamiento intensivas, como snapshots, clonación y replicación.

Virtual Volumes también le permite administrar el rendimiento y el almacenamiento de la máquina virtual a través de los perfiles de directivas de almacenamiento en vSphere. Estos perfiles de directivas de almacenamiento determinan servicios de almacenamiento por máquina virtual. Este tipo de aprovisionamiento granular aumenta el uso de la capacidad. Puede implementar un grupo de escritorios en un clúster que contenga hasta 32 hosts ESXi.

Nota Virtual Volumes es compatible con la función de acelerador de almacenamiento de View, pero no con la función de formato de disco de espacio eficiente, que recupera espacio de disco mediante la reducción y borrado de discos.

Nota Los clones instantáneos no son compatibles con Virtual Volumes.

Utilizar VMware vSAN para almacenamiento de alto rendimiento y administración basada en directivas

VMware vSAN es un nivel de almacenamiento definido por software, disponible con vSphere 5.5 Update 2 o una versión posterior, que virtualiza los discos de almacenamiento físicos y locales disponibles en un clúster de hosts de vSphere. Especifique solo un almacén de datos cuando cree un grupo de escritorios automatizado o una granja automatizada, y los distintos componentes, como los archivos de la máquina virtual, las réplicas, los datos de usuario y los archivos del sistema operativo, se ubican en los discos de la unidad de estado sólido (SSD) o los discos duro de conexión directa (HDD).

vSAN implementa un enfoque basado en directivas para administrar el almacenamiento. Cuando utiliza vSAN, Horizon 7 define los requisitos de almacenamiento de máquina virtual (como capacidad, rendimiento y disponibilidad) en forma de perfiles de directivas de almacenamiento predeterminados y los implementa automáticamente en los escritorios virtuales de vCenter Server. Las directivas se aplican automáticamente e individualmente por disco (objetos de vSAN) y se mantienen durante todo el ciclo de vida del escritorio virtual. El almacenamiento se aprovisiona y se configura automáticamente según las directivas asignadas. Puede modificar estas directivas en vCenter. Horizon crea directivas de vSAN para grupos de escritorios de clones vinculados, grupos de escritorios de clones instantáneos, grupos de escritorios de clones completos o una granja automatizada por clúster de Horizon.

Puede habilitar el cifrado de un clúster vSAN para cifrar todos los datos en reposo (compatibles con todos los tipos de grupos de escritorios de Horizon 7) en el almacén de datos vSAN. El cifrado de vSAN está disponible con la versión 6.6 o posterior de vSAN. Para obtener más información sobre el cifrado de un clúster de vSAN, consulte la documentación de *VMware vSAN*.

Cada máquina virtual mantiene su directiva independientemente de su ubicación física en el clúster. Si la directiva se vuelve incompatible por un fallo de red, disco o host, o por cambios en la carga de trabajo, vSAN volverá a configurar los datos de los equilibradores de carga y de las máquinas virtuales afectadas para cumplir las directivas de cada máquina virtual.

Además de respaldar funciones de VMware que requieren almacenamiento compartido, como HA, vMotion y DRS, vSAN elimina la necesidad de contar con una infraestructura de almacenamiento compartido externo y simplifica la configuración de almacenamiento y las actividades de aprovisionamiento de las máquinas virtuales.

Importante La función vSAN disponible con vSphere 6.0 y versiones posteriores contiene numerosas mejoras de rendimiento en comparación con la función disponible con vSphere 5.5 Update 2. Con vSphere 6.0, esta función también tiene una mayor compatibilidad de hardware (HCL). Además, VMware vSAN 6.0 admite una arquitectura Flash que usa dispositivos basados en Flash para el almacenamiento persistente y en caché.

Requisitos y limitaciones

La función vSAN tiene las siguientes limitaciones cuando se utiliza en una implementación de Horizon 7:

- Esta versión no admite el uso de la función del formato de disco de espacio eficiente de Horizon 7, que recupera espacio de disco al reducir y borrar los discos.
- vSAN no admite la función Array Integration de View Composer (VCAI), ya que vSAN no usa dispositivos NAS.

Nota vSAN es compatible con la función del acelerador de almacenamiento de View. vSAN proporciona una capa de caché en los discos SSD y la función Acelerador de almacenamiento de View proporciona una caché basada en el contenido que reduce la E/S por segundo y mejora el rendimiento durante arranques masivos.

La función vSAN tiene los siguientes requisitos:

- vSphere 5.5 Update 2 o una versión posterior.
- Hardware adecuado. Por ejemplo, VMware recomienda una NIC de 10 GB y, al menos, un SSD y un HDD para cada nodo que aporte capacidad. Para obtener más información, consulte la [Guía de compatibilidad de VMware](#).
- Un clúster de, al menos, tres hosts ESXi. Necesita suficientes hosts ESXi para realizar la configuración, aunque use dos hosts ESXi con un clúster ampliado vSAN. Para obtener más información, consulte el documento *Valores máximos de configuración de vSphere*.
- Una capacidad SSD que sea, como mínimo el 10% de la capacidad del HDD.
- Suficientes HDD para establecer la configuración. No supere el 75% de uso en un disco magnético.

Para más información sobre los requisitos de vSAN, consulte cómo trabajar con vSAN en el documento *Almacenamiento de vSphere 5.5 Update 2*. Para vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware vSAN*. Para obtener más información acerca de ajustar el tamaño y diseñar los componentes clave de las infraestructuras de escritorio virtual de Horizon 7 para VMware vSAN, consulte el documento técnico disponible en <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Usar Virtual Volumes con el almacenamiento situado en máquinas virtuales y la administración basada en directivas

Con Virtual Volumes (VVols), disponible con vSphere 6.0 o una versión posterior, una máquina virtual individual, no un almacén de datos, pasa a ser una unidad de administración del almacenamiento. El hardware de almacenamiento obtiene más control sobre la administración, el diseño y el contenido del disco virtual.

Con Virtual Volumes, los contenedores de almacenamiento abstractos reemplazan los volúmenes de almacenamiento tradicionales basados en recursos compartidos de NFS o LUN. Virtual Volumes asigna discos virtuales y sus derivados, clonaciones, snapshots y réplicas directamente a objetos, llamados volúmenes virtuales, en un sistema de almacenamiento. Con esta asignación, vSphere puede trasladar al sistema de almacenamiento la carga de las operaciones de almacenamiento intensivas como snapshots, clonaciones y réplicas. El resultado, por ejemplo, es que una operación de clonación que antes tardaba una hora, ahora puede tardar unos minutos usando Virtual Volumes.

Importante Una de las ventajas más importantes de Virtual Volumes es la capacidad de usar la administración basada en directivas de software (SPBM). Sin embargo, para esta versión, Horizon 7 no crea las directivas de almacenamiento granular predeterminadas que crea vSAN. En su lugar, puede establecer una directiva de almacenamiento global predeterminada en vCenter Server que se aplique a todos los almacenes de datos de Virtual Volumes.

Virtual Volumes tiene las siguientes ventajas:

- Virtual Volumes admite la descarga de varias operaciones al hardware de almacenamiento. Estas operaciones incluyen la creación de snapshots, el proceso de clonación y Storage DRS.
- Con Virtual Volumes, puede usar servicios de almacenamiento avanzado que incluyen la replicación, el cifrado, la deduplicación y la compresión de discos virtuales individuales.
- Virtual Volumes admite funciones de vSphere como vMotion, Storage vMotion, snapshots, clones vinculados, Flash Read Cache y DRS.
- Puede usar Virtual Volumes con matrices de almacenamiento que admitan vSphere API for Array Integration (VAAI).

Requisitos y limitaciones

La función Virtual Volumes tiene las siguientes limitaciones cuando se utiliza en una implementación de Horizon 7:

- Esta versión no admite el uso de la función del formato de disco de espacio eficiente de Horizon 7, que recupera espacio de disco al reducir y borrar los discos.
- Virtual Volumes no admite el uso de Array Integration de View Composer (VCAI).

- Los almacenes de datos de Virtual Volumes no son compatibles con los grupos de escritorios de clones instantáneos.

Nota Virtual Volumes es compatible con la función del acelerador de almacenamiento de View. vSAN proporciona una capa de caché en los discos SSD y la función Acelerador de almacenamiento de View proporciona una caché basada en el contenido que reduce la E/S por segundo y mejora el rendimiento durante arranques masivos.

La función Virtual Volumes tiene los siguientes requisitos:

- vSphere 6.0 o una versión posterior.
- Hardware adecuado. Algunos proveedores de almacenamiento se encargan de proporcionar tipos de almacenamiento que se pueden integrar con vSphere y proporcionan compatibilidad con Virtual Volumes. Cada proveedor de almacenamiento debe estar certificado por VMware y correctamente implementado.
- Todos los discos virtuales que aprovisionen en un almacén de datos virtual debe ser un múltiplo par de 1 MB.

Virtual Volumes es una función de vSphere 6.0. Para obtener más información sobre los requisitos, las funciones, el segundo plano y los requisitos de configuración, consulte los temas sobre Virtual Volumes en el documento *Almacenamiento de vSphere*.

Reducir requisitos de almacenamiento con Composer

Como Composer crea imágenes de escritorio que comparten discos virtuales con una imagen de base, puede reducir entre un 50 y un 90 por ciento la capacidad de almacenamiento necesaria.

Composer usa una imagen de base o una máquina virtual principal para crear un grupo de hasta 2000 máquinas virtuales de clones vinculados. Cada clon vinculado actúa como un escritorio independiente, con una dirección IP y un nombre de host únicos; sin embargo, el clon requiere mucho menos espacio de almacenamiento.

Réplicas y clones vinculados en el mismo almacén de datos

Cuando cree un grupo de escritorios de clones vinculados o una granja de hosts RDS de Microsoft, se creará por primera vez un clon completo de la máquina virtual principal. El clon completo, o réplica, y los clones vinculados a ella pueden colocarse en el mismo almacén de datos o en número de unidad lógica (LUN). Si es necesario, puede usar la función de reequilibrio para mover la réplica y los grupos de escritorios de clones vinculados de un LUN a otro o bien para mover grupos de escritorios de clones vinculados a un almacén de datos de vSAN o de un almacén de datos de vSAN a un LUN.

Réplicas y clones vinculados en diferentes almacenes de datos

También se pueden colocar clones vinculados y réplicas de Composer en almacenes de datos distintos con características de rendimiento diferentes. Por ejemplo, puede almacenar las máquinas virtuales de réplica en una unidad de estado sólido (SSD). Las unidades de estado sólido tienen poca capacidad de almacenamiento y un rendimiento de lectura alto que normalmente soporta decenas de miles de operaciones de E/S por segundo. Puede almacenar clones vinculados en almacenes de datos

tradicionales de copia de seguridad de medios. Estos discos proporcionan un rendimiento menor, pero son más económicos y proporcionan una alta capacidad de almacenamiento, por lo que son adecuados para almacenar los numerosos clones vinculados de un grupo grande. Puede usar configuraciones de almacenamiento en niveles para gestionar de manera rentable escenarios de E/S intensivos como reinicios simultáneos de muchas máquinas virtuales o escaneos antivirus programados.

Si desea obtener más información, consulte la guía de prácticas recomendadas *Consideraciones de almacenamiento para VMware View*.

Si usa almacenes de datos de vSAN o de Virtual Volumes, no podrá seleccionar manualmente distintos almacenes de datos para réplicas y clones vinculados. Como las funciones de vSAN y de Virtual Volumes colocan objetos automáticamente en el tipo adecuado de disco y en la caché de todas las operaciones de E/S, no es necesario usar niveles para los almacenes de datos de vSAN y de Virtual Volumes.

Discos descartables para los archivos temporales y de paginación

Cuando crea una granja o un grupo de clones vinculados, también puede configurar de forma opcional otro disco virtual descartable para almacenar los archivos temporales y de paginación del sistema operativo invitado que se generan durante las sesiones de usuario. Cuando la máquina virtual se desconecta, el disco descartable se borra. Al usar discos descartables puede ahorrar espacio de almacenamiento, ya que se ralentiza el crecimiento de los clones vinculados y se reduce el espacio usado por las máquinas virtuales desconectadas.

Discos persistentes para escritorios de asignación dedicada

Cuando cree grupos de escritorios de asignación dedicada, Composer también puede crear, de manera opcional, otro disco virtual persistente para cada escritorio virtual. Los datos de aplicaciones y del perfil del usuario de Windows se guardan en el disco persistente. Cuando un clon vinculado se actualiza, se recompone o se vuelve a equilibrar, los contenidos del disco virtual persistente se conservan. VMware recomienda que guarde los discos persistentes de Composer en otro almacén de datos. Así podrá hacer una copia de seguridad de todo el LUN que contiene los discos persistentes.

Almacenes de datos locales para los escritorios de asignación flotante sin estado

Los escritorios de clones vinculados pueden almacenarse en almacenes de datos locales, que son discos de reserva internos de los hosts ESXi. El almacenamiento local ofrece ventajas como un hardware económico, un aprovisionamiento de máquina virtual rápido, un rendimiento alto de las operaciones de alimentación y una administración sencilla. Sin embargo, el uso del almacenamiento local limita las opciones de configuración de la infraestructura de vSphere que estén disponibles. El uso del almacenamiento local es útil en algunos entornos, pero no es apropiado para otros.

Nota Las limitaciones que se describen en esta sección no se aplican a los almacenes de datos de vSAN, que también usan discos de almacenamiento local pero que requieren hardware específico, tal y como se describe en la sección anterior sobre vSAN.

Es más probable que el uso de almacenes de datos locales funcione bien si los escritorios remotos de su entorno son sin estado. Por ejemplo, es posible que use almacenes de datos locales si implementa puestos de formación y aulas o quioscos sin estado.

Si pretende sacar partido a los beneficios del almacenamiento local, debe considerar atentamente las siguientes limitaciones:

- No puede usar ni VMotion, ni VMware High Availability (HA) ni vSphere Distributed Resource Scheduler (DRS).
- No puede usar la operación de reequilibrio de Composer para equilibrar la carga de las máquinas virtuales en un grupo de recurso.
- No puede almacenar clones vinculados y una réplica de Composer en otros almacenes de datos. De hecho, VMware recomienda que los almacene en el mismo volumen.

Si administra el uso del disco local controlando el número de máquinas virtuales y el crecimiento de sus discos, y si usa asignaciones flotantes y realiza operaciones de actualización y eliminación con regularidad, puede implementar clones vinculados en almacenes de datos locales correctamente.

Si desea obtener más información, consulte el capítulo sobre la creación de grupos de escritorios en el documento *Configurar escritorios virtuales en Horizon 7*.

Reducir requisitos de almacenamiento con clones instantáneos

La función de clones instantáneos usa la tecnología vSphere vmFork (disponible con vSphere 6.0 U1 y versiones posteriores) para poner en modo inactivo una imagen base que se está ejecutando, o una máquina virtual principal y crear y personalizar rápidamente un grupo de escritorios virtuales.

Los clones instantáneos no solo comparten los discos virtuales con la máquina virtual principal en el momento de la creación, sino que también comparten la memoria de la máquina virtual principal. Cada clon instantáneo actúa como un escritorio independiente, con una dirección IP y un nombre de host únicos; sin embargo, el clon requiere mucho menos espacio de almacenamiento. Los clones reducen entre un 50 y un 90 por ciento la capacidad de almacenamiento necesaria. También reducen el requisito de memoria general en el momento de creación del clon. Para obtener más información sobre los requisitos de almacenamiento y los límites de tamaño, consulte el artículo <https://kb.vmware.com/kb/2150348> de la base de conocimientos de VMware.

A partir de Horizon 7 7.8, los clones instantáneos admiten las funciones vSphere TRIM y UNMAP para almacenes de datos vSAN.

Réplicas y clones instantáneos en el mismo almacén de datos

Cuando crea un grupo de escritorios de clones instantáneos, se creará por primera vez un clon completo de la máquina virtual principal. El clon completo, o réplica, y los clones vinculados a ella pueden colocarse en el mismo almacén de datos o en número de unidad lógica (LUN).

Réplicas y clones instantáneos en diferentes almacenes de datos

De forma alternativa, puede colocar clones vinculados y réplicas de clones instantáneos en otros almacenes de datos con características de rendimiento diferentes. Por ejemplo, puede almacenar las máquinas virtuales de réplica en una unidad de estado sólido (SSD). Las unidades de estado sólido tienen poca capacidad de almacenamiento y un rendimiento de lectura alto que normalmente soporta decenas de miles de operaciones de E/S por segundo.

Puede almacenar clones instantáneos en almacenes de datos de medios giratorios. Estos discos proporcionan un rendimiento menor, pero son más económicos y proporcionan una alta capacidad de almacenamiento, por lo que son adecuados para almacenar los numerosos clones instantáneos de un grupo grande. Puede usar configuraciones de almacenamiento en niveles para gestionar de manera rentable escenarios de E/S intensivos como escaneos antivirus programados simultáneos.

Si usa almacenes de datos de vSAN, no podrá seleccionar manualmente diferentes almacenes de datos para réplicas y clones instantáneos. Como vSAN coloca objetos automáticamente en el tipo adecuado de disco y envía a memoria caché todas las operaciones de E/S, no es necesario usar niveles de réplica para los almacenes de datos de vSAN. Los grupos de clones instantáneos son compatibles con los almacenes de datos de vSAN.

Almacenar clones instantáneos en almacenes de datos locales

Las máquinas virtuales de clones instantáneos pueden almacenarse en almacenes de datos locales, que son discos de reserva internos de los hosts ESXi. El almacenamiento local ofrece ventajas como un hardware económico, un aprovisionamiento de máquina virtual rápido, un rendimiento alto de las operaciones de alimentación y una administración sencilla. Sin embargo, el uso del almacenamiento local limita las opciones de configuración de la infraestructura de vSphere que estén disponibles. El uso del almacenamiento local es útil en algunos entornos de Horizon 7, pero no es apropiado para otros.

Nota Las limitaciones que se describen en este tema no se aplican a los almacenes de datos de vSAN, que también usan discos de almacenamiento local pero requieren un hardware específico.

Es más probable que el uso de almacenes de datos locales funcione bien si los escritorios de Horizon 7 de su entorno son sin estado. Por ejemplo, es posible que use almacenes de datos locales si implementa puestos de formación y aulas o quioscos sin estado.

Considere usar almacenes de datos locales si las máquinas virtuales tienen asignaciones flotantes, no están dedicadas a usuarios finales individuales y se pueden eliminar o actualizar a intervalos regulares, como en cada cierre de sesión del usuario. Este enfoque le permite controlar cada almacén de datos local sin tener que mover ni equilibrar la carga de las máquinas virtuales en los almacenes de datos.

Sin embargo, debe tener en cuenta los límites que se aplican en la implementación de la granja o del escritorio de Horizon 7 por usar almacenes de datos locales:

- No puede usar VMotion para administrar Virtual Volumes.
- No puede usar VMware High Availability.
- No puede usar vSphere Distributed Resource Scheduler (DRS).

Si va a implementar clones instantáneos en un único host ESXi con un almacén de datos local, debe configurar un clúster que contenga ese host ESXi. Si tiene un clúster de dos o más hosts ESXi con almacenes de datos locales, seleccione el almacén de datos local de cada uno de los hosts del clúster. De lo contrario, se producirá un error en la creación de los clones instantáneos. Este comportamiento es diferente al comportamiento de los almacenes de datos locales con clones vinculados de Composer.

- No se pueden almacenar réplicas y clones instantáneos en distintos almacenes de datos.
- Si selecciona las unidades de discos locales, es posible que el rendimiento no coincida con el de la matriz de almacenamiento que está disponible comercialmente. Las unidades locales con discos giratorios y una matriz de almacenamiento podrían tener capacidades similares, pero ambos tipos de almacenamiento tienen rendimientos muy diferentes. El rendimiento aumenta a medida que lo hace el número de ejes. Si selecciona discos de estado sólido (SSD) conectados directamente, es posible que el rendimiento sea superior al de muchas matrices de almacenamiento.
- Si quiere aprovechar las ventajas del almacenamiento local, debe tener en cuenta las consecuencias de no tener VMotion, High Availability, DRS ni otras funciones disponibles. Si administra el uso del disco local controlando el número de máquinas virtuales y el crecimiento de sus discos, y si usa asignaciones flotantes y realiza operaciones de actualización y eliminación con regularidad, puede implementar clones instantáneos en almacenes de datos locales correctamente.
- Los clones instantáneos pueden usar almacenes de datos locales tanto con escritorios virtuales como con escritorios publicados.

Diferencias entre clones instantáneos y clones vinculados de Composer

Dado que los clones instantáneos se pueden crear considerablemente más rápido que los clones vinculados, no necesitará las siguientes funciones de los clones vinculados cuando aprovisiona un grupo de clones instantáneos:

- Los grupos de clones instantáneos no admiten la configuración de otro disco virtual descartable para almacenar los archivos temporales y de paginación del sistema operativo invitado. Cada vez que un usuario cierra la sesión en un escritorio de clon instantáneo, Horizon 7 borra automáticamente el clon y aprovisiona y enciende otro clon instantáneo basado en la imagen del SO más reciente disponible para el grupo. Todos los archivos temporales y de paginación del sistema operativo invitado se eliminan automáticamente durante la operación de cierre de sesión.
- Los grupos de clones instantáneos no admiten la creación de otro disco virtual persistente para cada escritorio virtual. En lugar de ello, puede almacenar los datos de aplicaciones y el perfil de Windows del usuario final en los discos grabables de usuario de App Volumes. Los discos grabables de un usuario final se unen a un escritorio de clones instantáneos cuando el usuario final inicia sesión. Además, los discos grabables del usuario pueden usarse para conservar las aplicaciones instaladas por el usuario.
- Debido al carácter efímero de los escritorios de clones instantáneos, estos clones no admiten el formato de disco de espacio eficiente (SE sparse), porque no es compatible con el proceso de borrado y reducción.

- Los grupos de escritorios de clones instantáneos son compatibles con Storage vMotion. Los grupos de escritorios de clones vinculados de Composer no son compatibles con Storage vMotion.

Aprovisionamiento de aplicaciones

Horizon 7 ofrece distintas opciones de aprovisionamiento de aplicaciones: se puede usar técnicas de aprovisionamiento tradicionales, proporcionar aplicaciones publicadas en lugar de escritorios remotos, distribuir paquetes de aplicaciones creados con VMware ThinApp, implementar aplicaciones como parte de View Composer o imágenes de base de clones instantáneos, o vincular aplicaciones mediante App Volumes.

- **Implementar aplicaciones individuales mediante un host RDS**

Es posible proporcionar a los usuarios finales aplicaciones publicadas en lugar de escritorios remotos. El desplazamiento por aplicaciones individuales publicadas puede resultar más sencillo en dispositivos móviles pequeños.

- **Implementar aplicaciones y actualizaciones del sistema con View Composer**

Como los grupos de escritorios de clones vinculados comparten una imagen de base, se pueden implementar rápidamente actualizaciones y revisiones actualizando la máquina virtual principal.

- **Implementar aplicaciones y actualizaciones del sistema con clones instantáneos**

Como los grupos de escritorios de clones instantáneos comparten una imagen de base, se pueden implementar rápidamente actualizaciones y revisiones actualizando la máquina virtual principal.

- **Administrar las aplicaciones VMware ThinApp en Horizon Administrator**

VMware ThinApp™ permite empaquetar una aplicación en un único archivo que se ejecuta en un entorno de pruebas (sandbox) de aplicaciones virtualizada. El resultado de esta estrategia es un aprovisionamiento de aplicaciones flexible y sin conflictos.

- **Implementar y administrar aplicaciones mediante App Volumes**

VMware App Volumes ofrece una manera alternativa de administrar aplicaciones mediante la virtualización de las mismas por encima del sistema operativo. Mediante esta estrategia, las aplicaciones, los archivos de datos, el middleware y las configuraciones actúan como contenedores en capas independientes.

- **Utilizar procesos existentes o VMware Mirage para el aprovisionamiento de aplicaciones**

Horizon 7 permite seguir utilizando las técnicas de aprovisionamiento de aplicaciones que se utilicen en ese momento en la organización, y permite utilizar Mirage. Dos cuestiones adicionales que se deben considerar incluyen la administración del uso de CPU del servidor y la E/S de almacenamiento y determinar si los usuarios tienen permisos para instalar aplicaciones.

Implementar aplicaciones individuales mediante un host RDS

Es posible proporcionar a los usuarios finales aplicaciones publicadas en lugar de escritorios remotos. El desplazamiento por aplicaciones individuales publicadas puede resultar más sencillo en dispositivos móviles pequeños.

Los usuarios finales pueden acceder a aplicaciones publicadas basadas en Windows mediante el mismo Horizon Client que utilizaron anteriormente para acceder a escritorios remotos, y utilizan el mismo protocolo de visualización de Blast Extreme o PCoIP.

Para proporcionar una aplicación publicada, esta se instala en un host Microsoft Remote Desktop Session (RDS). Uno o varios hosts RDS constituyen una granja y, a partir de ella, los administradores crean grupos de aplicaciones de forma similar a como se crean grupos de escritorios. Si desea consultar recomendaciones sobre el tamaño de las granjas, consulte el artículo de la base de conocimientos de VMware: <http://kb.vmware.com/kb/2150348>.

Esta estrategia simplifica las tareas de agregar, eliminar y actualizar aplicaciones, agregar o eliminar actualizaciones de los usuarios para el uso de aplicaciones, y permitir el acceso a granjas de aplicaciones centralizadas o distribuidas desde cualquier dispositivo o red.

Implementar aplicaciones y actualizaciones del sistema con View Composer

Como los grupos de escritorios de clones vinculados comparten una imagen de base, se pueden implementar rápidamente actualizaciones y revisiones actualizando la máquina virtual principal.

La función de recomposición permite realizar cambios en la máquina virtual principal, tomar una snapshot del nuevo estado y enviar la nueva versión de la imagen a todos los usuarios y escritorios, o bien a un subconjunto de ellos. Esta función se puede utilizar para las siguientes tareas:

- Aplicar revisiones y actualizaciones del sistema operativo y del software
- Aplicar service packs
- Agregar aplicaciones
- Agregar dispositivos virtuales
- Cambiar otros ajustes de la máquina virtual, como la memoria disponible

Nota Como View Composer también se puede utilizar para crear granjas de hosts Microsoft RDS de clones vinculados, la función de recomposición permite actualizar las aplicaciones y el sistema operativo invitado en hosts RDS.

Se puede crear un disco persistente de View Composer que contenga la configuración del usuario y otros datos generados por el usuario. El disco persistente no se ve afectado por las operaciones de recomposición. Cuando un clon vinculado se elimina, puede conservar los datos del usuario. Si un empleado deja la compañía, otro empleado puede acceder a los datos de usuario de ese empleado. Un usuario que tenga varios escritorios puede unir los datos del usuario en un único escritorio.

Si se desea dejar de permitir que los usuarios agreguen o eliminen software o cambien la configuración, se puede utilizar la función de actualización para devolver el escritorio a sus valores originales. Esta función también reduce el tamaño de los clones vinculados, que tienden a aumentar de tamaño con el tiempo.

Implementar aplicaciones y actualizaciones del sistema con clones instantáneos

Como los grupos de escritorios de clones instantáneos comparten una imagen de base, se pueden implementar rápidamente actualizaciones y revisiones actualizando la máquina virtual principal.

La función de inserción de imagen permite realizar cambios en la máquina virtual principal, tomar una snapshot del nuevo estado y enviar la nueva versión de la imagen a todos los usuarios y escritorios de forma gradual. Con las actualizaciones graduales, se puede minimizar el periodo de inactividad asociado al mantenimiento de los grupos. Cuando un usuario cierra sesión en un escritorio virtual de un clon instantáneo, Horizon 7 elimina el clon instantáneo y crea uno nuevo a partir de la versión más reciente de la imagen y el nuevo clon estará preparado para que el siguiente usuario inicie la sesión.

Esta función se puede utilizar para las siguientes tareas:

- Aplicar revisiones y actualizaciones del sistema operativo y del software
- Aplicar service packs
- Agregar aplicaciones
- Agregar dispositivos virtuales
- Cambiar otros ajustes de la máquina virtual, como la memoria disponible

Administrar las aplicaciones VMware ThinApp en Horizon Administrator

VMware ThinApp™ permite empaquetar una aplicación en un único archivo que se ejecuta en un entorno de pruebas (sandbox) de aplicaciones virtualizada. El resultado de esta estrategia es un aprovisionamiento de aplicaciones flexible y sin conflictos.

VMware ThinApp permite virtualizar aplicaciones desacoplando una aplicación desde el sistema operativo subyacente y sus bibliotecas y entorno y empaquetando la aplicación en un único archivo ejecutable denominado paquete de la aplicación. Horizon Administrator se puede utilizar para distribuir aplicaciones de VMware ThinApp a escritorios y grupos.

Importante Si, en lugar de distribuir las ThinApps asignándolas a grupos y escritorios, prefiere asignarlas a usuarios y grupos de Active Directory, puede usar VMware Identity Manager.

Después de crear una aplicación virtualizada con VMware ThinApp, se puede elegir entre enviar la aplicación en streaming desde un servidor de archivos compartido o instalar la aplicación en escritorios virtuales. Si se configura la aplicación virtualizada para streaming, se deben tener en cuenta las siguientes consideraciones de la arquitectura:

- Acceso de los grupos de usuarios a los repositorios específicos de las aplicaciones en los que se almacena el paquete de la aplicación.
- Configuración del almacenamiento para el repositorio de la aplicación.
- El tráfico de red generado por el streaming, que depende en gran medida del tipo de aplicación.

Los usuarios inician las aplicaciones de streaming mediante un acceso directo del escritorio.

Si se asigna un paquete de ThinApp de manera que se instale en un escritorio virtual, las consideraciones de la arquitectura son similares a las que se deben tener en cuenta al utilizar el aprovisionamiento de software tradicional basado en MSI. La configuración del almacenamiento para el repositorio de aplicaciones se debe tener en cuenta tanto para aplicaciones de streaming como para paquetes de ThinApp instalados en los escritorios remotos.

Implementar y administrar aplicaciones mediante App Volumes

VMware App Volumes ofrece una manera alternativa de administrar aplicaciones mediante la virtualización de las mismas por encima del sistema operativo. Mediante esta estrategia, las aplicaciones, los archivos de datos, el middleware y las configuraciones actúan como contenedores en capas independientes.

Estos contenedores se denominan pilas de aplicaciones (AppStacks) cuando están en modo de solo lectura o volúmenes de escritura cuando están en modo de lectura y escritura. Los administradores pueden utilizar App Volumes Manager para crear AppStacks y asignar autorizaciones para aplicaciones, así como para entregar AppStacks aprovisionadas al sistema o a un usuario o grupo. Las aplicaciones entregadas mediante App Volumes tienen la apariencia y funcionalidad de las aplicaciones instaladas de forma nativa, y siguen a los usuarios en distintas sesiones y dispositivos. Los administradores pueden actualizar o reemplazar aplicaciones en tiempo real y eliminar cualquier aplicación asignada, ya sea inmediatamente, mientras el usuario mantiene la sesión iniciada, o al siguiente inicio de sesión o reinicio.

Para obtener más información, consulte la documentación de VMware App Volumes, disponible en <https://docs.vmware.com/es/VMware-App-Volumes/index.html>

Utilizar procesos existentes o VMware Mirage para el aprovisionamiento de aplicaciones

Horizon 7 permite seguir utilizando las técnicas de aprovisionamiento de aplicaciones que se utilicen en ese momento en la organización, y permite utilizar Mirage. Dos cuestiones adicionales que se deben considerar incluyen la administración del uso de CPU del servidor y la E/S de almacenamiento y determinar si los usuarios tienen permisos para instalar aplicaciones.

Si se envían aplicaciones a un gran número de escritorios remotos exactamente al mismo tiempo, se pueden observar picos significativos de uso de CPU y E/S de almacenamiento. Estos picos de carga de trabajo pueden tener un efecto notable en el rendimiento del escritorio. La práctica recomendada es programar la actualización de aplicaciones para que, si es posible, se realice fuera de las horas punta y escalonar las actualizaciones de los escritorios. También se debe verificar que la solución de almacenamiento esté diseñada para admitir tales cargas.

Si la empresa permite que los usuarios instalen aplicaciones, se pueden conservar las directivas actuales, pero no se podrán aprovechar ventajas de View Composer como la actualización y recomposición del escritorio. Con View Composer, si una aplicación no está virtualizada o no se incluye en el perfil o la configuración de datos del usuario, esa aplicación se descarta cuando se produzca una

operación de actualización, recomposición o reequilibrado de View Composer. En muchos casos, esta capacidad para controlar rigurosamente las aplicaciones que se instalan es una ventaja. Proporcionar soporte a los escritorios de View Composer es muy sencillo, porque se mantienen en una configuración próxima a una configuración buena conocida.

Si los usuarios tienen requisitos estrictos para instalar sus propias aplicaciones y que esas aplicaciones persistan durante la vida del escritorio remoto, en lugar de utilizar View Composer para el aprovisionamiento de aplicaciones, se pueden utilizar clones instantáneos junto con App Volumes. Otra solución consiste en crear clones completos de escritorios dedicados, permitir que los usuarios instalen aplicaciones y, a continuación, utilizar Mirage para administrar y actualizar los escritorios sin sobrescribir las aplicaciones instaladas por los usuarios.

Importante Mirage también se utiliza para administrar escritorios sin conexión instalados localmente y sus aplicaciones. Para obtener más información, consulte la página de documentación de [Mirage](#).

Utilizar GPO de Active Directory para administrar usuarios y escritorios

Horizon 7 incluye muchas plantillas administrativas ADMX de directivas de grupo para centralizar la administración y configuración de escritorios remotos y componentes de Horizon 7.

Después de importar estas plantillas a Active Directory, se pueden utilizar para establecer directivas que se apliquen a los siguientes componentes y grupos:

- Todos los sistemas, independientemente del usuario que inicie la sesión
- Todos los usuarios, independientemente del sistema en el que inicien la sesión
- Configuración del servidor de conexión
- Configuración de Horizon Client
- Configuración de Horizon Agent

Después de aplicar una GPO, las propiedades se almacenan en el registro local de Windows del componente especificado.

Los GPO se pueden utilizar para establecer todas las directivas disponibles en la interfaz del usuario (IU) de Horizon Administrator. Las GPO también se pueden utilizar para establecer directivas que no están disponibles en la UI. Para obtener una descripción y una lista completa de las opciones disponibles a través de las plantillas ADMX, consulte *Configurar funciones de escritorios remotos en Horizon 7*.

Utilizar directivas Smart

Directivas de Smart también se puede utilizar para crear directivas que controlen el comportamiento del redireccionamiento USB, la impresión virtual, el redireccionamiento del portapapeles, el redireccionamiento de unidades del cliente y funciones del protocolo de visualización PCoIP en escritorios remotos específicos. Para usar esta función, se necesita User Environment Manager.

Directivas de Smart permite crear directivas que solo tengan efecto si se cumplen determinadas condiciones. Por ejemplo, se puede configurar una directiva que deshabilite la función de redireccionamiento de unidades del cliente si un usuario se conecta a un escritorio remoto desde fuera de la red corporativa.

En general, la configuración de directivas de Horizon que se configure para las funciones de escritorio remoto en User Environment Manager prevalecen sobre cualquier configuración de directiva de grupo y clave de registro equivalente.

Elementos de diseño de la arquitectura y directrices de planificación para implementaciones de escritorios remotos

4

Un diseño típico de arquitectura de Horizon 7 utiliza una estrategia de pod. Las definiciones de los pods pueden variar en función de la configuración de hardware, las versiones de software de Horizon 7 y vSphere utilizadas y otros factores de diseño específicos del entorno.

Los ejemplos de este documento ilustran un diseño escalable que se puede adaptar al entorno y a los requisitos especiales de su empresa. Este capítulo incluye detalles clave relativos a los requisitos de memoria, CPU, capacidad de almacenamiento, componentes de red y hardware para proporcionar a arquitectos y planificadores de TI un conocimiento práctico de lo que se requiere para la implementación de una solución de Horizon 7.

Importante En este capítulo, no se tratan los temas siguientes:

Diseño de la arquitectura para aplicaciones alojadas	Un pod de Horizon 7 puede tener soporte para granjas de hosts de Microsoft RDS, donde cada granja contiene hosts RDS. Si desea obtener más información, consulte <i>Configurar aplicaciones y escritorios publicados en Horizon 7</i> . Si tiene previsto utilizar máquinas virtuales para hosts RDS, consulte también Configuración de la máquina virtual del host RDS .
Diseño de la arquitectura para el complemento Horizon 7 Agent Direct Connect	Si este complemento se ejecuta en un escritorio de máquina virtual, el cliente puede conectar directamente a la máquina virtual. Todas las funciones de escritorio remoto, incluyendo PCoIP, HTML Access, RDP, redireccionamiento USB y administración de sesiones, funcionan de la misma manera, como si el usuario se hubiera conectado a través del servidor de conexión de View. Para obtener más información, consulte <i>Horizon 7 Administración del complemento Agent Direct-Connection</i> .

Este capítulo incluye los siguientes temas:

- [Requisitos de máquina virtual para escritorios remotos](#)
- [Nodo de Horizon 7ESXi](#)
- [Grupos de escritorios para tipos específicos de trabajo](#)
- [Configuración de la máquina virtual del escritorio](#)
- [Configuración de la máquina virtual del host RDS](#)
- [Configuración de máquinas virtuales de vCenter Server y View Composer](#)

- [Máximos del servidor de conexión de Horizon y configuración de máquinas virtuales](#)
- [Clústeres de vSphere](#)
- [Requisitos de almacenamiento y ancho de banda](#)
- [Bloques de creación de Horizon 7](#)
- [Pods de Horizon 7](#)
- [Ventajas de utilizar varios servidores vCenter Server en un pod](#)

Requisitos de máquina virtual para escritorios remotos

Al planificar las especificaciones para escritorios remotos, las elecciones que se hagan en cuanto a RAM, CPU y espacio de disco tienen un efecto significativo en las opciones de hardware y los gastos de almacenamiento y de servidor.

- [Planificación basada en tipos de trabajadores](#)

En muchos elementos de configuración, entre los que se incluyen el tamaño del almacenamiento, la RAM y la CPU, los requisitos dependen en gran medida del tipo de trabajador que utilice el escritorio virtual y de las aplicaciones que se deban instalar.

- [Estimar los requisitos de memoria para escritorios de máquinas virtuales](#)

La RAM de los servidores es más cara que la de los PC. Como el costo de la RAM es una parte importante de los costos del hardware del servidor y de la capacidad de almacenamiento total necesaria, es esencial determinar la asignación de memoria correcta al planificar la implementación de los escritorios.

- [Estimar los requisitos de CPU para escritorios de máquinas virtuales](#)

Al estimar la CPU, se debe recopilar información sobre el promedio de uso de CPU para diversos tipos de trabajadores de la empresa.

- [Elegir el tamaño adecuado del disco del sistema](#)

Al asignar espacio de disco, se debe proporcionar solo espacio suficiente para el sistema operativo, las aplicaciones y el contenido adicional que los usuarios puedan instalar o generar. Normalmente, esta cantidad es inferior al tamaño del disco que se incluye en un disco de PC físico.

Planificación basada en tipos de trabajadores

En muchos elementos de configuración, entre los que se incluyen el tamaño del almacenamiento, la RAM y la CPU, los requisitos dependen en gran medida del tipo de trabajador que utilice el escritorio virtual y de las aplicaciones que se deban instalar.

Para planificar la arquitectura, los trabajadores se pueden categorizar en varios tipos.

Trabajadores en tareas

Los trabajadores en tareas son trabajadores administrativos que realizan tareas repetitivas dentro de un pequeño conjunto de aplicaciones, por lo general en un equipo estacionario. Las aplicaciones no requieren normalmente un uso de CPU ni de memoria tan intensivo como las de los

trabajadores del conocimiento. Los trabajadores en tareas que trabajan determinados turnos pueden iniciar la sesión en sus escritorios virtuales todos a la vez. Entre los trabajadores en tareas, se incluyen analistas de centros de llamadas, empleados de comercios minoristas, trabajadores de almacén, etc.

Trabajadores del conocimiento

Las tareas diarias de los trabajadores del conocimiento incluyen el acceso a Internet, el uso de correo electrónico y la creación de presentaciones, hojas de cálculo y documentos complejos. Entre los trabajadores del conocimiento, se incluyen contables, directores de ventas, analistas de investigación de mercado, etc.

Usuarios avanzados

Entre los usuarios avanzados, se incluyen desarrolladores de aplicaciones y personas que utilizan aplicaciones que hacen un uso intensivo de gráficos.

Usuarios de quiosco

Estos usuarios necesitan compartir un escritorio situado en un lugar público. Entre los ejemplos de usuarios de quiosco, se incluyen estudiantes que utilizan un equipo compartido en una clase, enfermeras en salas de enfermería y equipos utilizados para contratación y publicación de ofertas de empleo. Estos escritorios requieren un inicio de sesión automático. La autenticación se puede hacer mediante determinadas aplicaciones si es necesario.

Estimar los requisitos de memoria para escritorios de máquinas virtuales

La RAM de los servidores es más cara que la de los PC. Como el costo de la RAM es una parte importante de los costos del hardware del servidor y de la capacidad de almacenamiento total necesaria, es esencial determinar la asignación de memoria correcta al planificar la implementación de los escritorios.

Si la asignación de RAM es demasiado baja, la E/S del almacenamiento se puede ver negativamente afectada porque se produce demasiada paginación de Windows. Si la asignación de RAM es demasiado elevada, la capacidad de almacenamiento se puede ver negativamente afectada debido a que el archivo de paginación del sistema operativo invitado y los archivos de intercambio y suspensión de cada una de las máquinas virtuales aumentarán demasiado su tamaño.

Impacto del tamaño de la RAM en el rendimiento

Al asignar RAM, se debe evitar elegir un valor excesivamente conservador. Se debe tener en cuenta lo siguiente:

- Si la asignación de RAM es insuficiente, se producirá una paginación de Windows excesiva, lo que puede generar operaciones de E/S que degraden significativamente el rendimiento y aumentar la carga de E/S del almacenamiento.

- VMware ESXi admite sofisticados algoritmos de administración de recursos de memoria, como el uso compartido de páginas transparentes y el aumento de memoria, lo que puede reducir significativamente la cantidad de RAM física necesaria para admitir una determinada asignación de RAM al invitado. Por ejemplo, aunque se pueden asignar 2 GB a un escritorio virtual, solo se consume una pequeña parte de esa cifra en RAM física.
- Como el rendimiento del escritorio virtual se ve afectado por los tiempos de respuesta, en el host ESXi se deben establecer valores distintos a cero en la configuración de reserva de memoria. Al reservar algo de RAM, se garantiza que los escritorios en uno pero inactivos no se trasladen nunca por completo al disco. También se puede reducir el espacio de almacenamiento consumido por los archivos de intercambio de ESXi. Sin embargo, una configuración de reserva mayor afecta a la capacidad para sobreasignar memoria en un host ESXi y puede afectar a las operaciones de mantenimiento de VMotion.

Impacto del tamaño de la RAM en el almacenamiento

La cantidad de RAM asignada a una máquina virtual está directamente relacionada con el tamaño de determinados archivos utilizados por la máquina virtual. Para acceder a los archivos de la lista siguiente, se debe utilizar el sistema operativo Windows invitado para localizar los archivos de paginación y de hibernación de Windows, y el sistema de archivos del host de ESXi para localizar los archivos de suspensión y el archivo de intercambio de ESXi.

Archivo de paginación de Windows

El tamaño predeterminado del archivo es un 150% de la RAM del invitado. Este archivo, que de forma predeterminada se encuentra en `C:\pagefile.sys`, hace que el almacenamiento de aprovisionamiento ligero aumente de tamaño, porque se accede a él con frecuencia. En máquinas virtuales de clones vinculados de View Composer, el archivo de paginación y los archivos temporales se pueden redirigir a un disco virtual independiente que se borra al apagar las máquinas virtuales. El redireccionamiento de archivos de paginación desechables ahorra almacenamiento, reduce el aumento de tamaño de los clones vinculados y puede también aumentar el rendimiento. Aunque el tamaño se puede ajustar desde Windows, hacerlo así puede tener un impacto negativo en el rendimiento de las aplicaciones.

En los clones instantáneos, los archivos temporales y de paginación de los sistemas operativos se borran automáticamente durante la operación de cierre de sesión y, por tanto, no tienen tiempo para aumentar mucho de tamaño. Cada vez que un usuario cierra la sesión en un escritorio de clon instantáneo, Horizon borra el clon y aprovisiona y enciende otro clon instantáneo basado en la imagen del SO más reciente disponible para el grupo.

Archivo de hibernación de Windows para portátiles

Este archivo puede ser igual al 100% de la RAM del invitado. Este archivo se puede borrar con seguridad porque no se necesita en implementaciones de Horizon.

Archivo de intercambio de ESXi

Este archivo, que tiene la extensión `.vswp`, se crea si se reserva menos del 100% de la RAM de la máquina virtual. El tamaño del archivo de intercambio es igual a la porción no reservada de la RAM del invitado. Por ejemplo, si se reserva el 50% de la RAM del invitado y esta es de 2 GB, el archivo de intercambio de ESXi es de 1 GB. Este archivo se puede almacenar en el almacén de datos local en el clúster o en el host de ESXi.

Archivo de suspensión de ESXi

Este archivo, que tiene la extensión `.vmss`, se crea si se establece una directiva de cierre de sesión para el grupo de escritorios de manera que el escritorio virtual se ponga en suspensión cuando el usuario cierre la sesión. El tamaño de este archivo es igual al tamaño de la RAM del invitado.

Tamaño de la RAM para configuraciones de monitor específicas cuando se utiliza PColP o Blast Extreme

Además de la memoria del sistema, una máquina virtual requiere también una pequeña cantidad de RAM en el host ESXi para el procesamiento de video. Este requisito de tamaño de VRAM depende de la resolución de la pantalla y del número de monitores configurado para los usuarios finales. [Tabla 4-1. Procesamiento de visualización en el cliente de PColP o Blast Extreme](#) indica la cantidad de RAM de procesamiento requerida para distintas configuraciones. Las cantidades de memoria indicadas en las columnas se añaden a la cantidad de memoria requerida para otras funciones de PColP o Blast Extreme.

Tabla 4-1. Procesamiento de visualización en el cliente de PColP o Blast Extreme

Resolución de visualización estándar	Ancho, en píxeles	Alto, en píxeles	Procesamiento con 1 monitor	Procesamiento con 2 monitores	Procesamiento con 3 monitores	Procesamiento con 4 monitores
VGA	640	480	1,20 MB	3,20 MB	4,80 MB	5,60 MB
WXGA	1280	800	4,00 MB	12,50 MB	18,75 MB	25,00 MB
1080p	1920	1080	8,00 MB	25,40 MB	38,00 MB	50,60 MB
WQXGA	2560	1600	16,00 MB	60,00 MB	84,80 MB	109,60 MB
UHD (4K)	3840	2160	32,00 MB	78,00 MB	124,00 MB	170,00MB

Para calcular los requisitos del sistema, los valores de VRAM se suman a la RAM del sistema base para la máquina virtual. La memoria de procesamiento se calcula y configura automáticamente al especificar el número máximo de monitores y seleccionar la resolución de visualización en Horizon Administrator.

Si se utiliza la función de procesamiento 3D y se selecciona Soft3D o vSGA, se puede volver a calcular con los valores de VRAM adicionales en un control de Horizon Administrator para configurar la VRAM para invitados que usen 3D. Alternativamente, y para otros tipos de aceleración gráfica además de Soft3D y vSGA, se puede especificar la cantidad exacta de VRAM si se decide administrar la VRAM mediante vSphere Client.

De forma predeterminada, la configuración de varios monitores coincide con la topología del host. Se precalcula un procesamiento adicional para más de 2 monitores para acomodar esquemas de topología adicionales. Si al iniciar una sesión de escritorio remoto aparece una pantalla negra, compruebe que los valores del número de monitores y de la resolución de pantalla, que se establecen en Horizon Administrator, coincidan con los del sistema host, o bien ajuste manualmente la cantidad de memoria seleccionando la opción **Administrar mediante vSphere Client** en Horizon Administrator y establezca a continuación el valor de la memoria de vídeo total a un máximo de 128 MB.

Tamaño de la RAM para sistemas operativos y cargas de trabajo específicas

Como la cantidad de RAM requerida puede variar mucho, en función del tipo de trabajador, muchas empresas realizan una fase piloto para determinar el ajuste correcto para distintos grupos de trabajadores de la empresa.

Un buen comienzo es asignar 1 GB para escritorios con Windows 7 o versiones posteriores de 32 bits y 2 GB para escritorios con Windows 7 o versiones posteriores de 64 bits. Si se desea usar una de las funciones de aceleración de gráficos por hardware para trabajos 3D, VMware recomienda 2 CPU virtuales y 4 GB de RAM. Durante el programa piloto, se debe supervisar el rendimiento y el espacio de disco utilizado con distintos tipos de trabajadores y realizar los ajustes necesarios hasta encontrar la configuración óptima para cada grupo de trabajadores.

Estimar los requisitos de CPU para escritorios de máquinas virtuales

Al estimar la CPU, se debe recopilar información sobre el promedio de uso de CPU para diversos tipos de trabajadores de la empresa.

Los requisitos de CPU varían según el tipo de trabajador. Durante la fase piloto, se debe utilizar una herramienta de supervisión del rendimiento, como Perfmon, en la máquina virtual, esxtop en ESXi, o herramientas de supervisión del rendimiento de vCenter Server, para conocer los niveles de uso de CPU tanto medios como pico para estos grupos de trabajadores. Se deben usar también las siguientes directrices:

- Los desarrolladores de software u otros usuarios avanzados con elevadas necesidades de rendimiento pueden tener unos requerimientos de CPU mucho más altos que los trabajadores del conocimiento y los trabajadores en tareas. Se recomienda utilizar CPU virtuales Dual o Quad para máquinas virtuales Windows 7 de 64 bits que ejecuten tareas de computación intensivas, tales como el uso de aplicaciones CAD, la reproducción de vídeos en HD o el uso de resoluciones de pantalla de 4K.
- Para los demás casos, se recomienda generalmente CPU virtuales simples.

Como muchas máquinas virtuales se ejecutan en un servidor, la CPU puede experimentar un pico si todos los agentes, como antivirus, comprueban si hay actualizaciones al mismo tiempo. Determine qué agentes y cuántos de ellos podrían ocasionar problemas de rendimiento y adopte una estrategia para solucionarlos. Por ejemplo, las siguientes estrategias pueden resultar útiles en la empresa:

- Utilizar clones instantáneos o clones vinculados de View Composer para actualizar imágenes en lugar de que los agentes de administración de software descarguen actualizaciones de software en cada escritorio virtual individual.
- Programar la ejecución de actualizaciones de antivirus y software fuera de las horas punta, cuando probablemente sean pocos los usuarios que hayan iniciado sesión.
- Escalonar el momento en que se realizan las actualizaciones o realizarlas aleatoriamente.
- Usar un producto antivirus compatible con la API de VMware vShield. Por ejemplo, esta API se ha integrado en VMware vCloud[®] Networking and Security 5.1 y versiones posteriores.

A modo de aproximación inicial informal al cálculo del tamaño, se puede suponer para comenzar que cada máquina virtual requiere entre 1/8 y 1/10 del núcleo de una CPU como capacidad de computación garantizada mínima. Es decir, se debe planificar un programa piloto en el que se utilicen entre 8 y 10 máquinas virtuales por núcleo. Por ejemplo, si se supone que hay 8 máquinas virtuales por núcleo y se tiene un host ESXi de 2 zócalos y 8 núcleos, se pueden alojar 128 máquinas virtuales en el servidor durante el programa piloto. Supervise el uso general de CPU en el host durante este período y asegúrese de que rara vez exceda de un margen de seguridad, como de 80%, para dejar capacidad suficiente para los picos.

Elegir el tamaño adecuado del disco del sistema

Al asignar espacio de disco, se debe proporcionar solo espacio suficiente para el sistema operativo, las aplicaciones y el contenido adicional que los usuarios puedan instalar o generar. Normalmente, esta cantidad es inferior al tamaño del disco que se incluye en un disco de PC físico.

Como el espacio de disco en el centro de datos suele costar más por gigabyte que el espacio de disco de escritorios o portátiles en implementaciones de equipos tradicionales, se debe optimizar el tamaño de la imagen del sistema operativo. Las sugerencias siguientes pueden servir de ayuda para optimizar el tamaño de la imagen:

- Eliminar los archivos innecesarios. Por ejemplo, reducir las cuotas para los archivos temporales de Internet.
- Desactivar servicios de Windows tales como el servicio de indexación, el servicio de desfragmentación y los puntos de restauración. Para obtener más información, consulte el documento *Configurar escritorios virtuales en Horizon 7*.
- Se debe elegir un tamaño de disco suficientemente grande para permitir un crecimiento futuro, pero que no sea exageradamente grande.
- Para aplicaciones instaladas por el usuario y contenido generado por el usuario, se deben usar recursos compartidos centralizados, un disco persistente de View Composer o App Volumes.

- Si se utiliza vSphere 5.1 o una versión posterior, se debe habilitar la recuperación de espacio para vCenter Server y para los grupos de escritorios de clones vinculados.

Si los escritorios de máquinas virtuales utilizan el formato de disco para eficiencia del espacio disponible en vSphere 5.1 o versiones posteriores, el espacio ocupado por los datos antiguos o borrados dentro de un sistema operativo invitado se recupera automáticamente mediante un proceso de limpieza y reducción.

La cantidad de espacio de almacenamiento requerida debe tener en cuenta los siguientes archivos para cada escritorio virtual:

- El archivo de suspensión ESXi es equivalente a la cantidad de RAM asignada a la máquina virtual.
- De forma predeterminada, el archivo de paginación de Windows es equivalente al 150% de la RAM.
- Los archivos de registro pueden ocupar hasta 100 MB por cada máquina virtual.
- El disco virtual, o archivo .vmdk, debe albergar el sistema operativo, las aplicaciones y futuras aplicaciones y actualizaciones de software. El disco virtual también debe albergar datos de usuario locales y aplicaciones instaladas por el usuario si se encuentran en el escritorio virtual en lugar de estar en recursos compartidos.

Si se utiliza View Composer, los archivos .vmdk aumentan de tamaño a lo largo del tiempo, pero es posible controlar este aumento programando operaciones de actualización de View Composer, estableciendo una directiva de exceso de disponibilidad de almacenamiento para grupos de escritorios de máquina virtual y redirigiendo los archivos temporales y de paginación de Windows a un disco independiente no persistente.

Si se utilizan clones instantáneos, el tamaño de los archivos .vmdk aumentará con el tiempo dentro de una sesión iniciada. Cuando un usuario cierre la sesión, el escritorio del clon instantáneo se borra automáticamente y se crea un nuevo clon instantáneo preparado para que el siguiente usuario inicie la sesión. Con este proceso, el escritorio se actualiza eficazmente y vuelve a su tamaño original.

También se puede agregar un 15% a esta estimación para asegurar que los usuarios no se queden sin espacio de disco.

Nodo de Horizon 7ESXi

Un nodo es un único host VMware ESXi en el que se alojan escritorios de máquinas virtuales en una implementación de Horizon 7.

Horizon 7 es económicamente más rentable cuando se maximiza el índice de consolidación, que es el número de escritorios alojados en un host ESXi. Aunque son muchos los factores que afectan a la selección del servidor, si lo que se está optimizando es el precio de adquisición, se deben encontrar configuraciones de servidor que tengan un equilibrio adecuado de memoria y potencia de procesamiento.

No hay nada mejor para medir el rendimiento que situaciones del mundo real, como un programa piloto, para determinar un índice de consolidación adecuado de la configuración de hardware del entorno. Los índices de consolidación pueden variar significativamente, según los patrones de uso y los factores ambientales. Utilice las siguientes directrices:

- Como marco de trabajo general, considere la capacidad de computación en términos de 8 o 10 escritorios virtuales por núcleo de CPU. Para obtener información sobre el cálculo de los requisitos de CPU para cada máquina virtual, consulte [Estimar los requisitos de CPU para escritorios de máquinas virtuales](#).
- Piense en la capacidad de memoria en términos de RAM del escritorio virtual, RAM del host e índice de sobreasignación. Aunque se pueden tener entre 8 y 10 escritorios virtuales por núcleo de CPU, si los escritorios virtuales tienen una memoria RAM de 1 GB o más, también se deben considerar cuidadosamente los requerimientos de RAM física. Para obtener información relativa al cálculo de la cantidad de RAM requerida por máquina virtual, consulte [Estimar los requisitos de memoria para escritorios de máquinas virtuales](#).

Tenga en cuenta que los costes de RAM física no son lineales y que, en algunas situaciones, puede ser económicamente más rentable adquirir más servidores pequeños que no utilizan chips DIMM caros. En otros casos, la densidad del rack, la conectividad del almacenamiento, las posibilidades de administración y otras consideraciones pueden hacer que minimizar el número de servidores de una implementación sea una mejor opción.

- En Horizon 7, la función de acelerador de almacenamiento de View está activada de forma predeterminada, lo que permite que los hosts ESXi 5.5 Update 2 y versiones posteriores guarden en la caché datos de discos habituales de máquinas virtuales. El acelerador de almacenamiento de View puede aumentar el rendimiento y reducir la necesidad de ancho de banda de E/S de almacenamiento adicional para gestionar sobrecargas de arranque y sobrecargas de E/S de análisis antivirus. Para esta función, se requiere 1 GB de RAM por host ESXi.
- Por último, se deben tener en cuenta los requisitos del clúster y de la conmutación por error. Si desea obtener más información, consulte [Determinar los requisitos para alta disponibilidad](#).

Para obtener información sobre las especificaciones de los hosts de ESXi en vSphere, consulte el documento de *VMware vSphere valores máximos de configuración*.

Grupos de escritorios para tipos específicos de trabajo

Horizon 7 le facilita muchas funciones para ayudar a conservar almacenamiento y reducir la cantidad de potencia de procesamiento necesaria para varios usos. Muchas de estas funciones están disponibles como opciones de configuración de grupos.

La pregunta más importante que debe considerarse es si un cierto tipo de usuario necesita una imagen de escritorio con cortafuegos o sin cortafuegos. Los usuarios que necesiten una imagen de escritorio con cortafuegos tienen datos en la propia imagen del sistema operativo que deben ser conservados, mantenidos y respaldados. Por ejemplo, estos usuarios instalan algunas de sus propias aplicaciones o tienen datos que no pueden guardarse fuera de la propia máquina virtual, como en un servidor de archivos o en una base de datos de aplicaciones.

Imágenes de escritorios sin cortafuegos

También conocidos como escritorios no persistentes, las arquitecturas sin cortafuegos tienen múltiples ventajas, como un soporte más fácil y costos de almacenamiento más bajos. Otras ventajas son la escasa necesidad de hacer copias de seguridad de las máquinas virtuales y una recuperación y continuidad de las actividades en caso de desastres es menos costosa.

Imágenes de escritorios con cortafuegos

También conocidos como escritorios persistentes, es posible que estas imágenes requieran técnicas tradicionales de gestión de imágenes. Las imágenes con cortafuegos pueden tener costos bajos de almacenamiento si se utiliza conjuntamente con algunas tecnologías de sistemas de almacenamiento. Las tecnologías de copia de seguridad y de recuperación, como VMware Site Recovery Manager, son importantes en cuanto a estrategias de copia de seguridad, recuperación y continuación de las actividades.

Hay dos formas de crear imágenes de escritorio sin estado en Horizon 7:

- Puede crear grupos de asignación flotantes o grupos de asignación dedicada de máquinas virtuales de clones instantáneos. El redireccionamiento de carpetas y los perfiles de itinerancia pueden usarse opcionalmente para almacenar datos del usuario.
- Puede usar View Composer para crear grupos de asignación flotante o dedicada de máquinas virtuales de clones vinculados. De forma opcional, se puede usar perfiles de itinerancia y el redireccionamiento de carpetas para almacenar los datos de usuario o configurar discos persistentes para conservar datos de usuario.

Existen dos formas de crear imágenes de escritorio con estado en Horizon 7:

- Puede crear clones completos o máquinas virtuales completas. Algunos proveedores de almacenamiento disponen de soluciones de almacenamiento rentables para clones completos. A menudo, estos proveedores tienen sus propias prácticas recomendadas y utilidades de aprovisionamiento. Si usa uno de estos proveedores, es posible que necesite crear un grupo manual de asignación dedicada.
- Puede crear grupos de máquinas virtuales de clones instantáneos o vinculada y usar volúmenes grabables de usuario de App Volumes para adjuntar los datos de usuario y las aplicaciones instaladas por el usuario.

La decisión de usar escritorios con o sin cortafuegos depende del tipo específico de trabajo.

- **Grupos de trabajadores con tareas específicas**

Puede estandarizar imágenes de escritorio sin cortafuegos para los trabajadores con tareas específicas de modo que la imagen siempre tenga una configuración fácilmente admisible y reconocible y los trabajadores puedan iniciar sesión en cualquier escritorio disponible.

- **Grupos para trabajadores del conocimiento y usuarios avanzados**

Los trabajadores del conocimiento deben ser capaces de crear documentos complejos y conservarlos en el escritorio. Los usuarios avanzados deben poder instalar sus propias aplicaciones y conservarlas. En función del tipo y de la cantidad de datos personales que deban conservarse, el escritorio puede ser tanto de tipo con estado como de tipo sin estado.

- **Grupos de usuarios de pantalla completa**

Entre los usuarios de pantalla completa, se pueden incluir clientes en estaciones de registros de líneas aéreas, estudiantes en clases o bibliotecas, personal sanitario en estaciones de trabajo en las que se introducen información médica o clientes en puntos de autoservicio. Las cuentas asociadas a dispositivos clientes en lugar de a usuarios están autorizadas para usar estos grupos de escritorios, ya que los usuarios no necesitan iniciar sesión para usar los dispositivos cliente o los escritorios remotos. Aun así, se les solicitará a los usuarios que proporcionen credenciales de autenticación en algunas aplicaciones.

Grupos de trabajadores con tareas específicas

Puede estandarizar imágenes de escritorio sin cortafuegos para los trabajadores con tareas específicas de modo que la imagen siempre tenga una configuración fácilmente admisible y reconocible y los trabajadores puedan iniciar sesión en cualquier escritorio disponible.

Dado que los trabajadores con tareas específicas realizan tareas repetitivas mediante un pequeño conjunto de aplicaciones, puede crear imágenes de escritorio sin cortafuegos que permiten conservar espacio de almacenamiento y procesar requisitos.

Utilice la siguiente configuración de grupo en los grupos de escritorios de clones instantáneos:

- Para optimizar el uso de recursos en los grupos de clones instantáneos, use aprovisionamiento bajo demanda para aumentar o reducir el grupo según su uso. Asegúrese de especificar escritorios de reserva suficientes para satisfacer la tasa de inicio de sesión.
- En los grupos de escritorios de clones instantáneos, Horizon 7 elimina automáticamente el clon instantáneo siempre que un usuario cierra sesión. Se crea un nuevo clon instantáneo que está preparado para que el siguiente usuario inicie sesión, actualizándose de forma eficaz cada vez que se cierra sesión.

Utilice la siguiente configuración de grupo en los grupos de escritorios de clones vinculados de View Composer:

- Para los grupos de escritorios de View Composer, determine qué acción realizar, si fuera necesario, cuando los usuarios cierran sesión. Los discos aumentan de tamaño con el tiempo. Puede ahorrar espacio de disco si actualiza el escritorio a su estado original cuando los usuarios cierran sesión. También puede programar una actualización de escritorios periódica. Por ejemplo, puede programar los escritorios para que se actualicen diariamente, semanalmente o mensualmente.
- Si corresponde, y si usa grupos de clones vinculados de View Composer, considere almacenar los escritorios en almacenes de datos ESXi locales. Esta estrategia ofrece ventajas como un hardware económico, un aprovisionamiento de máquina virtual rápido, un rendimiento alto de las operaciones de alimentación y una administración sencilla. Para obtener una lista de limitaciones, consulte [Almacenes de datos locales para los escritorios de asignación flotante sin estado](#). Los grupos de clones instantáneos no son compatibles con los almacenes de datos locales.

Nota Si desea obtener información sobre otro tipo de opciones de almacenamiento, consulte [Reducir y administrar requisitos de almacenamiento](#).

- Use la función Persona Management para que los usuarios siempre tengan la configuración de aplicaciones y el aspecto de escritorio preferidos, como con los perfiles de usuario de Windows. Si los escritorios no están configurados para actualizarse o eliminarse después del cierre de sesión, puede configurar el perfil para que se elimine al cerrar sesión.

Importante Persona Management facilita la implementación de un grupo de asignación flotante para aquellos usuarios que quieran conservar su configuración de una sesión a otra. Antes, una de las limitaciones de los escritorios de asignación flotante era que, cuando los usuarios cerraban sesión, perdían toda su configuración y todos los datos almacenados en el escritorio remoto.

Cada vez que los usuarios iniciaban sesión, su fondo de escritorio era el fondo de pantalla predeterminado y tenían que volver a configurar las preferencias de todas las aplicaciones. Con Persona Management, el usuario final de un escritorio de asignación flotante no puede detectar ninguna diferencia entre su sesión y una sesión que se ejecuta en un escritorio de asignación dedicada.

Utilice la siguiente configuración de grupo general en todos los grupos de escritorios:

- Cree un grupo automatizado para que los escritorios puedan crearse cuando el grupo se cree o para que puedan generarse bajo demanda según el uso del grupo.
- Use asignación flotante para que los usuarios inicien sesión en cualquier escritorio disponible. Esta opción reduce el número de escritorios necesarios si no todo el mundo necesita tener la sesión iniciada al mismo tiempo.
- Cree escritorios de clones instantáneos o de clones vinculados de View Composer para que los escritorios compartan la misma imagen base y usen menos espacio de almacenamiento en el centro de datos que las máquinas virtuales completas.

Grupos para trabajadores del conocimiento y usuarios avanzados

Los trabajadores del conocimiento deben ser capaces de crear documentos complejos y conservarlos en el escritorio. Los usuarios avanzados deben poder instalar sus propias aplicaciones y conservarlas. En función del tipo y de la cantidad de datos personales que deban conservarse, el escritorio puede ser tanto de tipo con estado como de tipo sin estado.

Para los trabajadores del conocimiento que no necesiten tener aplicaciones instaladas por el usuario excepto para uso temporal, puede crear imágenes de escritorio sin estado y guardar todos sus datos personales fuera de la máquina virtual en un servidor de archivos o en una base de datos de aplicaciones. Para otros trabajadores del conocimiento y para los usuarios avanzados, puede crear imágenes de escritorio con estado.

Utilice la siguiente configuración de grupo en los grupos de escritorios de clones instantáneos:

- Si usa escritorios de clones instantáneos, implemente un recurso compartido de archivos, un perfil de itinerancia u otra solución de administración de perfiles.

Utilice la siguiente configuración de grupo en los grupos de escritorios de clones vinculados de View Composer:

- Si usa View Composer con escritorios virtuales vSphere, habilite la función de recuperación de espacio de vCenter Server y del grupo de escritorios. Con la función de recuperación de espacio, los datos eliminados u obsoletos de un sistema operativo invitado se recuperan automáticamente con un proceso de reducción y borrado.
- View Composer puede generar y conservar identificadores de seguridad (SID) del equipo local para las máquinas virtuales de clones vinculados en algunas situaciones. También puede configurar discos persistentes para que pueda actualizar y recomponer los discos de sistema operativo del clon vinculado mientras se conserva una copia del perfil de usuario en los discos persistentes.
- Use la función Persona Management para que los usuarios siempre tengan la configuración de aplicaciones y el aspecto de escritorio preferidos, como con los perfiles de usuario de Windows.

Utilice la siguiente configuración de grupo general en todos los grupos de escritorios:

- Es posible que algunos usuarios avanzados y trabajadores del conocimiento, como contables, jefes de ventas o analistas financieros, necesiten iniciar sesión en el mismo escritorio en cada ocasión. Cree grupos de asignación dedicada para ellos.
- Use vStorage Thin Provisioning para que, al principio, cada escritorio use solo la cantidad de espacio de almacenamiento que necesita el disco para su funcionamiento inicial.
- Para usuarios avanzados y trabajadores del conocimiento que deben instalar sus propias aplicaciones y que, por lo tanto, agregan datos al disco del sistema operativo, tiene dos opciones. Una opción es crear escritorios de máquina virtual completa.

La segunda opción consiste en crear un grupo de clones vinculados o instantáneos y usar App Volumes para conservar las aplicaciones instaladas por los usuarios y los datos de usuario cada vez que se inicie sesión.

- Si los trabajadores del conocimiento no necesitan aplicaciones instaladas por los usuarios excepto para uso temporal, puede crear escritorios de clones instantáneos o escritorios de clones vinculados de View Composer. Las imágenes de escritorio comparten la misma imagen de base y utilizan menos espacio de almacenamiento que las máquinas virtuales completas.

Grupos de usuarios de pantalla completa

Entre los usuarios de pantalla completa, se pueden incluir clientes en estaciones de registros de líneas aéreas, estudiantes en clases o bibliotecas, personal sanitario en estaciones de trabajo en las que se introducen información médica o clientes en puntos de autoservicio. Las cuentas asociadas a dispositivos clientes en lugar de a usuarios están autorizadas para usar estos grupos de escritorios, ya que los usuarios no necesitan iniciar sesión para usar los dispositivos cliente o los escritorios remotos. Aun así, se les solicitará a los usuarios que proporcionen credenciales de autenticación en algunas aplicaciones.

Los escritorios de máquina virtual que están configurados para ejecutarse en modo de pantalla completa usan imágenes de escritorio sin cortafuegos ya que no es necesario conservar los datos de usuario en el disco del sistema operativo. Los escritorios de modo de pantalla completa se usan en dispositivos cliente ligeros o en equipos bloqueados. Debe comprobar que la aplicación de escritorio implemente los mecanismos de autenticación para realizar transacciones seguras, que la red física sea segura ante ataques snooping y manipulaciones, y que todos los dispositivos conectados a la red sean de confianza.

Como práctica recomendada, use las instancias del servidor de conexión dedicadas para administrar clientes en modo de pantalla completa y para crear grupos y unidades organizativas dedicadas en Active Directory para las cuentas de dichos clientes. Esta práctica no solo realiza particiones en estos sistemas ante intrusiones no deseadas, sino que también facilita la configuración y la administración de los clientes.

Para configurar el modo de pantalla completa, debe usar la interfaz de la línea de comandos `vdmadmin` y realizar varios procedimientos que aparecen en los temas sobre el modo de pantalla completa en el documento *Administración de Horizon 7*.

Como parte de esta configuración, puede usar una de las siguientes opciones de grupos de escritorios de clones instantáneos.

- Si está usando grupos de escritorios de clones instantáneos, Horizon 7 elimina automáticamente el clon instantáneo siempre que un usuario cierra sesión. Se crea un nuevo clon instantáneo que está preparado para que el siguiente usuario inicie sesión, actualizándose de forma eficaz cada vez que se cierra sesión.

Como parte de esta configuración, puede usar las siguientes opciones de grupos de escritorios de clones vinculados de View Composer.

- Si está usando escritorios de clones vinculados de View Composer, instituya una directiva de actualización para que el escritorio se actualice frecuentemente, por ejemplo, cada vez que un usuario cierra sesión.
- Si corresponde, considere almacenar escritorios en almacenes de datos ESXi locales. Esta estrategia ofrece ventajas como un hardware económico, un aprovisionamiento de máquina virtual

rápido, un rendimiento alto de las operaciones de alimentación y una administración sencilla. Para obtener una lista de limitaciones, consulte [Almacenes de datos locales para los escritorios de asignación flotante sin estado](#). Los grupos de clones instantáneos no son compatibles con los almacenes de datos locales.

Nota Si desea obtener información sobre otro tipo de opciones de almacenamiento, consulte [Reducir y administrar requisitos de almacenamiento](#).

Como parte de esta configuración, puede usar las siguientes opciones generales en todos los grupos de escritorios.

- Cree un grupo automatizado para que los escritorios puedan crearse cuando el grupo se cree o para que puedan generarse bajo demanda según el uso del grupo.
- Use asignación flotante para que los usuarios puedan acceder a cualquier escritorio disponible en el grupo.
- Cree escritorios de clones instantáneos o de clones vinculados de View Composer para que los escritorios compartan la misma imagen base y usen menos espacio de almacenamiento en el centro de datos que las máquinas virtuales completas.
- Use un objeto de directiva de grupo (GPO) de Active Directory para configurar la impresión según ubicación para que el escritorio use la impresora más cercana. Para obtener una descripción y una lista completa de las opciones disponibles a través de las plantillas administrativas (ADMX) de directivas de grupo, consulte *Configurar funciones de escritorios remotos en Horizon 7*.
- Use un GPO o directivas de Smart para controlar si los dispositivos USB locales se conectan al escritorio cuando este se inicia o cuando los dispositivos USB se conectan al equipo cliente.

Configuración de la máquina virtual del escritorio

Las configuraciones de ejemplo de elementos como la memoria, el número de procesadores virtuales y el espacio de disco son específicas de Horizon 7.

La cantidad de espacio de disco del sistema necesaria depende del número de aplicaciones que se necesiten en la imagen de base. VMware ha validado una configuración que incluía 8 GB de espacio de disco. Las aplicaciones incluían Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer, McAfee Antivirus y PKZIP.

La cantidad de espacio de disco necesaria para los datos del usuario depende de la función del usuario final y de las directivas de la organización para el almacenamiento de datos. Si se utiliza View Composer, estos datos se guardan en un disco persistente.

Las directrices indicadas en la tabla siguiente se aplican a un escritorio de máquina virtual estándar con Windows 7 o una versión más reciente.

Tabla 4-2. Ejemplo de escritorio de máquina virtual para Windows 7 o Windows 8

Elemento	Ejemplo
Sistema operativo	Windows 7 de 32 o 64 bits o una versión posterior (con el service pack más reciente)
RAM	1 GB (4 GB si los usuarios deben tener aceleración de gráficos por hardware para procesamiento 3D)
CPU virtual	1 (2 en el caso de sistemas de 64 bits o si los usuarios tienen que reproducir vídeo de alta definición o a pantalla completa)
Capacidad de disco del sistema	24 GB (algo menos de lo habitual)
Capacidad para datos del usuario (como disco persistente)	5 GB (punto de inicio)
Tipo de adaptador SCSI virtual	LSI Logic SAS (el predeterminado)
Adaptador de red virtual	VMXNET 3

Configuración de la máquina virtual del host RDS

Para proporcionar aplicaciones publicadas y escritorios remotos basados en sesión a los usuarios finales, se utilizan hosts RDS (Servicios de Escritorio remoto de Windows).

Un host RDS puede ser una máquina física o una máquina virtual. En este ejemplo, se utiliza una máquina virtual con las especificaciones indicadas en la tabla siguiente. El host ESXi de esta máquina virtual puede ser parte de un clúster VMware HA para protegerse contra fallos del servidor físico.

Tabla 4-3. Ejemplo de máquina virtual del host RDS

Elemento	Ejemplo
Sistema operativo	Windows Server 2008 R2 o Windows Server 2012 R2 de 64 bits
RAM	24 GB
CPU virtual	4
Capacidad de disco del sistema	40 GB
Tipo de adaptador SCSI virtual	LSI Logic SAS (el predeterminado para Windows Server 2008)
Adaptador de red virtual	VMXNET 3
1 NIC	1 Gigabit
Número máximo total de conexiones de cliente (incluyendo conexiones de aplicaciones publicadas y conexiones de escritorios remotos basados en sesión)	50

Nota Si configura hosts RDS en el punto inferior de las especificaciones de los recursos, pueden aparecer restricciones en estos al utilizar todas las funciones en lugar de la instalación predeterminada.

Para obtener más información sobre la configuración del host RDS y las cargas de trabajo comprobadas, consulte el documento técnico *Arquitectura de referencia de VMware Horizon 6* disponible en <http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf>.

Configuración de máquinas virtuales de vCenter Server y View Composer

Es posible instalar vCenter Server y View Composer en la misma máquina virtual o en servidores independientes. Estos servidores necesitan mucha más memoria y capacidad de procesamiento que una máquina virtual de escritorios.

VMware realizó pruebas en las que View Composer creó y aprovisionó 2.000 escritorios por grupo utilizando vSphere 5.1 o una versión posterior. VMware también realizó pruebas en las que View Composer efectuó una operación de recomposición en 2.000 escritorios a la vez. Para estas pruebas, vCenter Server y View Composer se instalaron en máquinas virtuales independientes.

El tamaño del grupo de escritorios está limitado por los siguientes factores:

- Cada grupo de escritorios solo puede contener un clúster de vSphere.
- En algunas configuraciones, los clústeres pueden contener hasta 32 hosts. En otras configuraciones, los clústeres se limitan a 8 hosts. Si desea obtener más información, consulte [Clústeres de vSphere](#).
- Cada núcleo de CPU tiene capacidad de computación para entre 8 y 10 escritorios virtuales.
- El número de direcciones IP disponibles para la subred limita el número de escritorios del grupo. Por ejemplo, si la red está configurada de manera que la subred del grupo contiene solo 256 direcciones IP utilizables, el tamaño del grupo se limita a 256 escritorios. No obstante, se pueden configurar varias etiquetas de red para expandir enormemente el número de direcciones IP asignadas a las máquinas virtuales de un grupo.

Aunque es posible instalar vCenter Server y View Composer en una máquina física, en este ejemplo se utilizan máquinas virtuales independientes con las especificaciones indicadas en las tablas siguientes. El host ESXi de esta máquina virtual puede ser parte de un clúster VMware de alta disponibilidad para protegerse contra fallos del servidor físico.

En este ejemplo, se supone que se utiliza Horizon 7 con vSphere 5.1 o una versión posterior y vCenter Server 5.1 o una versión posterior.

Importante En este ejemplo, también se supone que View Composer y vCenter Server están instalados en máquinas virtuales independientes.

Tabla 4-4. vCenter Server Ejemplo de máquina virtual

Elemento	Ejemplo de un vCenter Server que administra 10.000 escritorios	Ejemplo de un vCenter Server que administra 2.000 escritorios
Sistema operativo	Windows Server 2008 R2 Enterprise de 64 bits	Windows Server 2008 R2 Enterprise de 64 bits
RAM	48 GB	10-24 GB, según la versión de vSphere

Tabla 4-4. vCenter Server Ejemplo de máquina virtual (continuación)

Elemento	Ejemplo de un vCenter Server que administra 10.000 escritorios	Ejemplo de un vCenter Server que administra 2.000 escritorios
CPU virtual	16	2-8, según la versión de vSphere
Capacidad de disco del sistema	180 GB	40 GB
Tipo de adaptador SCSI virtual	LSI Logic SAS (el predeterminado para Windows Server 2008)	LSI Logic SAS (el predeterminado para Windows Server 2008)
Adaptador de red virtual	E1000 (el predeterminado)	VMXNET 3 (aunque E1000, el predeterminado, también se puede usar)
Número máximo de operaciones de aprovisionamiento de vCenter simultáneas	20	20
Número máximo de operaciones de encendido/apagado simultáneas	50	50

Tabla 4-5. Ejemplo de máquina virtual de View Composer

Elemento	Ejemplo de una instancia de View Composer que administra 10.000 escritorios	Ejemplo de una instancia de View Composer que administra 2.000 escritorios
Sistema operativo	Windows Server 2008 R2 Enterprise de 64 bits	Windows Server 2008 R2 Enterprise de 64 bits
RAM	10 GB o más, según la versión de vSphere	4-10 GB, según la versión de vSphere
CPU virtual	4 o más, según la versión de vSphere	2-4, según la versión de vSphere
Capacidad de disco del sistema	50 GB	40 GB
Tipo de adaptador SCSI virtual	LSI Logic SAS (el predeterminado para Windows Server 2008)	LSI Logic SAS (el predeterminado para Windows Server 2008)
Adaptador de red virtual	VMXNET 3	VMXNET 3
Tamaño máximo del grupo de View Composer	2.000 escritorios	1.000 escritorios
Número máximo de operaciones de mantenimiento simultáneas de View Composer	12	12
Número máximo de operaciones de aprovisionamiento simultáneas de View Composer	8	8

Importante VMware recomienda colocar la base de datos a la que se conectan vCenter Server y View Composer en una máquina virtual independiente.

Máximos del servidor de conexión de Horizon y configuración de máquinas virtuales

Al instalar el servidor de conexión de Horizon, se instala también la interfaz del usuario de Horizon Administrator.

Configuración del servidor de conexión

Aunque es posible instalar el servidor de conexión en un equipo físico, en este ejemplo se utiliza una máquina virtual con las especificaciones indicadas en Ejemplo de máquina virtual de servidor de conexión. El host ESXi de esta máquina virtual puede ser parte de un clúster VMware HA para protegerse contra fallos del servidor físico.

Tabla 4-6. Ejemplo de máquina virtual de servidor de conexión

Elemento	Ejemplo
Sistema operativo	Consulte los sistemas operativos admitidos en el documento <i>Instalación de Horizon 7</i> .
RAM	10 GB
CPU virtual	4
Capacidad de disco del sistema	70 GB
Tipo de adaptador SCSI virtual	LSI Logic SAS (el predeterminado para Windows Server 2008)
Adaptador de red virtual	VMXNET 3
Adaptador de red	NIC de 1 Gbps

Consideraciones para el diseño del clúster del servidor de conexión

Se pueden implementar varias instancias replicadas del servidor de conexión en un grupo para que admitan equilibrado de carga y alta disponibilidad. Los grupos de instancias replicadas están diseñados para admitir clústeres dentro de un entorno de centro de datos único conectado en una LAN.

Importante Para utilizar un grupo de instancias replicadas del servidor de conexión a través de una WAN, una MAN (red de área metropolitana) u otras redes que no sean LAN, en escenarios en los que una implementación de Horizon debe abarcar centros de datos, debe utilizar la función Arquitectura de Cloud Pod. Para obtener más información, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

Conexiones máximas para el servidor de conexión

Conexiones de escritorio remoto proporciona información sobre los límites probados en relación al número de conexiones simultáneas que puede admitir una implementación de Horizon 7.

Tabla 4-7. Conexiones de escritorio remoto

Instancias de servidores de conexión por implementación	Tipo de conexión	Número máximo de conexiones simultáneas
1 servidor de conexión	Conexión directa, RDP, Blast Extreme o PCoIP	4.000 (configuración comprobada)
1 servidor de conexión	Conexión de túnel, RDP	2.000 (configuración predeterminada) 4.000 (configuración comprobada)
1 servidor de conexión	conexión de puerta de enlace segura de PCoIP	2.000 (configuración predeterminada) 4.000 (configuración comprobada)
1 servidor de conexión	Conexión de puerta de enlace segura de Blast	2.000 (configuración predeterminada) 4.000 (configuración comprobada)
1 servidor de conexión	Unified Access para PC físicos	2.000 (configuración comprobada)
1 servidor de conexión	Unified Access para hosts RDS	2.000 (configuración comprobada)
7 servidores de conexión	Conexión directa, RDP, Blast Extreme o PCoIP	Hosts RDS <ul style="list-style-type: none"> ■ 10.000 (configuración predeterminada) ■ 20.000 (configuración comprobada) Escritorios virtuales <ul style="list-style-type: none"> ■ 12.000 (configuración comprobada)

Nota Las configuraciones comprobadas se admiten por completo. Para obtener la configuración comprobada de un máximo de 4.000 conexiones simultáneas en un solo servidor de conexión para la conexión de túnel, de puerta de enlace segura PCoIP y de puerta de enlace segura de Blast, cree el archivo de `locked.properties` en la máquina virtual en la que esté instalado el servidor de conexión: `C:\Program Files\VMware\VMware View\Server\sslgateway\conf`. A continuación, asigne el valor `maxConnections=4000` al archivo `locked.properties` y reinicie el servidor de conexión. Como Unified Access Gateway actualmente admite 2.000 sesiones, se utilizaron 14 dispositivos Unified Access Gateway para probar 20.000 sesiones.

Es necesario utilizar conexiones de puerta de enlace segura de PCoIP si se utilizan servidores de seguridad o dispositivos de Unified Access Gateway para las conexiones de PCoIP desde fuera de la red corporativa. Es necesario utilizar conexiones de puerta de enlace segura de Blast si se utilizan servidores de seguridad o dispositivos de Unified Access Gateway para conexiones de Blast Extreme o HTML Access desde fuera de la red corporativa. Es necesario utilizar conexiones de túnel si se utilizan servidores de seguridad o dispositivos de Unified Access Gateway para conexiones RDP desde fuera de la red corporativa y aceleración de redireccionamiento USB y de multimedia (MMR) con una conexión de puerta de enlace segura de Blast o PCoIP. Es posible emparejar varios servidores de seguridad con una sola instancia del servidor de conexión.

Aunque un único servidor de seguridad o dispositivo Unified Access Gateway puede dar soporte a un máximo de 2.000 conexiones simultáneas, en lugar de usar solo un servidor de seguridad por instancia de servidor de conexión (con 2.000 sesiones), puede elegir usar 2 o 4. La supervisión del servidor de seguridad podría indicar que la actividad para 2.000 usuarios es excesiva. El uso de CPU y la cantidad de memoria necesaria pueden obligar a que se agreguen más servidores de seguridad por cada

instancia del servidor de conexión para repartir la carga. Por ejemplo, se podrían usar 2 servidores de seguridad, cada uno de los cuales gestionaría 1.000 conexiones, o 4 servidores de seguridad, cada uno de los cuales gestionaría 500 conexiones. La proporción de servidores de seguridad en relación a las instancias del servidor de conexión depende de los requisitos de cada entorno particular.

El número de conexiones por dispositivo de Unified Access Gateway es similar al de los servidores de seguridad. Para obtener más información sobre los dispositivos de Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Nota En este ejemplo, aunque 5 instancias del servidor de conexión (configuradas correctamente) podrían gestionar 20.000 conexiones, en la tabla aparecen 7 por razones de planificación de la disponibilidad y para acomodar conexiones procedentes tanto de dentro como de fuera de la red corporativa.

Por ejemplo, si hubiera 20.000 usuarios de los cuales 16.000 están dentro de la red corporativa, se necesitarían 5 instancias del servidor de conexión dentro de la red corporativa. De esa manera, si una de las instancias dejara de estar disponible, las 4 restantes podrían gestionar la carga. De forma similar, para las 4.000 conexiones procedentes de fuera de la red corporativa, se usarían 2 instancias del servidor de conexión de manera que, si una dejara de estar disponible, seguiría quedando otra que podría gestionar la carga.

Estos números asumen que las conexiones externas se presentan mediante una puerta de enlace. En este ejemplo, cada instancia del servidor de conexión que gestiona conexiones externas se emparejaría con 3 servidores de seguridad, por lo que si uno deja de estar disponible, los 2 servidores de seguridad restantes podrían gestionar la carga. Si usa dispositivos Unified Access Gateway en lugar de servidores de seguridad, podría necesitar 3 en total y equilibrar la carga en ambas instancias del servidor de conexión, de forma que si una deja de estar disponible, los 2 dispositivos restantes pueden gestionar la carga.

En todos los casos, los usuarios necesitarían volver a conectarse si estaban usando un servidor de conexión o una puerta de enlace que deja de estar disponible.

Requisitos de hardware para Unified Access Gateway con Horizon 7

VMware recomienda utilizar 2 vCPU y 4GB de RAM para que los dispositivos de Unified Access Gateway admitan el número máximo de conexiones cuando se utiliza con Horizon 7.

Tabla 4-8. Requisitos de hardware para Unified Access Gateway

Elemento	Ejemplo
Sistema operativo	OVA
RAM	4 GB
CPU virtual	2
Capacidad de disco del sistema	20 GB (si se cambia el nivel de registro predeterminado se necesita más espacio)
Tipo de adaptador SCSI virtual	LSI Logic Parallel (el predeterminado para OVA)

Tabla 4-8. Requisitos de hardware para Unified Access Gateway (continuación)

Elemento	Ejemplo
Adaptador de red virtual	VMXNET 3
Adaptador de red	NIC de 1 Gbps
Asignación de redes	Opción de una sola NIC

Clústeres de vSphere

Las implementaciones de Horizon 7 pueden utilizar clústeres de alta disponibilidad de VMware para protegerse de fallos del servidor físico. Dependiendo de la configuración, los clústeres pueden contener hasta 32 nodos.

vSphere y vCenter Server ofrecen un gran número de funciones para administrar clústeres de servidores que alojan escritorios de máquinas virtuales. La configuración del clúster también es importante porque cada grupo de escritorios de máquina virtual debe estar asociado a un grupo de recursos de vCenter Server. Por tanto, el número máximo de escritorios por grupo está en relación al número de servidores y máquinas virtuales que se prevé ejecutar por clúster.

En implementaciones muy grandes de Horizon 7, el rendimiento y la capacidad de respuesta de vCenter Server se puede mejorar si se tiene solo un objeto de clúster por cada objeto de centro de datos, que no es el comportamiento predeterminado. De forma predeterminada, vCenter Server crea nuevos clústeres dentro del mismo objeto de centro de datos.

Nota Si desea ver las recomendaciones y la información más reciente sobre los límites de tamaño de Horizon 7, consulte el artículo de la base de conocimientos de VMware <https://kb.vmware.com/s/article/2150348>.

En las condiciones siguientes, los clústeres de vSphere pueden contener hasta 32 hosts ESXi, o nodos:

- vSphere 5.1 y versiones posteriores, con grupos de clones vinculados de View Composer, y discos de réplicas de almacén en almacenes de datos NFS o almacenes de datos VMFS5 o versiones posteriores
- vSphere 6.0 y versiones posteriores, y grupos de almacén en almacenes de datos de Virtual Volumes

Si tiene vSphere 5.5 Update 1 y versiones posteriores, y grupos de almacenamiento en almacenes de datos vSAN, los clústeres de vSphere pueden contener hasta 20 hosts ESXi.

Si se almacenan réplicas de View Composer en una versión de VMFS anterior a VMFS5, un clúster puede tener como máximo ocho hosts. Los discos de SO y los discos persistentes se pueden almacenar en almacenes de datos NFS o VMFS.

Si desea obtener más información, consulte el capítulo sobre la creación de grupos de escritorio en el documento *Configurar escritorios virtuales en Horizon 7*. Los requisitos de red dependen del tipo de servidor, el número de adaptadores de red y la manera en que se configure VMotion.

Determinar los requisitos para alta disponibilidad

vSphere, gracias a su eficiencia y administración de recursos, permite conseguir niveles de máquinas virtuales por servidor líderes en la industria. Sin embargo, conseguir una mayor densidad de máquinas virtuales por servidor significa que el número de usuarios afectados si falla un servidor es mayor.

Los requisitos de la alta disponibilidad pueden diferir sustancialmente en función de la finalidad del grupo de escritorios. Por ejemplo, un grupo de imágenes de escritorios sin estado (asignación flotante) puede tener requisitos de objetivo de punto de recuperación (RPO) distintos a un grupo de imágenes de escritorio con estado (asignación dedicada). En grupos de asignación flotante, una solución aceptable podría ser hacer que los usuarios iniciaran la sesión en un escritorio diferente si el que están utilizando deja de estar disponible.

En casos en los que los requerimientos de disponibilidad sean elevados, es esencial realizar una configuración apropiada de alta disponibilidad de VMware. Si se utiliza la alta disponibilidad de VMware y se planifica un número fijo de escritorios por servidor, se debe ejecutar cada servidor con una capacidad reducida. Si el servidor falla, la capacidad de escritorios por servidor no se excede cuando los escritorios se reinician en un host diferente.

Por ejemplo, en un clúster de 8 hosts, en el que cada host puede ejecutar 128 escritorios, y el objetivo es tolerar el fallo de un servidor única, se debe asegurar que no se ejecuten más de $128 * (8 - 1) = 896$ escritorios en dicho clúster. También se puede usar VMware DRS (Distributed Resource Scheduler) para ayudar a equilibrar los escritorios entre los 8 hosts. Se consigue un pleno uso de la capacidad adicional del servidor sin permitir que ningún recurso de reserva en caliente permanezca inactivo. Además, DRS pueden ayudar a reequilibrar el clúster después de volver a poner en servicio un servidor que haya fallado.

También se debe asegurar que el almacenamiento esté configurado correctamente para admitir la carga de E/S originada cuando numerosas máquinas virtuales se reinician a la vez en respuesta a un fallo del servidor. Las operaciones de IOPS de almacenamiento son las que afectan más a la rapidez con que se recuperan los escritorios de un fallo del servidor.

Ejemplo: Ejemplos de configuración de clústeres

Las configuraciones indicadas en las tablas siguientes son específicas de Horizon 7. Para obtener información sobre los límites de los clústeres de alta disponibilidad en vSphere, consulte el documento de *VMware vSphere valores máximos de configuración*.

Nota El siguiente ejemplo de infraestructura se probó con View 5.2 y vSphere 5.1. En el ejemplo, se utilizan clones vinculados de View Composer, en lugar de clones instantáneos, porque la prueba se realizó con View 5.2. La función de clones instantáneos se introdujo en Horizon 7. Otras funciones que no estaban disponibles con View 5.2 incluyen vSAN y Virtual Volumes.

Tabla 4-9. Ejemplo de clúster de infraestructura de Horizon 7

Elemento	Ejemplo
Máquinas virtuales	Instancias de vCenter Server, Active Directory, servidor de base de datos SQL, View Composer, instancias del servidor de conexión, servidores de seguridad, máquinas virtuales principales para usar como orígenes de grupos de escritorios
Nodos (hosts ESXi)	6 servidores Dell PowerEdge R720 (16 núcleos * 2 GHz; y 192 GB de RAM en cada host)
Almacenamiento SSD	Máquinas virtuales para vCenter Server, View Composer, servidor de base de datos SQL y las máquinas virtuales principales
Almacenamiento no SSD	Máquinas virtuales para Active Directory, el servidor de conexión y el servidor de seguridad
Tipo de clúster	DRS (Distributed Resource Scheduler)/HA

Tabla 4-10. Ejemplo de clúster de escritorios de máquinas virtuales

Elemento	Ejemplo
Número de clústeres	5
Número de escritorios y grupos por clúster	1 grupo de 2.000 escritorios (máquinas virtuales) por clúster
Nodos (hosts ESXi)	A continuación, se incluyen ejemplos de diversos servidores que se podrían utilizar para cada clúster: <ul style="list-style-type: none"> ■ 12 servidores Dell PowerEdge R720 (16 núcleos * 2 GHz; y 192 GB de RAM en cada host) ■ 16 servidores Dell PowerEdge R710 (12 núcleos * 2,526 GHz; y 144 GB de RAM en cada host) ■ 8 servidores Dell PowerEdge R810 (24 núcleos * 2 GHz; y 256 GB de RAM en cada host) ■ 6 servidores Dell PowerEdge R810 + 3 PowerEdge R720
Almacenamiento SSD	Máquinas virtuales de réplica
Almacenamiento no SSD	32 almacenes de datos no SSD para clonaciones (450 GB por almacén de datos)
Tipo de clúster	DRS (Distributed Resource Scheduler)/HA

Requisitos de almacenamiento y ancho de banda

Al planificar el almacenamiento compartido para escritorios de máquinas virtuales, los requisitos de ancho de banda de almacenamiento durante las sobrecargas de E/S y las necesidades de ancho de banda de la red, es necesario considerar varias cuestiones.

En los temas relacionados, se incluyen los detalles de los componentes de la red y el almacenamiento utilizados en una configuración de prueba en VMware.

■ [Ejemplo de almacenamiento compartido](#)

En un entorno de prueba de View 5.2, se colocaron máquinas virtuales de réplica de View Composer en unidades de estado sólido (SSD) con alto rendimiento de lectura, que admiten decenas de miles de operaciones de E/S por segundo (IOPS). Los clones vinculados se colocaron en almacenes de datos de medios giratorios de bajo rendimiento, que son menos caros y ofrecen una mayor capacidad de almacenamiento. En el ejemplo, se usan clones vinculados de View Composer en lugar de clones instantáneos, porque la prueba se realizó con View 5.2. La función de clones instantáneos se introdujo en Horizon 7.

- **Consideraciones de ancho de banda de almacenamiento**

En un entorno de Horizon 7, las sobrecargas de inicio de sesión son el principal factor a tener en cuenta al determinar los requisitos de ancho de banda.

- **Consideraciones de ancho de banda**

Para admitir una carga de trabajo normal, se necesitan determinados componentes de red físicos y virtuales.

- **Resultados de la prueba de rendimiento de View Composer**

Estos resultados describen una configuración de View 5.2 con 10.000 escritorios, en la que una instancia de vCenter Server 5.1 administraba 5 grupos de 2.000 escritorios de máquinas virtuales cada uno. Solo se requirió un período de mantenimiento para el aprovisionamiento de un nuevo grupo o para recomponer, actualizar o reequilibrar un grupo existente de 2.000 máquinas virtuales. También se probó una sobrecarga de inicio de sesión de 10.000 usuarios.

- **Compatibilidad WAN**

En redes de área extendida (WAN), se deben tener en cuenta las restricciones de ancho de banda y los problemas de latencia. Los protocolos de visualización PCoIP y Blast Extreme proporcionados por VMware se adaptan a condiciones cambiantes de latencia y ancho de banda.

Ejemplo de almacenamiento compartido

En un entorno de prueba de View 5.2, se colocaron máquinas virtuales de réplica de View Composer en unidades de estado sólido (SSD) con alto rendimiento de lectura, que admiten decenas de miles de operaciones de E/S por segundo (IOPS). Los clones vinculados se colocaron en almacenes de datos de medios giratorios de bajo rendimiento, que son menos caros y ofrecen una mayor capacidad de almacenamiento. En el ejemplo, se usan clones vinculados de View Composer en lugar de clones instantáneos, porque la prueba se realizó con View 5.2. La función de clones instantáneos se introdujo en Horizon 7.

Las consideraciones relativas al diseño del almacenamiento constituyen uno de los elementos más importantes para el éxito de una arquitectura de Horizon 7. La decisión que tiene mayor impacto en la arquitectura es decidir si utilizar escritorios de View Composer, que emplean tecnología de clones vinculados. Los archivos binarios de ESXi, los archivos de intercambio de la máquina virtual y las réplicas de View Composer de máquinas virtuales principales se almacenan en un sistema de almacenamiento compartido.

El sistema de almacenamiento externo que utiliza vSphere puede ser una red SAN (red de área de almacenamiento) de canal de fibra o iSCSI, o bien un NAS (almacenamiento adjunto a la red) NFS (Network File System). Con la función vSAN, disponible con vSphere 5.5 Update 1 o versiones posteriores, el sistema de almacenamiento también puede ser almacenamiento agregado adjunto al servidor local.

En el ejemplo siguiente, se describe la estrategia de almacenamiento en niveles utilizada en una configuración de prueba de View 5.2, en la que un vCenter Server administró 10.000 escritorios.

Nota Este ejemplo se utilizó en una configuración de View 5.2, que se realizó antes de la publicación de VMware vSAN. Para obtener más información acerca de ajustar el tamaño y diseñar los componentes clave de las infraestructuras de escritorio virtual de View para VMware vSAN, consulte el documento técnico disponible en <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

La función vSAN disponible con vSphere 6.0 y versiones posteriores contiene numerosas mejoras de rendimiento en comparación con la función disponible con vSphere 5.5 Update 1. Con vSphere 6.0, esta función también tiene una mayor compatibilidad de hardware (HCL). Para obtener más información sobre vSAN en vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware vSAN*.

Almacenamiento físico

- Solo bloque EMC VNX7500
- 1,8 TB Fast Cache (SSD)
- Ocho conexiones front-end FCoE de 10 Gbit (4 por controlador).

Nivel de almacenamiento SSD

Un solo grupo de almacenamiento RAID5:

- 12 EFD de 200 GB
- LUN de 250 GB para imágenes principales
- LUN de 500 GB para infraestructura
- LUN de 75 GB para almacenes de réplicas (1 por clúster de grupos de escritorios)

Nivel de almacenamiento de escritorios de máquinas virtuales

Dos grupos de almacenamiento RAID 1/0:

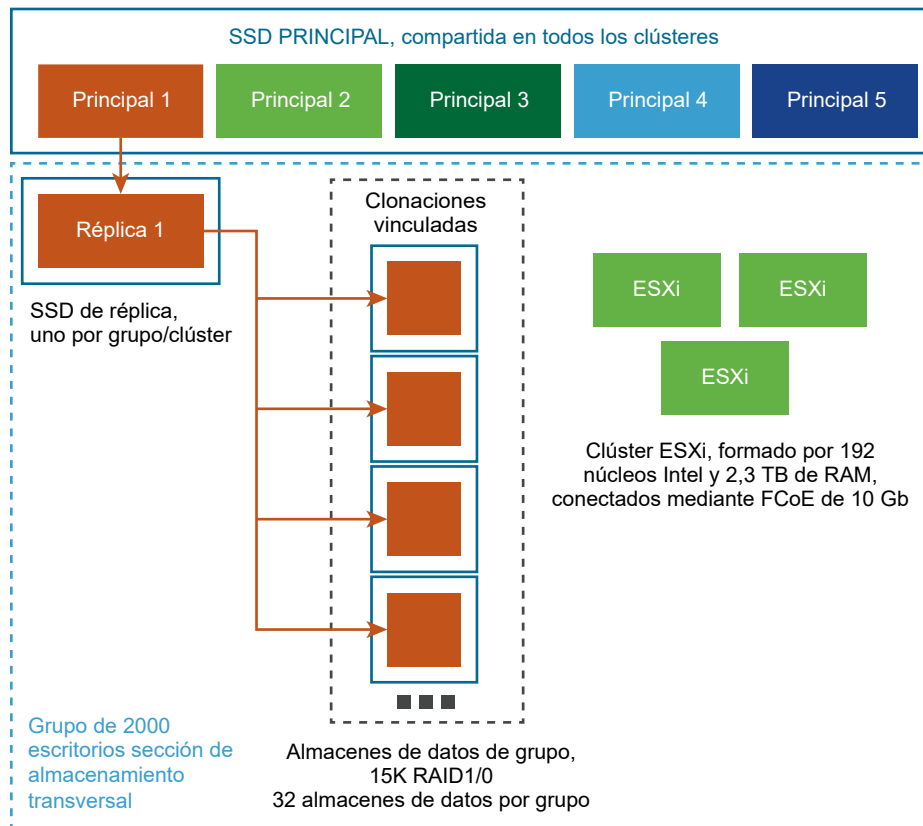
Para el grupo 1:

- 360 discos duros de 300 GB y 15.000 rpm (47 TB utilizables)
- 97 LUN de 450 GB para escritorios

Para el grupo 2:

- 296 discos duros de 300 GB y 15.000 rpm (39 TB utilizables)
- 7 LUN de 450 GB para infraestructura
- 85 LUN de 450 GB para escritorios

Esta estrategia de almacenamiento se ilustra en la figura siguiente.

Figura 4-1. Ejemplo de almacenamiento en niveles para un grupo de escritorios grande

Desde la perspectiva de la arquitectura, View Composer crea imágenes de escritorio que comparte una imagen de base, lo que puede reducir los requisitos de almacenamiento un 50% o más. Los requisitos de almacenamiento se pueden reducir aún más si se configura una directiva de actualización que devuelva periódicamente el escritorio a su estado original y recupere espacio utilizado para el seguimiento de cambios desde la última operación de actualización.

Si se utiliza View Composer con escritorios de máquina virtual vSphere 5.1 o versiones posteriores, se puede utilizar la función de recuperación de espacio. Con esta función, el espacio ocupado por los datos antiguos o borrados de un sistema operativo invitado se recupera automáticamente mediante un proceso de limpieza y reducción cuando la cantidad de espacio de disco sin utilizar alcanza un determinado umbral. Tenga en cuenta que la función de recuperación de espacio no es compatible con almacenes de datos vSAN.

Para reducir el espacio de disco ocupado por el sistema, se pueden usar también discos persistentes de View Composer o un servidor de archivos compartidos como repositorio principal para el perfil y los documentos del usuario. Como View Composer permite separar los datos de usuario del sistema operativo, es posible que solo sea necesario replicar o hacer una copia de seguridad del disco persistente, lo que reduce aún más los requisitos de almacenamiento. Si desea obtener más información, consulte [Reducir requisitos de almacenamiento con Composer](#).

Nota El mejor momento para tomar decisiones relativas a los componentes de almacenamiento dedicado es durante una fase piloto. El elemento principal a considerar es las operaciones de E/S por segundo (IOPS). Se puede probar a utilizar una estrategia de almacenamiento en niveles o almacenamiento de vSAN para maximizar el rendimiento y la reducción de costes.

Si desea obtener más información, consulte la guía de prácticas recomendadas *Consideraciones de almacenamiento para VMware View*.

Consideraciones de ancho de banda de almacenamiento

En un entorno de Horizon 7, las sobrecargas de inicio de sesión son el principal factor a tener en cuenta al determinar los requisitos de ancho de banda.

Aunque numerosos elementos son importantes al diseñar un sistema de almacenamiento que admita un entorno de Horizon 7, desde una perspectiva de configuración del servidor, es esencial planificar el ancho de banda de almacenamiento adecuado. También se deben considerar los efectos del hardware de consolidación de puertos.

Los entornos de Horizon 7 pueden experimentar ocasionalmente sobrecargas de E/S, durante las cuales todas las máquinas virtuales realizan una actividad al mismo tiempo. Las sobrecargas de E/S pueden ser debidas a agentes basados en el invitado, como software antivirus o agentes de actualización de software. Las sobrecargas de E/S también se pueden deber al comportamiento humano, como cuando todos los empleados inician la sesión prácticamente al mismo tiempo por la mañana. VMware ha probado un escenario de sobrecarga para 10.000 escritorios. Si desea obtener más información, consulte [Resultados de la prueba de rendimiento de View Composer](#).

Estas sobrecargas se pueden minimizar mediante el empleo de prácticas operativas recomendadas, tales como el escalonamiento de las actualizaciones en distintas máquinas virtuales. También se pueden probar varias directivas de cierre de sesión durante una fase piloto para determinar si suspender o apagar las máquinas virtuales cuando el usuario cierra la sesión provoca una sobrecarga de E/S. Si se almacenan réplicas de View Composer en almacenes de datos de alto rendimiento independientes, se pueden acelerar las operaciones intensivas y simultáneas de lectura para enfrentarse a las sobrecargas de E/S. Por ejemplo, se puede usar una de las siguientes estrategias de almacenamiento:

- Configurar manualmente el grupo para que las réplicas se almacenen en almacenes de datos de alto rendimiento independientes.
- Utilizar vSAN, disponible con vSphere 5.5 Update 1 o versiones posteriores, que utiliza una administración basada en directivas de software para determinar qué tipos de discos se deben utilizar para replicas.

- Utilizar Virtual Volumes, disponible con vSphere 6.0 o versiones posteriores, que utiliza una administración basada en directivas de software para determinar qué tipos de discos se deben utilizar para réplicas.

Además de determinar las prácticas recomendadas, VMware recomienda proporcionar un ancho de banda de 1 Gbps por cada 100 máquinas virtuales, aunque el promedio de ancho de banda sea 10 veces inferior a ese. Una planificación tan conservadora garantiza suficiente conectividad de almacenamiento para picos de carga.

Consideraciones de ancho de banda

Para admitir una carga de trabajo normal, se necesitan determinados componentes de red físicos y virtuales.

Son muchos los elementos que pueden afectar al ancho de banda en el caso del tráfico de visualización, tales como el protocolo utilizado, la resolución y configuración del monitor y la cantidad de contenido multimedia de la carga de trabajo. El lanzamiento simultáneo de aplicaciones de streaming también puede ocasionar picos de uso.

Como los efectos de estos elementos pueden variar mucho, numerosas empresas supervisan el consumo de ancho de banda como parte de un proyecto piloto. Como punto de inicio para un programa piloto, se puede prever una capacidad entre 150 y 200 Kbps para un trabajador del conocimiento normal.

Si se utiliza el protocolo de visualización PCoIP o Blast Extreme, en una LAN conmutada de 100 Mb o 1Gb, los usuarios finales pueden esperar un rendimiento excelente en las siguientes condiciones:

- Dos monitores (1920 x 1080)
- Uso intensivo de aplicaciones de Microsoft Office
- Uso intensivo de navegación web con Flash
- Uso frecuente de multimedia con uso limitado del modo de pantalla completa
- Uso frecuente de periféricos basados en USB
- Impresión basada en red

Para obtener más información, consulte la guía sobre el *protocolo de visualización PCoIP: información y tamaño de las redes basadas en escenarios*.

Controles de optimización disponibles con PCoIP y Blast Extreme

Si se utiliza el protocolo de visualización PCoIP o Blast Extreme de VMware, se pueden ajustar varios elementos que afectan al uso de ancho de banda.

- Es posible configurar el nivel de calidad de la imagen y la velocidad de fotogramas utilizados en períodos de congestión de la red. La configuración del nivel de calidad permite limitar la calidad inicial de las regiones modificadas de la imagen de visualización. También es posible ajustar la velocidad de fotogramas.

Este control funciona bien con contenido de pantalla estático que no es necesario actualizar o en situaciones en las que solo sea necesario actualizar una parte.

- En cuanto al ancho de banda de la sesión, es posible configurar el ancho de banda máximo, en kilobits por segundo, para que se corresponda al tipo de conexión de red, como en el caso de una conexión a Internet de 4 Mbit/s. El ancho de banda incluye todo el tráfico de control de PCoIP o Blast, USB, canal virtual, audio e imágenes.

También se puede configurar un límite inferior, en kilobits por segundo, para el ancho de banda reservado para la sesión, de manera que el usuario no tenga que esperar a que haya ancho de banda disponible. Se puede especificar el tamaño de la unidad de transmisión máxima (MTU) para los paquetes UDP de una sesión, entre 500 y 1500 bytes.

Para obtener más información, consulte las secciones "Configuración general de PCoIP" y "Configuración de directivas de VMware Blast" en *Configurar funciones de escritorios remotos en Horizon 7*.

Ejemplo de configuración de red

En un pod de prueba de View 5.2 en el que una instancia de vCenter Server 5.1 administraba 5 grupos de 2.000 máquinas virtuales en cada grupo, cada uno de los hosts ESXi tenía el siguiente hardware y software para los requisitos de red.

Nota Este ejemplo se utilizó en una configuración de View 5.2, que se realizó antes de la publicación de VMware vSAN. Para obtener más información acerca de ajustar el tamaño y diseñar los componentes clave de las infraestructuras de escritorio virtual de View para VMware vSAN, consulte el documento técnico disponible en <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>. Además, en el ejemplo se usan clones vinculados de View Composer en lugar de clones instantáneos, porque la prueba se realizó con View 5.2. La función de clones instantáneos se introdujo en Horizon 7.

Componentes físicos para cada host

- Brocade 1860 Fabric Adapter con Ethernet de 10 Gb y FCoE para el tráfico de red y de almacenamiento, respectivamente.
- Conexión a un tejido Brocade VCS Ethernet formado por 6 conmutadores VDX6720-60. Los conmutadores se conectaron al resto de la red mediante dos conexiones ascendentes de 1 Gb a un router Juniper J6350.

Resumen de vLAN

- Una vLAN de 10 Gb por grupo de escritorios (5 grupos)
- Una vLAN de 1 Gb para la red de administración
- Una vLAN de 1 Gb para la red de VMotion
- Una vLAN de 10 Gb para la red de infraestructura

Virtual VMotion-dvswitch (1 enlace ascendente por host)

Este switch lo utilizaban los hosts ESXi de infraestructura y máquinas virtuales de escritorios y principales.

- Jumbo Frame (9000 MTU)
- 1 grupo de puertos distribuidos efímeros

Infra-dvswitch (2 enlaces ascendentes por host)	<ul style="list-style-type: none"> ■ Direccionamiento 192.168.x.x y VLAN privada <p>Este switch lo utilizaban los hosts ESXi de máquinas virtuales de infraestructura.</p> <ul style="list-style-type: none"> ■ Jumbo frame (9000 MTU) ■ 1 grupo de puertos distribuidos efímeros ■ Infraestructura VLAN /24 (256 direcciones)
Desktop-dvswitch (2 enlaces ascendentes por host)	<p>Este switch lo utilizaban los hosts ESXi de máquinas virtuales principales y de escritorios.</p> <ul style="list-style-type: none"> ■ Jumbo frame (9000 MTU) ■ 6 grupos de puertos distribuidos efímeros ■ 5 grupos de puertos de escritorio (1 por grupo) ■ Cada red era de /21, 2048 direcciones

Resultados de la prueba de rendimiento de View Composer

Estos resultados describen una configuración de View 5.2 con 10.000 escritorios, en la que una instancia de vCenter Server 5.1 administraba 5 grupos de 2.000 escritorios de máquinas virtuales cada uno. Solo se requirió un período de mantenimiento para el aprovisionamiento de un nuevo grupo o para recomponer, actualizar o reequilibrar un grupo existente de 2.000 máquinas virtuales. También se probó una sobrecarga de inicio de sesión de 10.000 usuarios.

Los resultados de la prueba incluidos aquí se obtuvieron con la configuración, el hardware y el software descritos en los temas siguientes:

- Configuraciones de grupos y escritorios descritas en [Máximos del servidor de conexión de Horizon y configuración de máquinas virtuales](#)
- Componentes de almacenamiento en niveles descritos en [Ejemplo de almacenamiento compartido](#)
- Componentes de red descritos en [Consideraciones de ancho de banda](#)

Capacidad para una sobrecarga de 10.000 usuarios durante una hora

Nota Este ejemplo se utilizó en una configuración de View 5.2, que se realizó antes de la publicación de VMware vSAN. Para obtener más información acerca de ajustar el tamaño y diseñar los componentes clave de las infraestructuras de escritorio virtual de View para VMware vSAN, consulte el documento técnico disponible en <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>. Para ver los resultados de la prueba con diversas cargas de trabajo y operaciones de View cuando se utiliza vSAN, consulte el documento técnico de la arquitectura de referencia que se encuentra en <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf>.

La función vSAN disponible con vSphere 6.0 y versiones posteriores contiene numerosas mejoras de rendimiento en comparación con la función disponible con vSphere 5.5 Update 1. Con vSphere 6.0, esta función también tiene una mayor compatibilidad de hardware (HCL). Para obtener más información sobre vSAN en vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware vSAN*.

En una configuración de prueba, las siguientes configuraciones de grupos y escritorios se usan en un escenario de inicio de sesión masivo de 10.000 escritorios. La directiva de alimentación de los escritorios estaba establecida como siempre activa.

Con 10.000 escritorios, el inicio de sesión masivo se produjo en un periodo de 60 minutos aproximadamente, usando una distribución normal de horas de inicio de sesión. Las máquinas virtuales se encendieron y estaban disponibles antes de que comenzara el inicio de sesión masivo. Después del inicio de sesión, se inició una carga de trabajo que incluye las siguientes aplicaciones: Adobe Reader, Microsoft Outlook, Internet Explorer, Microsoft Word y Notepad.

A continuación, aparecen detalles adicionales sobre el inicio de sesión masivo:

- 95% de inicios de sesión se producen en +/- 2 ventanas de desviación estándar (40 minutos).
- 68% de inicios de sesión se producen en +/- 1 ventana de desviación estándar (20 minutos).
- La velocidad máxima de inicio de sesión fue de 400 por minuto o de 6,67 por segundo.

Tiempo necesario para el aprovisionamiento de un grupo

Los grupos se aprovisionan previamente, cuando se crean, o bajo demanda, a medida que se asignan usuarios a ellos. El aprovisionamiento significa crear la máquina virtual y configurarla para que utilice la configuración de red y la imagen del sistema operativo correctas.

En una configuración de prueba que ya contenía 4 grupos de 2.000 máquinas virtuales en cada uno, el aprovisionamiento de un quinto grupo que contenía 2.000 máquinas virtuales tardó 4 horas. Todas las máquinas virtuales se aprovisionaron previamente.

Tiempo necesario para la recomposición de un grupo

Las operaciones de recomposición se pueden usar para proporcionar revisiones del sistema operativo, instalar o actualizar aplicaciones o modificar la configuración de hardware de los escritorios de las máquinas virtuales de un grupo. Antes de recomponer un grupo, se realiza una snapshot de una máquina virtual que tenga la nueva configuración. La operación de recomposición utiliza esa snapshot para actualizar todas las máquinas virtuales del grupo.

En una configuración de prueba con 5 grupos de 2.000 máquinas virtuales en cada uno, la recomposición de un grupo de 2.000 máquinas virtuales tardó 6 horas y 40 minutos. Todas las máquinas virtuales estaban encendidas y disponibles antes de comenzar la operación de recomposición.

Tiempo necesario para la actualización de un grupo

Como los discos aumentan de tamaño con el tiempo, se puede ahorrar espacio de disco actualizando un escritorio a su estado original cuando los usuarios cierran la sesión, o bien establecer un programa para la actualización periódica de los escritorios. Por ejemplo, puede programar los escritorios para que se actualicen diariamente, semanalmente o mensualmente.

En una configuración de prueba con 5 grupos de 2.000 máquinas virtuales en cada uno, la actualización de un grupo de 2.000 máquinas virtuales tardó 2 horas y 40 minutos. Todas las máquinas virtuales estaban encendidas y disponibles antes de comenzar la operación de actualización.

Tiempo necesario para el reequilibrado de un grupo

La operación de reequilibrado vuelve a distribuir uniformemente las máquinas virtuales de clones vinculados entre las unidades lógicas disponibles. La operación de reequilibrado ahorra espacio de almacenamiento en unidades sobrecargadas y asegura que ninguna unidad se infrutilice. Las operaciones de reequilibrado también se pueden utilizar para migrar todas las máquinas virtuales de un grupo de escritorios a o desde un almacén de datos vSAN.

En un pod de prueba que contenía 5 grupos con 2.000 máquinas virtuales en cada grupo, se agregaron 2 almacenes de datos al pod para una prueba. Para otra prueba, se eliminaron 2 almacenes de datos del pod. Después de agregar o eliminar los almacenes de datos, se realizó una operación de reequilibrado en uno de los grupos. El reequilibrado de un grupo de 2.000 máquinas virtuales tardó 9 horas. Todas las máquinas virtuales estaban encendidas y disponibles antes de comenzar la operación de reequilibrado.

Compatibilidad WAN

En redes de área extendida (WAN), se deben tener en cuenta las restricciones de ancho de banda y los problemas de latencia. Los protocolos de visualización PCoIP y Blast Extreme proporcionados por VMware se adaptan a condiciones cambiantes de latencia y ancho de banda.

Si se utiliza el protocolo de visualización RDP, se debe disponer de un producto de optimización de WAN para acelerar las aplicaciones para los usuarios de sucursales o pequeñas oficinas. Con PCoIP y Blast Extreme, muchas técnicas de optimización de WAN están integradas en el protocolo base.

- La optimización de WAN es valiosa para protocolos basados en TCP, tales como RDP, porque estos protocolos requieren muchos protocolos de enlace entre el cliente y el servidor. La latencia de estos protocolos de enlace puede ser bastante grande. Los aceleradores de WAN simulan respuestas a los protocolos de enlace para ocultar la latencia de la red al protocolo. Como PCoIP y Blast Extreme están basados en UDP, esta forma de aceleración de WAN es innecesaria.
- Los aceleradores de WAN también comprimen el tráfico de red entre el cliente y el servidor, pero esta compresión normalmente se limita a índices 2:1. PCoIP y Blast Extreme tienen índices de compresión mucho más elevados.

Para obtener información sobre los controles que se pueden utilizar para ajustar la manera en que PCoIP y Blast Extreme consumen ancho de banda, consulte [Controles de optimización disponibles con PCoIP y Blast Extreme](#).

Requisitos de ancho de banda para distintos tipos de usuarios

Al determinar los requisitos mínimos de ancho de banda para PCoIP, se deben tener en cuenta las siguientes estimaciones:

- Un ancho de banda medio de 100 a 150 Kbps para un escritorio de productividad de oficina básico: aplicaciones típicas de oficina sin vídeo, sin gráficos 3D y con la configuración predeterminada de Windows y Horizon 7.
- Un ancho de banda medio de 50 a 100 Kbps para un escritorio de productividad de oficina optimizado: aplicaciones típicas de oficina sin vídeo, sin gráficos 3D, con la configuración del escritorio de Windows optimizada y Horizon 7 optimizado.
- Un ancho de banda medio de 400 a 600 Kbps para escritorios virtuales utilizando varios monitores, 3D, Aero y Microsoft Office.
- Un ancho de banda pico mínimo de 500 Kbps a 1 Mbps para dejar margen para ráfagas de cambios de visualización. En general, se debe dimensionar la red utilizando el ancho de banda, pero se debe tener en cuenta el pico de ancho de banda para admitir ráfagas de tráfico de imágenes asociado a cambios de pantalla grandes.
- 2 Mbps por usuario simultáneo que ejecute vídeo de 480p, según el límite de velocidad de fotogramas configurado y el tipo de vídeo.

Nota La estimación de 50 a 150 Kbps por usuario típico se basa en la suposición de que todos los usuarios operan de forma continua y realizan tareas similares a lo largo de una jornada de 8-10 horas. La cifra de uso de ancho de banda de 50 Kbps se obtuvo de las pruebas de View Planner en una LAN con la función de compilación sin pérdida deshabilitada. Pueden darse situaciones en las que algunos usuarios puedan estar casi inactivos y sin consumir apenas ancho de banda, lo que permite más usuarios por vínculo. Por tanto, estas directrices tienen como finalidad proporcionar un punto de inicio para realizar una planificación y pruebas de ancho de banda más detalladas.

El ejemplo siguiente muestra cómo calcular el número de usuarios simultáneos de una sucursal u oficina remota que tienen una línea T1 de 1,5 Mbps.

Escenario de sucursal u oficina remota

- Los usuarios tienen aplicaciones de productividad básicas de Microsoft Office, sin vídeo, sin gráficos 3D y con teclados USB y dispositivos de mouse.
- El ancho de banda requerido por usuario típico de oficina en Horizon 7 es entre 50 y 150 Kbps.
- La capacidad de la red T1 es 1,5 Mbps.
- La utilización de ancho de banda es el 80% (factor de utilización de 0,8).

Fórmula para determinar el número de usuarios admitidos

- En el peor de los casos, los usuarios requieren 150 Kbps: $(1,5 \text{ Mbps} * 0,8) / 150 \text{ Kbps} = (1500 * 0,8) / 150 = 8$ usuarios
- En el mejor de los casos, los usuarios requieren 50 Kbps: $(1,5 \text{ Mbps} * 0,8) / 50 \text{ Kbps} = (1500 * 0,8) / 50 = 24$ usuarios

Resultado

Esta oficina remota puede admitir entre 8 y 24 usuarios simultáneos por línea T1 con una capacidad de 1,5 Mbps.

Importante Es posible que para conseguir esta densidad de usuarios sea necesario optimizar tanto la configuración del escritorio Windows como Horizon 7.

Bloques de creación de Horizon 7

Un bloque de creación está formado por servidores físicos, una infraestructura de vSphere, servidores Horizon 7, almacenamiento compartido y escritorios de máquinas virtuales para usuarios finales. Un bloque de creación es una construcción lógica y su tamaño no debe ser superior al necesario para 2.000 escritorios de Horizon. Los clientes incluyen normalmente hasta cinco bloques de creación en un pod de Horizon 7, aunque en teoría se pueden usar más bloques, siempre que el pod no supere 10.000 sesiones ni 7 instancias del servidor de conexión de Horizon.

Tabla 4-11. Ejemplo de un bloque de creación de Horizon basado en LAN para 2.000 escritorios de máquinas virtuales

Elemento	Ejemplo
Clústeres de vSphere	1 o más
Conmutador de red de 80 puertos	1
Sistema de almacenamiento compartido	1
vCenter Server con View Composer en el mismo host	1 (se puede ejecutar en el propio bloque)

Tabla 4-11. Ejemplo de un bloque de creación de Horizon basado en LAN para 2.000 escritorios de máquinas virtuales (continuación)

Elemento	Ejemplo
Base de datos	Servidor de base de datos MS SQL Server u Oracle (se puede ejecutar en el propio bloque)
VLAN	3 (una red Ethernet de 1 Gb para cada una: red de administración, red de almacenamiento y red de VMotion)

Cada vCenter Server puede admitir hasta 10.000 máquinas virtuales. Esta capacidad permite tener bloques de creación que contengan más de 2.000 escritorios de máquinas virtuales. No obstante, el tamaño real del bloque de creación también está sujeto a otras limitaciones específicas de Horizon 7.

Si solo cuenta con un bloque de creación en un pod, use dos instancias del servidor de conexión para obtener redundancia.

Pods de Horizon 7

Un pod es una unidad de organización determinada por los límites de escalabilidad de Horizon 7.

Ejemplo de pod utilizando cinco bloques de creación

Un pod de Horizon 7 tradicional integra cinco bloques de creación de 2.000 usuarios que se pueden administrar como una sola entidad.

Tabla 4-12. Ejemplo de un pod de Horizon 7 basado en LAN construido con 5 bloques de creación.

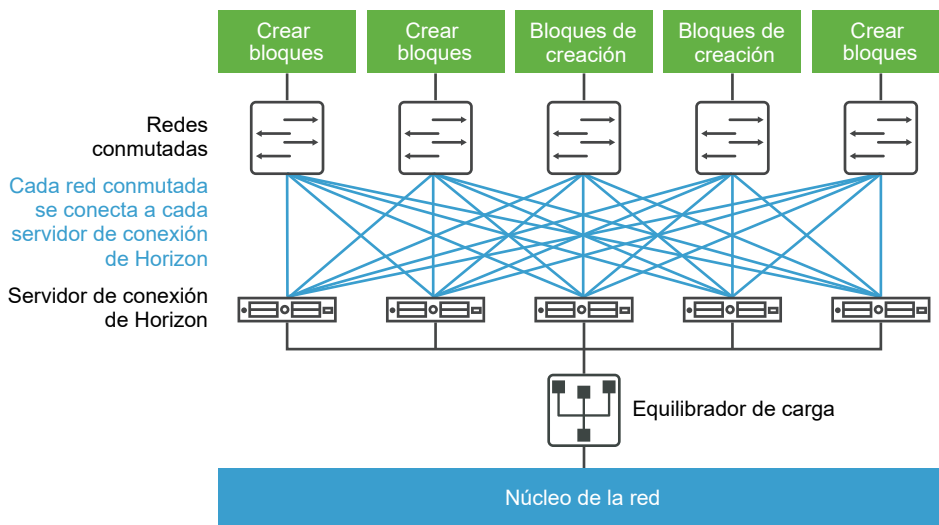
Elemento	Número
Bloques de creación para un pod de Horizon 7	5
vCenter Server y View Composer	5 (1 máquina virtual que aloje a ambos en cada bloque de creación)
Servidor de base de datos	5 servidores de base de datos MS SQL u Oracle (1 servidor de base de datos independiente en cada bloque de creación)
Servidores de conexión	7 (5 para conexiones desde dentro de la red corporativa y 2 para conexiones desde fuera)
VLAN	Consulte Tabla 4-11. Ejemplo de un bloque de creación de Horizon basado en LAN para 2.000 escritorios de máquinas virtuales.
Módulo Ethernet de 10 GB	1
Conmutador de red modular	1

Cada vCenter Server puede admitir hasta 35.000 máquinas virtuales registradas. Esta capacidad permite tener bloques de creación que contengan más de 2.000 escritorios de máquinas virtuales. No obstante, el tamaño real del bloque de creación también está sujeto a otras limitaciones específicas de Horizon 7.

En los dos ejemplos descritos, un núcleo de red puede equilibrar la carga de las solicitudes entrantes en las instancias del servidor de conexión. La compatibilidad con un mecanismo de redundancia y conmutación por error, normalmente en el nivel de red, puede evitar que el equilibrador de carga se convierta en un único punto de fallo. Por ejemplo, el protocolo Virtual Router Redundancy Protocol (VRRP) se puede comunicar con un equilibrador de carga para agregar capacidad de redundancia y conmutación por error.

Si se produce un error en una instancia del servidor de conexión o deja de responder durante una sesión activa, los usuarios no pierden datos. Los estados de los escritorios se conservan en el escritorio de la máquina virtual, de manera que los usuarios se pueden conectar a una instancia distinta del servidor de conexión y su sesión continúa desde el punto en que se produjo el fallo.

Figura 4-2. Diagrama de pods para 10.000 escritorios de máquinas virtuales



Ejemplo de pod utilizando un vCenter Server

En la sección anterior, el pod de Horizon 7 consistía en varios bloques de creación. Cada bloque admitía 2.000 máquinas virtuales con un único vCenter Server. VMware ha recibido numerosas peticiones, tanto de clientes como de partners, para usar un solo vCenter Server para administrar un pod de Horizon 7. Esta solicitud proviene del hecho de que una sola instancia de vCenter Server puede admitir 10.000 máquinas virtuales. Los clientes tienen la posibilidad de usar un solo vCenter Server para administrar un entorno de 10.000 escritorios. Este tema ilustra una arquitectura basada en el uso de un solo vCenter Server para administrar 10.000 escritorios.

Aunque es posible usar un vCenter Server y un View Composer para 10.000 escritorios, al hacerlo se crea una situación en la que existe un único punto de fallo. La pérdida de ese único vCenter Server hace que no esté disponible la totalidad de la implementación de escritorios para operaciones de encendido/apagado, aprovisionamiento y reajuste. Por esta razón, se debe elegir una arquitectura de implementación acorde a las necesidades generales de resiliencia de los componentes.

En este ejemplo, un pod de 10.000 usuarios está formado por servidores físicos, una infraestructura de vSphere, servidores Horizon 7, almacenamiento compartido y 5 clústeres de 2.000 escritorios virtuales por clúster.

Tabla 4-13. Ejemplo de un pod de Horizon 7 basado en LAN con un vCenter Server

Elemento	Ejemplo
Clústeres de vSphere	6 (5 clústeres con un grupo de clones vinculados por clúster y 1 clúster de infraestructura)
vCenter Server	1
View Composer	1 (independiente)
Servidor de base de datos	1 servidor de base de datos (independiente) MS SQL u Oracle
Servidor de Active Directory	1 o 2
Instancias del servidor de conexión	5
Servidores de seguridad	5
VLAN	8 (5 para los clústeres del grupo de escritorios, 1 para administración, 1 para VMotion y 1 para el clúster de infraestructura)

Descripción general de Arquitectura de Cloud Pod

Para utilizar un grupo de instancias replicadas del servidor de conexión a través de una WAN, una MAN (red de área metropolitana) u otras redes que no sean LAN, en escenarios en los que una implementación de Horizon debe abarcar centros de datos, debe utilizar la función Arquitectura de Cloud Pod.

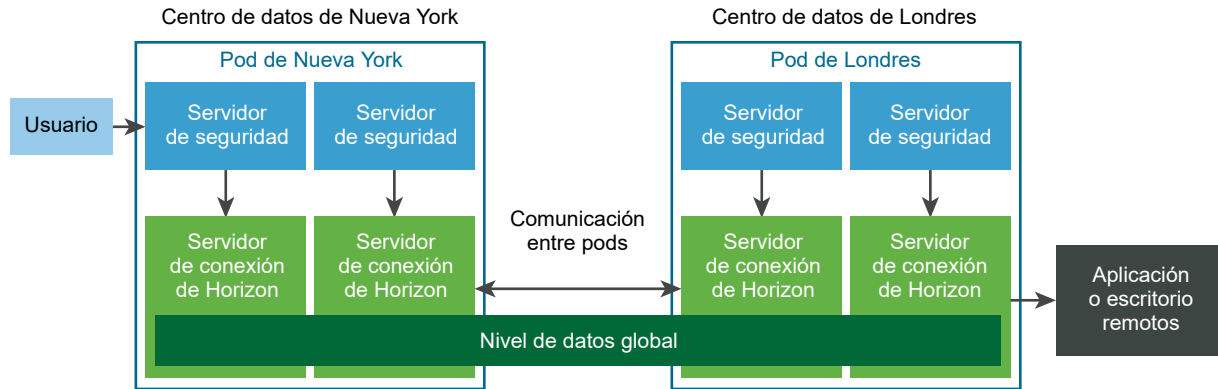
Esta función usa componentes estándar de Horizon para permitir la administración entre centros de datos, la asignación flexible y global de usuarios a escritorios, los escritorios de alta disponibilidad y la funcionalidad de recuperación ante desastres.

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

Tabla 4-14. Límites de la federación de pods

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

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



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

La función Arquitectura de Cloud Pod no se admite en un entorno IPv6.

Para obtener más información, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

Ventajas de utilizar varios servidores vCenter Server en un pod

Al crear un diseño para un entorno de producción de Horizon 7 con más de 500 escritorios, se deben considerar varias cuestiones para decidir si utilizar una instancia de vCenter Server en lugar de varias.

A partir de la versión 5.2 de View, VMware permite administrar hasta 10.000 máquinas virtuales de escritorio dentro de un solo pod de Horizon 7 con un único servidor vCenter versión 5.1 o posterior. Antes de intentar administrar 10.000 máquinas virtuales con una sola instancia de vCenter Server, tenga en cuenta los factores siguientes:

- Duración de los intervalos de mantenimiento en su empresa
- Capacidad de tolerar fallos de componentes de Horizon 7
- Frecuencia de las operaciones de encendido, aprovisionamiento y reajuste
- Simplicidad de la infraestructura

Duración de los intervalos de mantenimiento

La configuración de concurrencia de las operaciones de encendido, aprovisionamiento y mantenimiento de las máquinas virtuales se determinan por instancia de vCenter Server.

Diseños de pod con una instancia de vCenter Server	<p>La configuración de concurrencia determina el número de operaciones que se pueden poner en cola para un pod completo de Horizon 7 cada vez.</p> <p>Por ejemplo, si las operaciones de aprovisionamiento concurrentes se establecen en 20 y solo se tiene una instancia de vCenter Server en un pod, se realizarán en serie las operaciones de aprovisionamiento en grupos de más de 20 escritorios. Después de poner en cola 20 operaciones concurrentes simultáneamente, se debe completar una operación antes de que comience la siguiente. En implementaciones de Horizon 7 a gran escala, esta operación de aprovisionamiento puede tardar mucho tiempo.</p>
Diseños de pod con varias instancias de vCenter Server	Cada instancia puede aprovisionar 20 máquinas simultáneamente.

Para asegurar que se completen simultáneamente más operaciones dentro de un intervalo de mantenimiento, se pueden agregar varias instancias de vCenter Server (hasta cinco) al pod e implementar varios grupos de escritorios en clústeres de vSphere administrados por instancias de vCenter Server independientes. Un clúster de vSphere solo se puede administrar con una instancia de vCenter Server cada vez. Para conseguir concurrencia en todas las instancias de vCenter Server, se deben implementar los grupos de escritorios de la manera correspondiente.

Capacidad de tolerar fallos de componentes

La función de vCenter Server en los pods de Horizon 7 es proporcionar operaciones de encendido, aprovisionamiento y reajuste (actualización, recomposición y reequilibrado). Después de implementar y encender una máquina virtual, Horizon 7 no se basa en vCenter Server para el transcurso normal de las operaciones.

Como cada clúster de vSphere debe estar administrado por una sola instancia de vCenter Server, este servidor representa un solo punto de fallo en cada diseño de Horizon 7. El riesgo también es cierto para cada instancia de View Composer. (Hay una asignación de tipo uno a uno entre cada instancia de View Composer y de vCenter Server.) El uso de uno de los productos siguientes puede mitigar el impacto de una interrupción de vCenter Server o de View Composer:

- VMware vSphere High Availability (HA)
- Productos de conmutación por error compatibles de otros fabricantes

Importante Para utilizar una de estas estrategias de conmutación por error, la instancia de vCenter Server no se debe instalar en máquinas virtuales que formen parte del clúster que administra la instancia de vCenter Server.

Además de estas opciones automatizadas de conmutación por error de vCenter Server, se puede elegir también reconstruir el servidor fallido en una nueva máquina virtual o servidor físico. La mayor parte de la información clave se almacena en la base de datos de vCenter Server.

La tolerancia al riesgo es un factor importante para determinar si utilizar una o varias instancias de vCenter Server en el diseño del pod. Si las operaciones requieren capacidad para realizar tareas de administración de escritorios tales como el encendido y reajuste simultáneo de todos los escritorios, se debe repartir el impacto de una interrupción entre menos escritorios a la vez mediante la implementación

de varias instancias de vCenter Server. Si se puede tolerar que el entorno de escritorios no esté disponible durante un largo período de tiempo para realizar operaciones de administración o aprovisionamiento, o si se decide utilizar un proceso de reconstrucción manual, se puede implementar una sola instancia de vCenter Server para el pod.

Frecuencia de las operaciones de encendido, aprovisionamiento y reajuste

Algunas operaciones de encendido, aprovisionamiento y reajuste de máquinas virtuales de escritorios solo las pueden iniciar las acciones del administrador, son normalmente predecibles y controlables, y se pueden limitar a los intervalos de mantenimiento establecidos. Otras operaciones de encendido y reajuste de escritorios se activan mediante acciones del usuario, tales como la configuración de actualización al cerrar la sesión o la suspensión al cerrar la sesión, o bien mediante scripts de acciones, como el uso de la función Distributed Power Management (DPM) durante períodos de inactividad del usuario para apagar hosts ESXi inactivos.

Si el diseño de Horizon 7 no requiere operaciones de encendido y reajuste activadas por el usuario, probablemente una sola instancia de vCenter Server sea suficiente para sus necesidades. Si la frecuencia de las operaciones de encendido y reajuste activadas por el usuario no es elevada, no se puede acumular grandes colas de operaciones que puedan hacer que se agote el tiempo de espera del servidor de conexión de Horizon mientras vCenter Server completa las operaciones solicitadas dentro de los límites de concurrencia establecidos.

Muchos clientes eligen implementar grupos flotantes y utilizar la configuración de actualización al cerrar la sesión para proporcionar constantemente escritorios sin datos antiguos de sesiones anteriores. Un ejemplo de datos antiguos son las páginas de memoria no reclamadas en los archivos `pagefile.sys` o temporales de Windows. Los grupos flotantes también pueden minimizar el impacto del malware restableciendo con frecuencia los escritorios a un estado conocido.

Algunos clientes reducen el uso de electricidad configurando Horizon 7 para que apague los escritorios que no estén en uso, de manera que vSphere DRS (Distributed Resources Scheduler) pueda consolidar las máquinas virtuales en ejecución en un número mínimo de hosts ESXi. En estos casos, VMware Distributed Power Management apaga los hosts inactivos. En este tipo de casos, el uso de varias instancias de vCenter Server permite acomodar mejor la mayor frecuencia de operaciones de encendido y reajuste necesarias para evitar tiempos de espera de las operaciones.

Simplicidad de la infraestructura

Una sola instancia de vCenter Server en un diseño a gran escala de Horizon 7 ofrece algunas ventajas atractivas, tales como un único lugar para administrar imágenes maestras y máquinas virtuales principales, una única vista de vCenter Server que coincida con la vista de la consola de Horizon Administrator y menos servidores de bases de datos y bases de datos back-end de producción. La planificación de la recuperación ante desastres es más sencilla en el caso de una instancia de vCenter Server que en el caso de varias. Asegúrese de sopesar las ventajas de usar varias instancias de vCenter

Server, como la duración de los intervalos de mantenimiento y la frecuencia de las operaciones de encendido y reajuste, frente a las desventajas, como la carga administrativa adicional que supone administrar imágenes de máquinas virtuales principales y el mayor número de componentes de infraestructura requeridos.

El diseño se puede beneficiar de un enfoque híbrido. Se puede elegir tener grupos muy grandes y relativamente estáticos administrados por una instancia de vCenter Server y tener varios grupos de escritorio más pequeños y dinámicos administrados por varias instancias de vCenter Server. La mejor estrategia para actualizar pods a gran escala existentes es actualizar primero los componentes de software de VMware del pod existente. Antes de cambiar el diseño del pod, se debe evaluar el impacto de las mejoras de las operaciones de encendido, aprovisionamiento y reajuste de la versión más reciente y probar posteriormente a aumentar el tamaño de los grupos de escritorio hasta encontrar el equilibrio adecuado de grupos de escritorios mayores en un menor número de instancias de vCenter Server.

Planificar las funciones de seguridad

5

Horizon 7 ofrece una gran seguridad de red para proteger datos corporativos confidenciales. Para mayor seguridad, se puede integrar Horizon 7 con algunas soluciones de autenticación de usuarios, utilizar un servidor de seguridad e implementar la función de autorizaciones restringidas.

Importante Con Horizon 6 versión 6.2 y versiones posteriores, puede realizar operaciones criptográficas con algoritmos conformes la norma FIPS (Estándar federal de procesamiento de información) 140-2. Puede instalar Horizon 7 en modo FIPS para habilitar el uso de estos algoritmos. No todas las funciones se admiten en modo FIPS. Para obtener más información, consulte el documento *Instalación de Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Comprender el funcionamiento de las conexiones cliente](#)
- [Elegir un método de autenticación de usuarios](#)
- [Restringir el acceso a escritorios remotos](#)
- [Utilizar configuraciones de directivas de grupo para asegurar aplicaciones y escritorios remotos](#)
- [Usar Directivas de Smart](#)
- [Implementar procedimientos recomendados para proteger sistemas de cliente](#)
- [Asignar funciones de administrador](#)
- [Preparar el uso de un servidor de seguridad](#)
- [Comprender los protocolos de comunicaciones](#)

Comprender el funcionamiento de las conexiones cliente

Horizon Client y Horizon Administrator se comunican con un host del servidor de conexión de Horizon a través de conexiones HTTPS seguras. La información sobre el certificado del servidor en el servidor de conexión se comunica al cliente como parte del protocolo de enlace TLS entre el cliente y el servidor.

La conexión inicial de Horizon Client, que se utiliza para la autenticación del usuario y la selección de aplicaciones y escritorios remotos, se crea cuando un usuario abre Horizon Client y proporciona un nombre de dominio plenamente cualificado para el servidor de conexión, el servidor de seguridad o el host de Unified Access Gateway. La conexión de Horizon Administrator se crea cuando un administrador escribe la dirección URL de Horizon Administrator en un navegador web.

Durante la instalación del servidor de conexión, se genera un certificado de servidor TLS predeterminado. De forma predeterminada, este certificado se presenta a los clientes TLS cuando visitan una página segura como la de Horizon Administrator.

Se puede usar el certificado predeterminado para pruebas, pero se debería sustituir con uno propio lo antes posible. El certificado predeterminado no está firmado por una entidad de certificación (CA) comercial. El uso de certificados sin certificación puede permitir la interceptación del tráfico por terceros enmascarados como su servidor.

- **Conexiones de clientes mediante puertas de enlace seguras de Blast y PCoIP**

Cuando los clientes se conectan a una aplicación o un escritorio remotos con el protocolo de visualización PCoIP o Blast Extreme de VMware, Horizon Client puede establecer una segunda conexión al componente de puerta de enlace segura correspondiente de una instancia del servidor de conexión de Horizon, un servidor de seguridad o un dispositivo de Unified Access Gateway. Esta conexión proporciona el nivel de seguridad y conectividad requerido al acceder a aplicaciones y escritorios remotos desde Internet.

- **Conexiones de túnel de cliente con Microsoft RDP**

Cuando los usuarios se conectan a un escritorio remoto con el protocolo de visualización Microsoft RDP, Horizon Client puede realizar una segunda conexión HTTPS al host del servidor de conexión de Horizon. Esta conexión se llama conexión de túnel porque proporciona un túnel para transportar datos de RDP.

- **Conexiones directas del cliente**

Los administradores pueden configurar el servidor de conexión de Horizon de manera que las sesiones de aplicaciones publicadas y de escritorio remoto se establezcan directamente entre el sistema cliente y la máquina virtual de aplicaciones o escritorios publicados, sin pasar por el host del servidor de conexión. Este tipo de conexión se denomina conexión de cliente directa.

Conexiones de clientes mediante puertas de enlace seguras de Blast y PCoIP

Cuando los clientes se conectan a una aplicación o un escritorio remotos con el protocolo de visualización PCoIP o Blast Extreme de VMware, Horizon Client puede establecer una segunda conexión al componente de puerta de enlace segura correspondiente de una instancia del servidor de conexión de Horizon, un servidor de seguridad o un dispositivo de Unified Access Gateway. Esta conexión proporciona el nivel de seguridad y conectividad requerido al acceder a aplicaciones y escritorios remotos desde Internet.

Los servidores de seguridad y los dispositivos de Unified Access Gateway incluyen un componente de puerta de enlace segura PCoIP y un componente de puerta de enlace segura Blast, lo que ofrece las siguientes ventajas:

- El único tráfico de aplicaciones y escritorios remotos que puede entrar al centro de datos corporativo es el tráfico en nombre de un usuario perfectamente autenticado.
- Los usuarios solo pueden acceder a los recursos para los que tengan autorización.
- La conexión de puerta de enlace segura PCoIP admite PCoIP, y la conexión de puerta de enlace segura de Blast admite Blast Extreme. Ambos son protocolos de visualización remota avanzados que aumentan la eficiencia en el uso de la red mediante el encapsulamiento de paquetes de visualización de vídeo en UDP en lugar de TCP.
- PCoIP y Blast Extreme están asegurados de forma predeterminada mediante cifrado AES-128. No obstante, se puede cambiar el cifrado a AES-256.
- No se necesita ninguna VPN, siempre que el protocolo de visualización no sea bloqueado por ningún componente de red. Por ejemplo, alguien que intente acceder a su aplicación o escritorio remoto desde una habitación de hotel puede observar que el proxy que utiliza el hotel no está configurado para permitir el paso de paquetes UDP.

Si desea obtener más información, consulte [Reglas del firewall para servidores de seguridad basados en DMZ](#).

Los servidores de seguridad se ejecutan en sistemas operativos Windows Server 2008 R2 y Windows Server 2012 R2, y aprovechan todas las ventajas de la arquitectura de 64 bits. Este servidor de seguridad también puede aprovechar las ventajas de los procesadores Intel compatibles con las nuevas instrucciones AES (AESNI) para obtener un rendimiento altamente optimizado del cifrado y descifrado.

Para obtener más información sobre dispositivos virtuales de Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Conexiones de túnel de cliente con Microsoft RDP

Cuando los usuarios se conectan a un escritorio remoto con el protocolo de visualización Microsoft RDP, Horizon Client puede realizar una segunda conexión HTTPS al host del servidor de conexión de Horizon. Esta conexión se llama conexión de túnel porque proporciona un túnel para transportar datos de RDP.

La conexión de túnel ofrece las siguientes ventajas:

- Los datos de RDP se envían por el túnel mediante HTTPS y se cifran mediante SSL. La seguridad que proporciona este potente protocolo de seguridad es acorde a la proporcionada por otros sitios web seguros, como los que se utilizan para pagos con tarjeta de crédito y banca por Internet.
- Un cliente puede acceder a varios escritorios a través de una sola conexión HTTPS, lo que reduce el procesamiento general del protocolo.
- Como Horizon 7 administra la conexión HTTPS, la fiabilidad de los protocolos subyacentes aumenta significativamente. Si un usuario pierde temporalmente la conexión de red, la conexión HTTP se restablece cuando se restaure aquella y la conexión RDP continúa automáticamente sin necesidad de que el usuario vuelva a conectarse e iniciar la sesión.

En una implementación estándar de instancias del servidor de conexión de View, la conexión HTTPS segura termina en el servidor de conexión. En una implementación de zona DMZ, la conexión HTTPS segura termina en un servidor de seguridad o en un dispositivo de Unified Access Gateway. Para obtener información sobre las implementaciones en zonas DMZ y servidores de seguridad, consulte [Preparar el uso de un servidor de seguridad](#).

Los clientes que utilizan el protocolo de visualización PCoIP o Blast Extreme pueden usar la conexión de túnel para la aceleración del redireccionamiento de multimedia (MMR) y del redireccionamiento USB. Sin embargo, para todos los demás datos, PCoIP utiliza la puerta de enlace segura de PCoIP, mientras que Blast Extreme utiliza la puerta de enlace segura de Blast, bien sea en un servidor de seguridad o en un dispositivo de Unified Access Gateway. Si desea obtener más información, consulte [Conexiones de clientes mediante puertas de enlace seguras de Blast y PCoIP](#).

Para obtener más información sobre dispositivos virtuales de Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Conexiones directas del cliente

Los administradores pueden configurar el servidor de conexión de Horizon de manera que las sesiones de aplicaciones publicadas y de escritorio remoto se establezcan directamente entre el sistema cliente y la máquina virtual de aplicaciones o escritorios publicados, sin pasar por el host del servidor de conexión. Este tipo de conexión se denomina conexión de cliente directa.

En las conexiones directas de cliente, se sigue estableciendo una conexión HTTPS entre el cliente y el host del servidor de conexión para autenticar usuarios y seleccionar aplicaciones publicadas y escritorios remotos, pero no se utiliza la segunda conexión HTTPS (la conexión de túnel).

Las conexiones directas de PCoIP y Blast Extreme incluyen las siguientes funciones de seguridad integradas:

- Compatibilidad con cifrado Advanced Encryption Standard (AES), activado de forma predeterminada, e IP Security (IPsec)
- Compatibilidad con clientes VPN de otros proveedores

Para clientes que utilicen el protocolo de visualización Microsoft RDP, las conexiones directas del cliente solo son adecuadas si la implementación se realiza dentro de una red corporativa. En las conexiones directas del cliente, el tráfico RDP se envía sin cifrar a través de la conexión entre el cliente y la máquina virtual del escritorio.

Elegir un método de autenticación de usuarios

Horizon 7 utiliza la infraestructura existente de Active Directory de Microsoft para la administración y la autenticación de usuarios. Para mayor seguridad, se puede integrar Horizon 7 con soluciones de

autenticación de doble factor, como RSA SecurID y RADIUS, y soluciones de autenticación de tarjeta inteligente.

- **Autenticación de Active Directory**

Cada instancia del servidor de conexión de Horizon se une a un dominio de Active Directory y los usuarios se autentican en dicho dominio mediante Active Directory. Los usuarios también se autentican en aquellos dominios adicionales con los que exista un acuerdo de confianza.

- **Uso de la autenticación en dos fases**

Puede configurar una instancia del servidor de conexión de Horizon para que obligue a los usuarios a utilizar una autenticación RSA SecurID o RADIUS (Servicio de autenticación remota telefónica de usuario).

- **Autenticación con tarjeta inteligente**

Una tarjeta inteligente es una tarjeta de plástico pequeña que contiene un chip informático. Muchas agencias gubernamentales y grandes empresas utilizan tarjetas inteligentes para autenticar a los usuarios que acceden a sus redes informáticas. Un tipo de tarjeta inteligente que usa el Departamento de Defensa de los Estados Unidos se denomina Tarjeta de acceso común (CAC).

- **Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows**

Con Horizon Client para Windows, cuando los usuarios seleccionan **Iniciar sesión como usuario actual** en el menú **Opciones**, las credenciales que se proporcionaron al iniciar sesión en el sistema cliente se usan para autenticarse en la instancia del servidor de conexión de Horizon y en el escritorio remoto. No es necesaria otra autenticación del usuario.

Autenticación de Active Directory

Cada instancia del servidor de conexión de Horizon se une a un dominio de Active Directory y los usuarios se autentican en dicho dominio mediante Active Directory. Los usuarios también se autentican en aquellos dominios adicionales con los que exista un acuerdo de confianza.

Por ejemplo, si una instancia del servidor de conexión forma parte del dominio A y existe un acuerdo de confianza entre el dominio A y el dominio B, tanto los usuarios del dominio A como los del B se podrán conectar a dicha instancia con Horizon Client.

De forma similar, si existe un acuerdo de confianza entre el dominio A y un dominio MIT Kerberos en un entorno de dominios mixto, los usuarios del dominio kerberos podrán seleccionar el nombre de dicho dominio al conectarse a la instancia del servidor de conexión con Horizon Client.

Es posible colocar usuarios y grupos en los siguientes dominios de Active Directory:

- El dominio del servidor de conexión
- Un dominio diferente que tiene una relación de confianza bidireccional con el dominio del servidor de conexión.
- Un dominio en un bosque diferente al del dominio del servidor de conexión. Este último debe confiar de manera unidireccional y externa en él o debe existir una relación de confianza entre el dominio y un dominio kerberos.

- Un dominio en un bosque diferente al del dominio del servidor de conexión. Este último debe confiar de manera unidireccional en él o debe existir una relación de confianza transitiva bidireccional entre ambos.

El servidor de conexión determina los dominios a los que se puede acceder mediante relaciones de confianza transversales, comenzando por el dominio en el que reside el host. En un conjunto de dominios reducido y conectado correctamente, el servidor de conexión puede determinar rápidamente una lista completa de dominios, pero la duración de este proceso aumenta a medida que lo hace el número de dominios o que disminuye la conectividad entre ellos. La lista también puede incluir los dominios que prefiera no ofrecer a los usuarios cuando se inician la sesión en las aplicaciones y los escritorios remotos.

Los administradores pueden usar la interfaz de línea de comandos de `vdmadmin` para configurar los filtros de los dominios, lo que limita los dominios en los que la instancia del servidor de conexión busca y que muestra a los usuarios. Consulte el documento *Administración de Horizon 7* para obtener más información.

Los procedimientos operativos existentes de Active Directory también gestionan directivas como la restricción de horas en las que se permite el inicio de sesión y la configuración de la fecha de caducidad de las contraseñas.

Uso de la autenticación en dos fases

Puede configurar una instancia del servidor de conexión de Horizon para que obligue a los usuarios a utilizar una autenticación RSA SecurID o RADIUS (Servicio de autenticación remota telefónica de usuario).

- El soporte de RADIUS ofrece un amplio rango de opciones alternativas de autenticación basadas en un token de dos fases.
- Horizon 7 también proporciona una interfaz abierta de extensión estándar para permitir a los proveedores de soluciones de terceros integrar extensiones de autenticación avanzada en Horizon 7.

Como las soluciones de autenticación en dos fases, como RSA SecurID y RADIUS, funcionan con administradores de autenticación, que se encuentran instalados en servidores independientes, debe tener configurados esos servidores y que el host del servidor de conexión pueda acceder a ellos. Por ejemplo, si se utiliza RSA SecurID, el administrador de autenticación sería el Administrador de autenticación de RSA. Si se dispone de RADIUS, el administrador de autenticación sería un servidor de RADIUS.

Para utilizar la autenticación de dos factores, cada usuario debe tener un token, como un token RSA SecurID, que esté registrado con su administrador de autenticación. Un token de autenticación de dos factores es un producto de hardware o de software que genera un código de autenticación a intervalos fijos. Con frecuencia, la autenticación requiere conocer tanto un PIN como un código de autenticación.

Si tiene varias instancias del servidor de conexión, puede configurar una autenticación en dos fases en algunas instancias y un método de autenticación del usuario diferente en otras. Por ejemplo, puede configurar una autenticación en dos fases solo para los usuarios que acceden a las aplicaciones y los escritorios remotos desde fuera de la red corporativa y a través de Internet.

Horizon 7 se certifica a través del programa RSA SecurID Ready y admite el rango completo de características de SecurID, incluido el nuevo modo de PIN, el modo del siguiente código de token, RSA Authentication Manager y el equilibrio de carga.

Autenticación con tarjeta inteligente

Una tarjeta inteligente es una tarjeta de plástico pequeña que contiene un chip informático. Muchas agencias gubernamentales y grandes empresas utilizan tarjetas inteligentes para autenticar a los usuarios que acceden a sus redes informáticas. Un tipo de tarjeta inteligente que usa el Departamento de Defensa de los Estados Unidos se denomina Tarjeta de acceso común (CAC).

Los administradores pueden habilitar instancias individuales del servidor de conexión para la autenticación con tarjetas inteligentes. Para habilitar una instancia del servidor de conexión para usar la autenticación mediante tarjetas inteligentes, normalmente es necesario agregar el certificado raíz a un archivo de almacén de confianza y, a continuación, modificar la configuración del servidor de conexión.

Todas las conexiones de cliente, incluyendo las conexiones de clientes que utilicen autenticación con tarjeta inteligente, tienen habilitado TLS/SSL.

Para usar las tarjetas inteligentes, los equipos cliente deben tener un software intermedio y un lector de tarjetas inteligentes. Para instalar certificados en tarjetas inteligentes, debe configurar el equipo para que actúe como una estación de inscripción. Para obtener información sobre si un tipo concreto de Horizon Client admite tarjetas inteligentes, consulte la documentación de Horizon Client en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows

Con Horizon Client para Windows, cuando los usuarios seleccionan **Iniciar sesión como usuario actual** en el menú **Opciones**, las credenciales que se proporcionaron al iniciar sesión en el sistema cliente se usan para autenticarse en la instancia del servidor de conexión de Horizon y en el escritorio remoto. No es necesaria otra autenticación del usuario.

Para dar soporte a esta función, las credenciales del usuario se almacenan en la instancia del servidor de conexión y en el sistema cliente.

- En la instancia del servidor de conexión, las credenciales del usuario están cifradas y se almacenan en la sesión del usuario junto al nombre de usuario, dominio y el UPN opcional. Las credenciales se agregan cuando se produce una autenticación y se eliminan cuando el objeto de sesión se destruye. El objeto de sesión se elimina cuando el usuario cierra sesión, se acaba el tiempo de espera de la sesión o se produce un error en la autenticación. El objeto de sesión reside en la memoria volátil y no se almacena en LDAP de Horizon ni en el archivo de disco.

- En la instancia del servidor de conexión, habilite la opción **Aceptar inicio de sesión como usuario actual** para permitir que la instancia del servidor de conexión acepte las credenciales y la identidad del usuario que se envían cuando los usuarios seleccionan **Iniciar sesión como usuario actual** en el menú **Opciones** de Horizon Client.

Importante Debe comprender los riesgos de seguridad antes de habilitar esta opción. Consulte "Opciones del servidor relacionadas con la seguridad para la autenticación de usuarios" en el documento *Seguridad de Horizon 7*.

- En el sistema cliente, las credenciales del usuario se cifran y se almacenan en una tabla del paquete de autenticación, que es un componente de Horizon Client. Las credenciales se agregan a la tabla cuando el usuario inicia sesión y se eliminan de la tabla cuando cierra sesión. La tabla se encuentra en una memoria volátil.

Los administradores pueden usar la configuración de la directiva de grupo de Horizon Client para controlar la disponibilidad de la opción **Iniciar sesión como usuario actual** del menú **Opciones** y para especificar su valor predeterminado. Los administradores también pueden usar la directiva de grupo para especificar las instancias del servidor de conexión que aceptan la información de la credencial y de la identidad de usuario que se transmite cuando los usuarios seleccionan **Iniciar sesión como usuario actual** en Horizon Client.

Se habilita la función Desbloqueo recursivo después de que un usuario inicie sesión en el servidor de conexión con la función Iniciar sesión como usuario actual. La función Desbloqueo recursivo desbloquea todas las sesiones remotas después de que lo hiciera el equipo cliente. Los administradores pueden controlar la función Desbloqueo recursivo con la opción de directiva global **Desbloquear sesiones remotas cuando la máquina cliente está desbloqueada** de Horizon Client. Para obtener más información sobre la configuración de directiva global de Horizon Client, consulte la documentación de Horizon Client en la página web [Documentación de VMware Horizon Client](#).

La función Iniciar sesión como usuario actual tiene las siguientes limitaciones y requisitos:

- Cuando la autenticación con tarjeta inteligente se establece como Requerida en una instancia del servidor de conexión, se produce un error en la autenticación de los usuarios que seleccionaron **Iniciar sesión como usuario actual** cuando se conectan a la instancia del servidor de conexión. Estos usuarios se deben volver a autenticar con la tarjeta inteligente y el PIN cuando inicien sesión en el servidor de conexión.
- La hora del sistema en el que el cliente inicia sesión y la hora del host del servidor de conexión deben estar sincronizadas.
- Si las asignaciones de los derechos del usuario **Tener acceso a este equipo desde la red** se modifican en el sistema cliente, deben modificarse como se describe en el artículo 1025691 de la base de conocimientos de VMware.
- El equipo cliente debe poder comunicarse con el servidor Active Directory corporativo y no debe usar las credenciales almacenadas en caché para la autenticación. Por ejemplo, si los usuarios inician

sesión en los equipos cliente desde fuera de la red corporativa, las credenciales almacenadas en caché se utilizan para la autenticación. Si el usuario intenta conectarse a un servidor de seguridad o a una instancia del servidor de conexión sin establecer en primer lugar una conexión VPN, se le solicitan las credenciales y la función Iniciar sesión como usuario actual no funciona.

Restringir el acceso a escritorios remotos

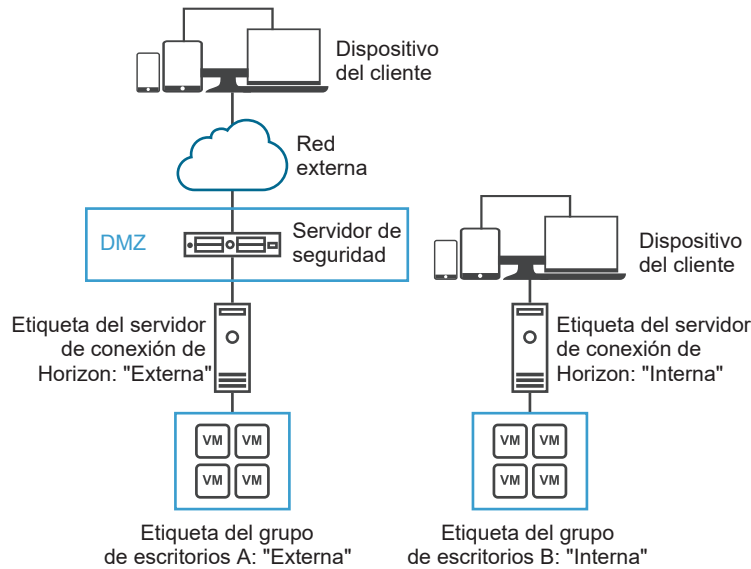
La función de autorizaciones restringidas se puede utilizar para restringir el acceso a escritorios remotos en función de la instancia del servidor de conexión de Horizon a la que se conecte el usuario.

Con las autorizaciones restringidas, asigne una o varias etiquetas a una instancia del servidor de conexión. A continuación, cuando configure un grupo de escritorios, seleccione las etiquetas de las instancias del servidor de conexión de Horizon que quiere que tengan acceso al grupo de escritorios. Cuando los usuarios inician sesión a través de una instancia del servidor de conexión, solo pueden acceder a los grupos de escritorios que tengan al menos una etiqueta que coincida o que no tengan ninguna etiqueta.

Por ejemplo, la implementación de Horizon 7 podría incluir dos instancias del servidor de conexión. La primera instancia es para los usuarios internos. La segunda se empareja con un servidor de seguridad y es para los usuarios externos. Para evitar que usuarios externos accedan a determinados escritorios, se podrían configurar autorizaciones restringidas, tal como se detalla a continuación:

- Asigne la etiqueta "Interno" a la instancia del servidor de conexión que admite usuarios internos.
- Asigne la etiqueta "Externo" a la instancia del servidor de conexión que está emparejada con el servidor de seguridad y que admite usuarios externos.
- Asigne la etiqueta "Interno" a los grupos de escritorios que solo deban estar accesibles para usuarios internos.
- Asigne la etiqueta "Externo" a los grupos de escritorios que solo deban estar accesibles para usuarios externos.

Los usuarios externos no pueden ver los grupos de escritorios etiquetados como Interno porque inician sesión a través de la instancia del servidor de conexión etiquetada como Externo, y los usuarios internos no pueden ver los grupos de escritorios etiquetados como Externo porque inician sesión a través de la instancia del servidor de conexión etiquetada como Interno. [Figura 5-1. Ejemplo de autorizaciones restringidas](#) ilustra esta configuración.

Figura 5-1. Ejemplo de autorizaciones restringidas

También puede usar autorizaciones restringidas para controlar el acceso a los escritorios según el método de autenticación de usuarios que se configure para una instancia específica del servidor de conexión. Por ejemplo, determinados grupos de escritorios pueden estar disponibles solo para usuarios que se autenticaran con una tarjeta inteligente.

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

Utilizar configuraciones de directivas de grupo para asegurar aplicaciones y escritorios remotos

Horizon 7 incluye plantillas administrativas de directivas de grupo (ADMX) que contienen configuraciones de directivas de grupo relacionadas con la seguridad que se pueden utilizar para asegurar aplicaciones y escritorios remotos.

Por ejemplo, se pueden utilizar configuraciones de directivas de grupo para realizar las siguientes tareas:

- Especificar las instancias del servidor de conexión que aceptarán la información de credenciales e identidad del usuario que se transmite cuando un usuario selecciona la casilla de verificación **Iniciar sesión como usuario actual** en Horizon Client para Windows.
- Habilitar single Sign-On para la autenticación con tarjetas inteligentes en Horizon Client.
- Configurar la comprobación del certificado TLS del servidor en Horizon Client.
- Impedir que los usuarios proporcionen información de credenciales con opciones de la línea de comandos de Horizon Client.

- Impedir que los sistemas que no sean Horizon Client utilicen RDP para conectar a escritorios remotos. Esta directiva se puede configurar de manera que las conexiones tengan que ser administradas por Horizon Client, lo que significa que los usuarios deberán usar Horizon 7 para conectar a escritorios remotos.

Consulte el documento *Configurar funciones de escritorios remotos en Horizon 7* para obtener información sobre cómo usar la configuración de directivas de grupo de Horizon Client y los escritorios remotos.

Usar Directivas de Smart

Puede utilizar Directivas de Smart para la configuración del entorno de usuario en una aplicación o un escritorio publicados, y también para la configuración del entorno de equipo que se aplica durante el arranque del equipo o la reconexión de la sesión.

Puede crear directivas para la configuración del entorno de usuario que controlan el comportamiento del redireccionamiento USB, la impresión virtual, el redireccionamiento del portapapeles, el redireccionamiento de unidades cliente, las funciones de transferencia de archivos Web y Chrome, y los perfiles de ancho de banda en un escritorio publicado o aplicación. Las directivas inteligentes de Horizon para la configuración del entorno de usuario se aplican durante el inicio de sesión y se pueden actualizar durante la reconexión de una sesión. Para volver a aplicar las directivas inteligentes de Horizon cuando un usuario vuelve a conectarse a una sesión, puede configurar una tarea activada.

Puede crear directivas para la configuración del entorno de equipos que Dynamic Environment Manager aplica mientras se inician los equipos de los usuarios finales. Estas directivas inteligentes de Horizon controlan el comportamiento del redireccionamiento multimedia Flash, la impresión integrada y el redireccionamiento USB. Las directivas inteligentes de Horizon para la configuración del entorno del equipo se aplican durante el arranque del equipo y se pueden actualizar durante la reconexión de una sesión.

Con Directivas de Smart, puede crear directivas que se apliquen únicamente si se cumplen ciertas condiciones. Por ejemplo, puede configurar una directiva que deshabilite la función del redireccionamiento de unidades cliente si un usuario se conecta a un escritorio remoto desde un lugar que no se encuentre dentro de la red corporativa.

Para usar la función Directivas de Smart es necesario Dynamic Environment Manager. Si desea obtener más información, consulte los temas sobre Directivas de Smart en *Configurar funciones de escritorios remotos en Horizon 7*.

Implementar procedimientos recomendados para proteger sistemas de cliente

Implemente estos procedimientos recomendados para proteger sistemas cliente.

- Asegúrese de que los sistemas de cliente estén configurados para entrar en suspensión tras un período de inactividad y que los usuarios deban introducir una contraseña para que el equipo se reactive.

- Exija a los usuarios que escriban un nombre de usuario y una contraseña al iniciar sistemas de cliente. No configure los sistemas de cliente de modo que permitan inicios de sesión automáticos.
- Para los sistemas de cliente Mac, considere establecer otras contraseñas para la cuenta de usuario y el llavero. Si las contraseñas son distintas, se pregunta a los usuarios antes de que el sistema introduzca en su nombre una contraseña. Asimismo, debería considerar el activar la protección FileVault.

Si desea consultar documentación concisa sobre todas las funciones de seguridad que proporciona Horizon 7, consulte el documento *Seguridad de Horizon 7*.

Asignar funciones de administrador

Una tarea de administración clave en un entorno de Horizon 7 es determinar quién puede usar Horizon Administrator y las tareas que esos usuarios pueden realizar.

La autorización para realizar tareas en Horizon Administrator se rige por un sistema de control de acceso que consta de privilegios y funciones de administrador. Una función es un conjunto de privilegios. Los privilegios otorgan la capacidad de realizar acciones específicas, como proporcionar autorización a un usuario para utilizar un grupo de escritorios o cambiar una configuración. Los privilegios también controlan qué puede ver un administrador en Horizon Administrator.

Un administrador puede crear carpetas para subdividir grupos de escritorios y delegar la administración de grupos de escritorios específicos a distintos administradores en Horizon Administrator. Un administrador configura el acceso a los recursos de una carpeta mediante la asignación de una función a un usuario en esa carpeta. Los administradores solo pueden acceder a los recursos que se encuentran en las carpetas para las que tienen funciones asignadas. La función que tiene un administrador en una carpeta determina el nivel de acceso que tiene ese administrador a los recursos de dicha carpeta.

Horizon Administrator incluye un conjunto de funciones predefinidas. Los administradores también pueden crear funciones personalizadas mediante la combinación de privilegios seleccionados.

Preparar el uso de un servidor de seguridad

Un servidor de seguridad es una instancia especial del servidor de conexión de Horizon que ejecuta un subconjunto de funciones del servidor de conexión. Se puede utilizar un servidor de seguridad para proporcionar una capa de seguridad adicional entre Internet y la red interna.

Importante Con Horizon 6 versión 6.2 y versiones posteriores, puede usar los dispositivos de Unified Access Gateway en lugar de servidores de seguridad. Los dispositivos de Unified Access Gateway se implementan como dispositivos virtuales endurecidos, que se basan en un dispositivo Linux personalizado para proporcionar acceso seguro. Para obtener más información sobre dispositivos virtuales de Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Un servidor de seguridad reside dentro de una zona DMZ y actúa como host proxy para las conexiones dentro de la red de confianza. Cada servidor de seguridad se empareja con una instancia del servidor de conexión y dirige todo el tráfico a esa instancia. Se pueden emparejar varios servidores con un único servidor de conexión. Este diseño proporciona una capa de seguridad adicional, protegiendo la instancia del servidor de conexión de la parte pública de Internet y forzando todas las solicitudes de sesión sin proteger a través del servidor de seguridad.

Para una implementación de servidor de seguridad basada en una zona DMZ, es necesario abrir varios puertos en el firewall para permitir que los clientes se conecten a los servidores de seguridad dentro de la zona DMZ. También se deben configurar puertos para la comunicación entre los servidores de seguridad y las instancias del servidor de conexión de la red interna. Para obtener información sobre puertos específicos, consulte [Reglas del firewall para servidores de seguridad basados en DMZ](#).

Como los usuarios se pueden conectar directamente con cualquier instancia del servidor de conexión desde su red interna, en una implementación basada en LAN no es necesario implementar un servidor de seguridad.

Nota Los servidores de seguridad incluyen los componentes de las puertas de enlaces seguros de PCoIP y Blast para que los clientes que usen estos protocolos de visualización puedan usar un servidor de seguridad en lugar de una VPN.

Para obtener más información sobre la configuración de VPN para usar PCoIP, consulte la información general de la solución VPN, disponible en la sección de recursos de partners de tecnología del centro de recursos técnicos, disponible en <http://www.vmware.com/products/view/resources.html>.

Prácticas recomendadas para las implementaciones de servidores de seguridad

Al utilizar un servidor de seguridad de una DMZ, se deben seguir las prácticas recomendadas de directivas de seguridad.

El documento técnico de *Virtualización de DMZ con VMware Infrastructure* incluye ejemplos de las prácticas recomendadas para DMZ virtualizados. Muchas de las recomendaciones de este documento técnico se aplican también a DMZ físicos.

Para limitar el ámbito de las transmisiones de fotogramas, las instancias del servidor de conexión de Horizon emparejadas con servidores de seguridad se deben implementar en una red aislada. Esta topología puede ayudar a evitar que usuarios maliciosos de la red interna supervisen las comunicaciones entre los servidores de seguridad y las instancias del servidor de conexión.

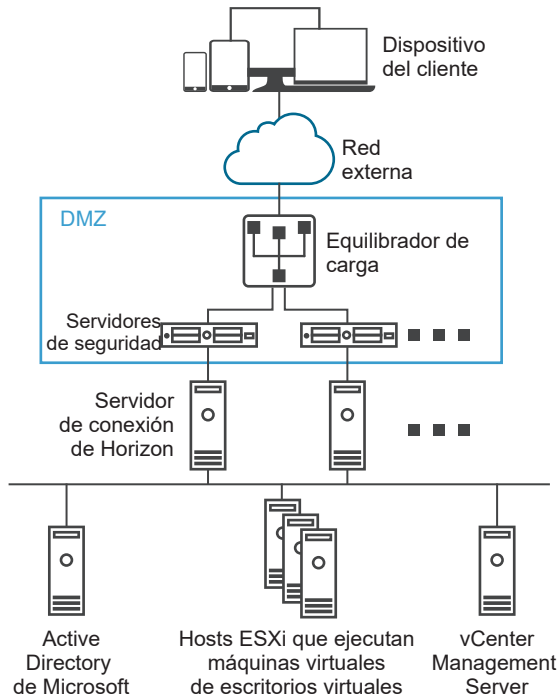
También es posible utilizar funciones de seguridad avanzadas del conmutador de red para evitar la supervisión maliciosa de las comunicaciones del servidor de seguridad y el servidor de conexión y protegerse de ataques de supervisión como el envenenamiento de caché ARP. Para obtener más información, consulte la documentación de su equipo de red.

Topologías de servidores de seguridad

Se pueden implementar diversas topologías de servidores de seguridad diferentes.

La topología ilustrada en [Figura 5-2. Servidores con equilibrio de carga en una zona DMZ](#) muestra un entorno de alta disponibilidad que incluye dos servidores de seguridad con equilibrio de carga en una zona DMZ. Los servidores de seguridad se comunican con las instancias del servidor de conexión de Horizon dentro de la red interna.

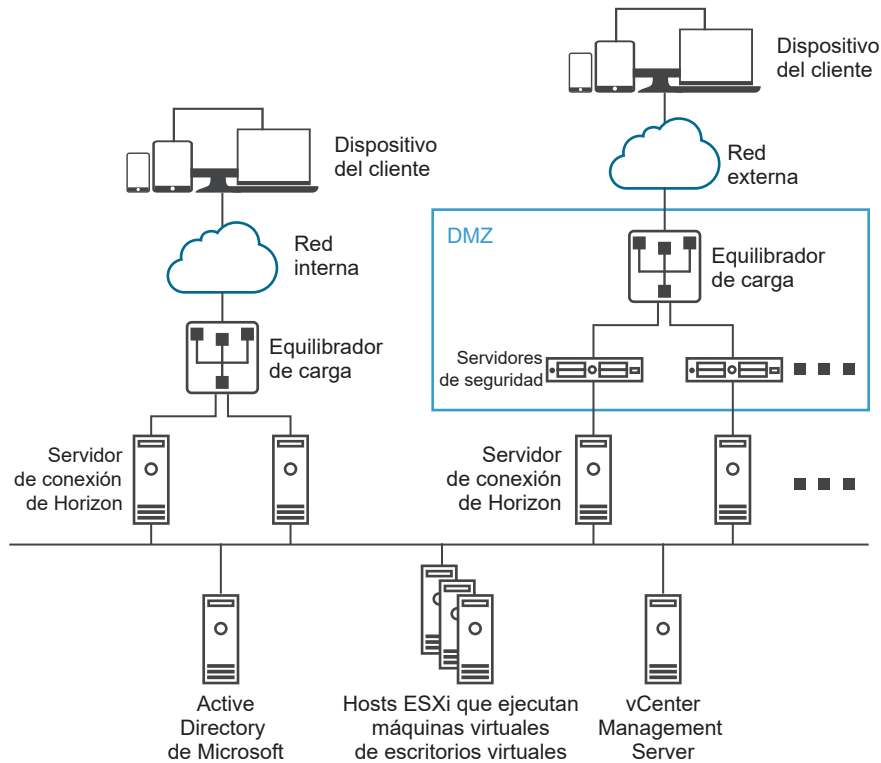
Figura 5-2. Servidores con equilibrio de carga en una zona DMZ



Cuando los usuarios fuera de la red corporativa se conectan a un servidor de seguridad, se deben autenticar correctamente antes de poder acceder a aplicaciones y escritorios remotos. Con reglas de firewall adecuadas en ambos lados de la zona DMZ, esta topología es adecuada para acceder a aplicaciones y escritorios remotos desde dispositivos cliente ubicados en Internet.

Es posible conectar varios servidores de seguridad a cada instancia del servidor de conexión. También se puede combinar una implementación de DMZ con una implementación estándar para ofrecer acceso a usuarios internos y externos.

La topología ilustrada en [Figura 5-3. Varios servidores de seguridad](#) muestra un entorno en el que cuatro instancias del servidor de conexión de View actúan como un grupo. Las instancias de la red interna están dedicadas a los usuarios de la red interna, y las instancias de la red externa a usuarios de la red externa. Si las instancias del servidor de conexión emparejadas con los servidores de seguridad tienen habilitada la autenticación RSA SecurID, todos los usuarios de la red externa se deberán autenticar mediante token de RSA SecurID.

Figura 5-3. Varios servidores de seguridad

Si se instala más de un servidor de seguridad, se debe implementar una solución de equilibrado de carga de hardware o de software. El servidor de conexión no proporciona una función de equilibrado de carga propia. El servidor de conexión funciona con soluciones de equilibrado de carga estándar de otros proveedores.

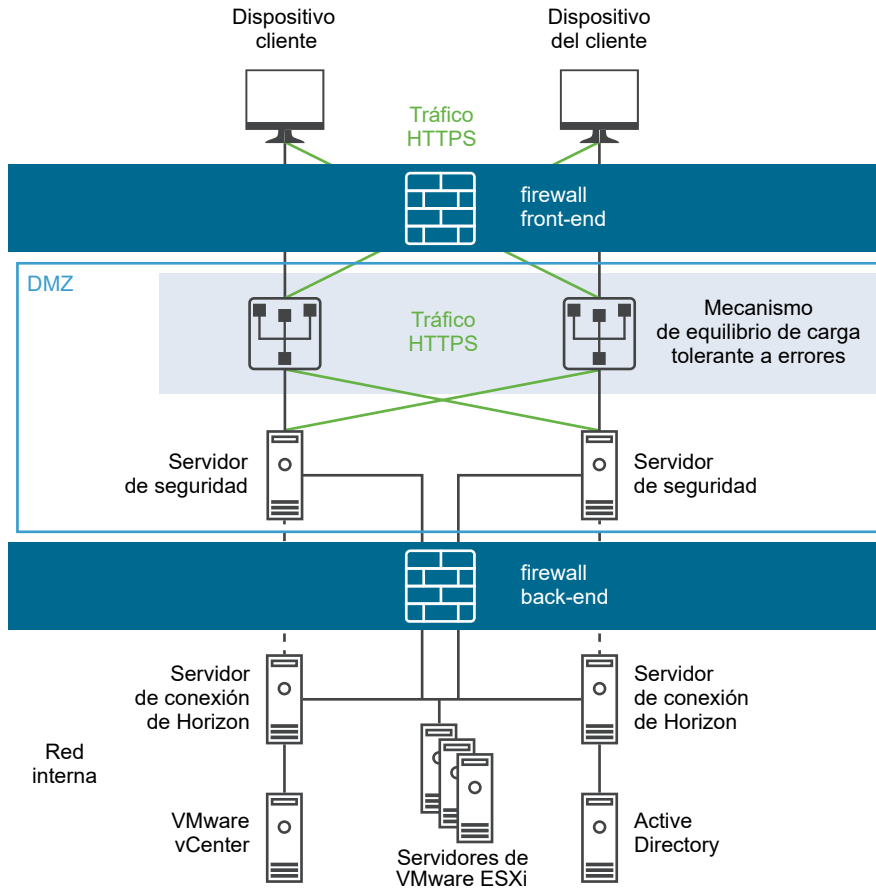
Firewall para servidores de seguridad basados en zonas DMZ

Una implementación de servidor de seguridad basada en una zona DMZ debe incluir dos firewall.

- Se necesita un firewall de front-end dirigido a la red externa, que protege tanto la DMZ como la red interna. Este firewall se configura para permitir que el tráfico de la red externa llegue a la DMZ.
- Se necesita un firewall de back-end entre la DMZ y la red interna, que proporciona un segundo nivel de seguridad. Este firewall se configura para aceptar solo el tráfico que se origina desde los servicios dentro de la DMZ.

La directiva del firewall controla estrictamente las comunicaciones entrantes de los servicios de la DMZ, lo que reduce en gran medida los riesgos para la red interna. Para obtener más información sobre los puertos necesarios para configurar los servidores de seguridad, consulte el documento *Seguridad de Horizon 7*.

La figura siguiente muestra un ejemplo de configuración que incluye firewall de front-end y de back-end.

Figura 5-4. Topología de doble firewall

Reglas del firewall para servidores de seguridad basados en DMZ

Los servidores de seguridad basados en DMZ requieren la configuración de ciertas reglas en los firewall de front-end y back-end. Durante la instalación, de forma predeterminada se configuran los servicios de Horizon 7 para la escucha en determinados puertos de la red. Si fuese necesario para cumplir las directivas de la organización o para evitar la contención, se pueden cambiar los números de puerto que se utilizan.

Importante Para obtener más detalles y recomendaciones de seguridad, consulte el documento *Horizon 7 Seguridad*.

Reglas del firewall de front-end

Para permitir que los dispositivos de clientes externos se conecten a un servidor de seguridad dentro de la zona DMZ, el firewall de front-end debe permitir el tráfico en determinados puertos TCP y UDP. [Tabla 5-1. Reglas del firewall de front-end](#) resume las reglas del firewall de front-end.

Tabla 5-1. Reglas del firewall de front-end

Origen	Puerto predeterminado	Protocolo	Destino	Puerto predeterminado	Notas
Horizon Client	TCP cualquiera	HTTP	Servidor de seguridad	TCP 80	(Opcional) Los dispositivos cliente externos conectados a un servidor de seguridad dentro de la zona DMZ en el puerto TCP 80 se dirigen automáticamente a HTTPS. Para obtener información sobre cuestiones de seguridad relativas a permitir a los usuarios conectar con HTTP en lugar de HTTPS, consulte la guía <i>Horizon 7 Seguridad</i> .
Horizon Client	TCP cualquiera	HTTPS	Servidor de seguridad	TCP 443	Los dispositivos cliente externos se conectan a un servidor de seguridad dentro de la zona DMZ en el puerto TCP 443 para comunicarse con una instancia del servidor de conexión y con aplicaciones y escritorios remotos.
Horizon Client	TCP cualquiera UDP cualquiera	PCoIP	Servidor de seguridad	TCP 4172 UDP 4172	Los dispositivos de clientes externos se conectan a un servidor de seguridad dentro de la zona DMZ en el puerto TCP 4172 y el puerto UDP 4172 para comunicarse con una aplicación o escritorio remoto mediante PCoIP.
Servidor de seguridad	UDP 4172	PCoIP	Horizon Client	UDP cualquiera	Los servidores de seguridad devuelven los datos de PCoIP a un dispositivo cliente externo desde el puerto UDP 4172. El puerto UDP de destino es el puerto de origen de los paquetes UDP recibidos. Como estos paquetes contienen datos de respuesta, no suele ser necesario agregar una regla de firewall específica para este tráfico.
Horizon Client o un navegador web del cliente	TCP cualquiera	HTTPS	Servidor de seguridad	TCP 8443 UDP 8443	Los dispositivos cliente externos y los clientes web externos (HTML Access) se conectan a un servidor de seguridad dentro de la zona DMZ en el puerto HTTPS 8443 para comunicarse con escritorios remotos.

Reglas del firewall de back-end

Para permitir que un servidor de seguridad se conecte con cada una de las instancias del servidor de conexión de View que residan en la red interna, el firewall de back-end debe permitir el tráfico entrante en determinados puertos TCP. Detrás del firewall back-end, los firewall internos se deben configurar de manera similar para permitir que las instancias del servidor de conexión y las aplicaciones y los escritorios remotos se comuniquen entre sí. [Tabla 5-2. Reglas del firewall de back-end](#) resume las reglas del firewall de back-end.

Tabla 5-2. Reglas del firewall de back-end

Origen	Puerto predeterminado	Protocolo	Destino	Puerto predeterminado	Notas
Servidor de seguridad	UDP 500	IPsec	Servidor de conexión	UDP 500	Los servidores de seguridad negocian la seguridad IPsec con las instancias del servidor de conexión en el puerto UDP 500.
Servidor de conexión	UDP 500	IPsec	Servidor de seguridad	UDP 500	Las instancias del servidor de conexión responden a los servidores de seguridad en el puerto UDP 500.
Servidor de seguridad	UDP 4500	NAT-T ISAKMP	Servidor de conexión	UDP 4500	Es obligatorio si se utiliza NAT entre un servidor de seguridad y su instancia del servidor de conexión emparejada. Los servidores de seguridad usan el puerto UDP 4500 para las NAT transversales y para negociar la seguridad IPsec.
Servidor de conexión	UDP 4500	NAT-T ISAKMP	Servidor de seguridad	UDP 4500	Si se utiliza NAT, las instancias del servidor de conexión responden a los servidores de seguridad en el puerto UDP 4500.
Servidor de seguridad	TCP cualquiera	AJP13	Servidor de conexión	TCP 8009	Los servidores de seguridad se conectan a las instancias del servidor de conexión del puerto TCP 8009 para redirigir el tráfico web de los dispositivos cliente externos. Si se habilita IPsec, el tráfico AJP13 no utiliza el puerto TCP 8009 después del emparejamiento. En lugar de ello, utiliza NAT-T (puerto UDP 4500) o ESP.
Servidor de seguridad	TCP cualquiera	JMS	Servidor de conexión	TCP 4001	Los servidores de seguridad se conectan a las instancias del servidor de conexión en el puerto TCP 4001 para intercambiar el tráfico de Java Message Service (JMS).
Servidor de seguridad	TCP cualquiera	JMS	Servidor de conexión	TCP 4002	Los servidores de seguridad se conectan a las instancias del servidor de conexión en el puerto TCP 4002 para intercambiar el tráfico seguro de Java Message Service (JMS).
Servidor de seguridad	TCP cualquiera	RDP	Escritorio remoto	TCP 3389	Los servidores de seguridad se conectan a escritorios remotos en el puerto TCP 3389 para intercambiar tráfico RDP.
Servidor de seguridad	TCP cualquiera	MMR	Escritorio remoto	TCP 9427	Los servidores de seguridad se conectan a escritorios remotos en el puerto TCP 9427 para recibir el tráfico relacionado con el redireccionamiento de multimedia (MMR) y el redireccionamiento de unidades cliente.
Servidor de seguridad	TCP cualquiera UDP 55000	PCoIP	Aplicación o escritorio remoto	TCP 4172 UDP 4172	Los servidores de seguridad se conectan a aplicaciones y escritorios remotos en el puerto TCP 4172 y el puerto UDP 4172 para intercambiar tráfico PCoIP.

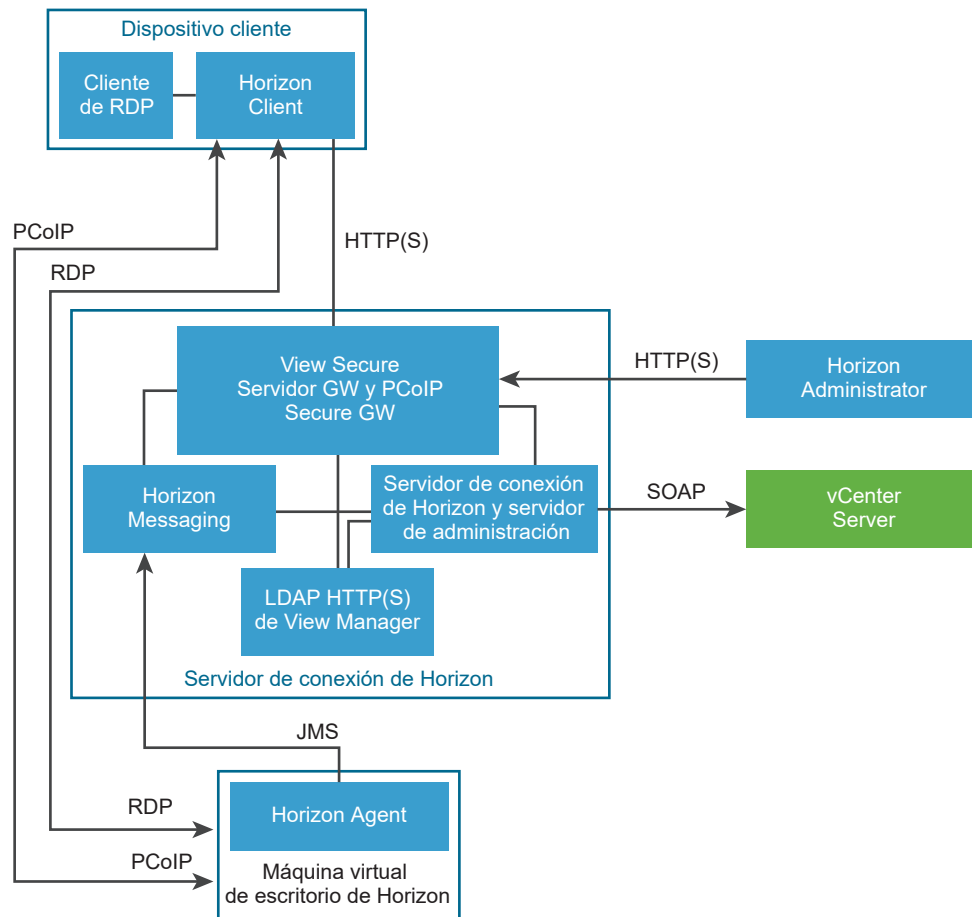
Tabla 5-2. Reglas del firewall de back-end (continuación)

Origen	Puerto predeterminado	Protocolo	Destino	Puerto predeterminado	Notas
Aplicación o escritorio remoto	UDP 4172	PCoIP	Servidor de seguridad	UDP 55000	Las aplicaciones y escritorios remotos devuelven datos PCoIP a los servidores de seguridad desde el puerto UDP 4172. El puerto UDP de destino será el puerto de origen de los paquetes UDP recibidos y, como se trata de datos de respuesta, no suele ser necesario agregar ninguna regla de firewall específica para ello.
Servidor de seguridad	TCP cualquiera	USB-R	Escritorio remoto	TCP 32111	Los servidores de seguridad se conectan a escritorios remotos en el puerto TCP 32111 para intercambiar tráfico de redireccionamiento entre dispositivos cliente externos y el escritorio remoto.
Servidor de seguridad	TCP o UDP cualquiera	Blast Extreme	Aplicación o escritorio remoto	TCP o UDP 22443	Los servidores de seguridad se conectan a aplicaciones y escritorios remotos en los puertos TCP y UDP 22443 para intercambiar tráfico de Blast Extreme.
Servidor de seguridad	TCP cualquiera	HTTPS	Escritorio remoto	TCP 22443	Si se utiliza HTML Access, los servidores de seguridad se conectan a escritorios remotos en el puerto HTTPS 22443 para comunicarse con el agente de Blast Extreme.
Servidor de seguridad		ESP	Servidor de conexión		Tráfico AJP13 encapsulado cuando no se requiere circulación NAT. ESP es el protocolo IP 50. No se especifican los números de puerto.
Servidor de conexión		ESP	Servidor de seguridad		Tráfico AJP13 encapsulado cuando no se requiere circulación NAT. ESP es el protocolo IP 50. No se especifican los números de puerto.

Comprender los protocolos de comunicaciones

Los componentes de Horizon 6 y Horizon 7 se envían mensajes usando diferentes protocolos.

[Figura 5-5. Protocolos y componentes de Horizon 6 y Horizon 7 sin servidores de seguridad](#) ilustra los protocolos que utiliza cada componente para la comunicación cuando no se ha configurado un servidor de seguridad. Es decir, que no están habilitados el túnel seguro para RDP, la puerta de enlace segura de Blast ni la puerta de enlace segura de PCoIP. Esta configuración puede utilizarse en una implementación LAN típica.

Figura 5-5. Protocolos y componentes de Horizon 6 y Horizon 7 sin servidores de seguridad

Nota Esta figura muestra las conexiones directas de clientes que utilizan PCoIP o RDP. El valor predeterminado, no obstante, es tener conexiones directas para PCoIP y conexiones de túnel para RDP.

Consulte [Tabla 5-3. Puertos predeterminados](#) para ver los puertos predeterminados que se utilizan para cada protocolo.

Figura 5-6. Protocolos y componentes de Horizon 6 y Horizon 7 con un servidor de seguridad ilustra los protocolos que utiliza cada componente para la comunicación cuando se ha configurado un servidor de seguridad. Esta configuración puede utilizarse en una implementación de red WAN típica.

Figura 5-6. Protocolos y componentes de Horizon 6 y Horizon 7 con un servidor de seguridad

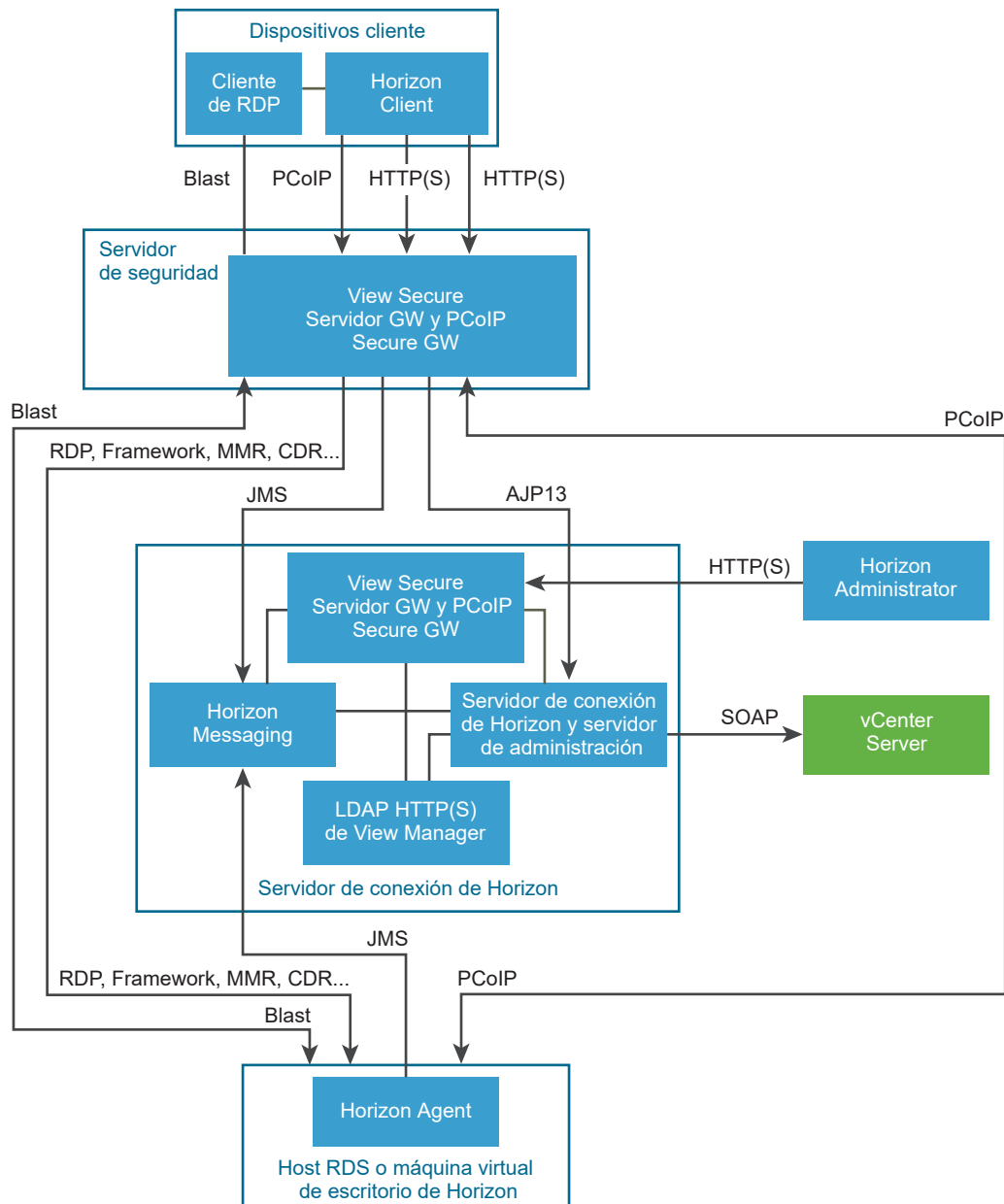


Tabla 5-3. Puertos predeterminados enumera los puertos predeterminados que se utilizan para cada protocolo. Si fuese necesario para cumplir las directivas de la organización o para evitar la contención, puede cambiar los números de puerto que se utilizan.

Tabla 5-3. Puertos predeterminados

Protocolo	Puerto
JMS	Puerto TCP 4001 Puerto TCP 4002
AJP13	Puerto TCP 8009 Nota AJP13 solo se utiliza en una configuración de servidor de seguridad.
HTTP	Puerto TCP 80
HTTPS	Puerto TCP 443
MMR/CDR	Para el redireccionamiento multimedia y de la unidad cliente, se utiliza el puerto TCP 9427.
RDP	Puerto TCP 3389 Nota Si la instancia del servidor de conexión se configura para las conexiones directas de cliente, estos protocolos se conectan directamente desde el cliente al escritorio remoto y no se hacen pasar por un túnel a través del componente del servidor de puerta de enlace segura de View.
SOAP	Puerto TCP 80 o 443
PCoIP	Puerto TCP 4172 Puertos UDP 4172, 50002, 55000
Redireccionamiento USB	Puerto TCP 32111. Este puerto también se utiliza para la sincronización de la zona horaria.
VMware Blast Extreme	Puerto TCP 8443, 22443 Puertos UDP 443, 8443, 22443
HTML Access	Puerto TCP 8443, 22443

Puertos TCP para la intercomunicación del servidor de conexión

Las instancias del servidor de conexión de un grupo utilizan puertos TCP adicionales para comunicarse entre sí. Por ejemplo, las instancias del servidor de conexión utilizan el puerto 4100 o 4101 para transmitir el tráfico entre enrutadores JMS (JMSIR) de una instancia a otra. Por lo general, no se utilizan firewalls entre las instancias del servidor de conexión de un grupo.

Servidor de puerta de enlace segura de View

El servidor de puerta de enlace segura de View es el componente del lado del servidor de la conexión HTTPS segura entre los sistemas cliente y un servidor de seguridad, un dispositivo Unified Access Gateway o una instancia del servidor de conexión.

Al configurar la conexión de túnel para el servidor de conexión, RDP, USB y redireccionamiento multimedia (MMR), el tráfico pasa por el túnel del componente puerta de enlace segura de View. Al configurar conexiones de cliente directas, estos protocolos conectan directamente desde el cliente al escritorio remoto y no pasan por el túnel del componente del servidor de puerta de enlace segura de View.

Nota Los clientes que utilizan el protocolo de visualización PCoIP o Blast Extreme pueden usar la conexión de túnel para la aceleración del redireccionamiento de multimedia (MMR) y del redireccionamiento USB. Sin embargo, para todos los demás datos, PCoIP utiliza la puerta de enlace segura de PCoIP, mientras que Blast Extreme utiliza la puerta de enlace segura de Blast, bien sea en un servidor de seguridad o en un dispositivo de Unified Access Gateway.

El servidor de puerta de enlace segura de View también es responsable de redirigir otro tráfico web, incluyendo el tráfico de autenticación de usuarios y selección de aplicaciones y escritorios, de los clientes al servidor de conexión. El servidor de puerta de enlace segura de Horizon también pasa el tráfico web del cliente de Horizon Administrator al componente servidor de administración.

Puerta de enlace segura de Blast

Los servidores de seguridad y los dispositivos de Unified Access Gateway incluyen un componente de puerta de enlace segura de Blast. Si la puerta de enlace segura de Blast está habilitada, después de la autenticación, los clientes que utilicen Blast Extreme o HTML Access pueden efectuar otra conexión segura a un servidor de seguridad o a un dispositivo de Unified Access Gateway. Esta conexión permite que los clientes accedan a aplicaciones y escritorios remotos desde Internet.

Al habilitar el componente de puerta de enlace segura de Blast, el tráfico de Blast Extreme se redirige mediante un servidor de seguridad o un dispositivo de Unified Access Gateway a las aplicaciones y escritorios remotos. Si los clientes que usan Blast Extreme utilizan también la función de redireccionamiento USB o la aceleración de redireccionamiento multimedia (MMR), se puede habilitar el componente de puerta de enlace segura de View para redirigir esos datos.

Al configurar conexiones de clientes directas, el tráfico de Blast Extreme y de otro tipo va directamente desde un cliente a una aplicación o un escritorio remoto.

Cuando usuarios finales, como personas que trabajan desde su hogar o usuarios móviles, acceden a los escritorios desde Internet, los servidores de seguridad o los dispositivos de Unified Access Gateway proporcionan el nivel necesario de seguridad y conectividad, de forma que no es necesaria una conexión VPN. El componente de puerta de enlace segura de Blast asegura que el único tráfico remoto que puede acceder al centro de datos corporativo es el tráfico en nombre de un usuario perfectamente autenticado. Los usuarios finales solo pueden acceder a los recursos para los que tengan autorización.

Un cliente nativo Blast que funciona a través de una puerta de enlace segura de Blast espera que el certificado TLS que está configurado en la puerta de enlace segura de Blast autentique la conexión TLS de la sesión Blast. Si la conexión Blast del cliente detecta otro certificado TLS, la conexión se descartará y el cliente notificará que una huella digital del certificado no coincide.

Si decide que el cliente establezca su conexión a un proxy con terminación TLS que se encuentre entre el cliente y la puerta de enlace segura de Blast, usted debe cumplir los requisitos del certificado del cliente y evitar que se produzca un error de falta de coincidencia de huellas digitales. Para ello, hará que el proxy presente una copia del certificado de la puerta de enlace segura de Blast (y la clave privada). De esta manera, se permite que se establezca correctamente la conexión Blast desde el cliente.

Como alternativa a copiar el certificado de la puerta de enlace segura de Blast al proxy, puede proporcionar a este último su propio certificado TLS y, a continuación, configurar la puerta de enlace segura Blast para aconsejar al cliente que espere y acepte el certificado del proxy en lugar del certificado de la puerta de enlace segura de Blast.

Puede configurar la puerta de enlace segura de Blast en Unified Access Gateway si carga el certificado del proxy en **Certificado del proxy de Blast** en la configuración de Unified Access Gateway de Horizon. Consulte el documento *Implementación y configuración de VMware Unified Access Gateway* en <https://docs.vmware.com/es/Unified-Access-Gateway/index.html>.

Nota Se cargará solo el certificado del proxy. Unified Access Gateway no conoce la clave privada correspondiente.

Puerta de enlace segura de PCoIP

Los servidores de seguridad y los dispositivos de Unified Access Gateway incluyen un componente de puerta de enlace segura de PCoIP. Si la puerta de enlace segura de PCoIP está habilitada, después de la autenticación, los clientes que utilicen PCoIP pueden efectuar otra conexión segura a un servidor de seguridad o a un dispositivo de Unified Access Gateway. Esta conexión permite que los clientes accedan a aplicaciones y escritorios remotos desde Internet.

Al habilitar el componente de puerta de enlace segura de PCoIP, el tráfico de PCoIP se redirige mediante un servidor de seguridad o un dispositivo de Unified Access Gateway a las aplicaciones y escritorios remotos. Si los clientes que usan PCoIP utilizan también la función de redireccionamiento USB o la aceleración de redireccionamiento de multimedia (MMR), se puede habilitar el componente de puerta de enlace segura de View para redirigir esos datos.

Al configurar conexiones de clientes directas, el tráfico de PCoIP y de otro tipo va directamente desde un cliente a una aplicación o un escritorio remoto.

Cuando usuarios finales, como personas que trabajan desde su hogar o usuarios móviles, acceden a los escritorios desde Internet, los servidores de seguridad o los dispositivos de Unified Access Gateway proporcionan el nivel necesario de seguridad y conectividad, de forma que no es necesaria una conexión VPN. El componente de puerta de enlace segura de PCoIP asegura que el único tráfico remoto que puede acceder al centro de datos corporativo es el tráfico en nombre de un usuario perfectamente autenticado. Los usuarios finales solo pueden acceder a los recursos para los que tengan autorización.

LDAP de View

LDAP de View es un directorio LDAP integrado en el servidor de conexión de View y es el repositorio de configuración para todos los datos de configuración de Horizon 7.

LDAP de View contiene entradas que representan cada aplicación y escritorio remotos, cada escritorio remoto accesible, varios escritorios remotos administrados conjuntamente, y configuraciones de componentes de Horizon 7.

LDAP de View también incluye un conjunto de DLL de complementos de Horizon 7 para proporcionar servicios de notificación y de automatización para otros componentes de Horizon 7.

Horizon Messaging

El componente Horizon Messaging proporciona el enrutador de mensajes para las comunicaciones entre componentes de Horizon Connection Server y entre Horizon Agent y el servidor de conexión.

Este componente es compatible con la API de Java Message Service (JMS), que se utiliza para mensajería en Horizon 7.

Para la validación de mensajes entre componentes, se usan claves DSA. El tamaño predeterminado de la clave es 512 bits, excepto en modo FIPS, en el que el tamaño de la clave es 2048 bits.

Nota Si el modo de seguridad de mensajes está establecido en **Mejorado**, para asegurar las conexiones JMS se utiliza SSL/TLS en lugar de cifrado por mensaje. En modo de seguridad de mensajes mejorado, la validación se aplica a solo un tipo de mensaje. Para utilizar el modo de mensaje mejorado, VMware recomienda aumentar el tamaño de la clave a 2048 bits. Si no se usa el modo de seguridad de mensaje mejorado, VMware recomienda no cambiar el valor predeterminado de 512 bits, ya que al aumentar el tamaño de la clave afecta al rendimiento y a la escalabilidad.

Si se desea que todas las claves sean de 1024 bits, se debe cambiar el tamaño de la clave RSA inmediatamente después de instalar la primera instancia del servidor de conexión y antes de crear servidores y escritorios adicionales. Consulte el artículo 1024431 de la base de conocimientos (KB) de VMware para obtener más información.

Reglas de firewall para el servidor de conexión de Horizon

Algunos puertos se deben abrir en el firewall para los servidores de seguridad y las instancias del servidor de conexión.

Cuando instale el servidor de conexión, el programa de instalación puede configurar de forma opcional las reglas del Firewall de Windows que necesita. Estas reglas abren los puertos que se utilizan de forma predeterminada. Si cambia los puertos predeterminados después de la instalación, debe configurar de forma manual el Firewall de Windows para que permita que los dispositivos de Horizon Client se conecten a Horizon 7 a través de los puertos actualizados.

La siguiente tabla muestra los puertos predeterminados que se pueden abrir de forma automática durante la instalación. Los puertos son de entrada a menos que se especifique lo contrario.

Tabla 5-4. Puertos abiertos durante la instalación del servidor de conexión de Horizon

Protocolo	Puertos	Tipo de instancia del servidor de conexión de Horizon
JMS	TCP 4001	Estándar y de réplica
JMS	TCP 4002	Estándar y de réplica

Tabla 5-4. Puertos abiertos durante la instalación del servidor de conexión de Horizon (continuación)

Protocolo	Puertos	Tipo de instancia del servidor de conexión de Horizon
JMSIR	TCP 4100	Estándar y de réplica
JMSIR	TCP 4101	Estándar y de réplica
AJP13	TCP 8009	Estándar y de réplica
HTTP	TCP 80	Servidor de seguridad, de réplica y estándar
HTTPS	TCP 443	Servidor de seguridad, de réplica y estándar
PCoIP	TCP 4172 integrado UDP 4172 ambas direcciones	Servidor de seguridad, de réplica y estándar
HTTPS	TCP 8443 UDP 8443	Servidor de seguridad, de réplica y estándar. Después de establecer la conexión inicial a Horizon 7, el navegador web o 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 View o del servidor de seguridad para permitir que se produzca esta segunda conexión.
HTTPS	TCP 8472	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la comunicación entre pods.
HTTP	TCP 22389	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la replicación LDAP global.
HTTPS	TCP 22636	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la replicación LDAP global de seguridad.

Reglas del firewall para Horizon Agent o View Agent

Los instaladores de View Agent y de Horizon Agent configuran de forma opcional las reglas del firewall de Windows en los escritorios remotos y los hosts RDS para abrir los puertos de red predeterminados. Los puertos son de entrada a menos que se especifique lo contrario.

Los instaladores de View Agent y de Horizon Agent configuran la regla del firewall local para que las conexiones RDP entrantes coincidan con el puerto RDP actual del sistema operativo del host, que suele ser 3389.

Si indica a los instaladores de View Agent o de Horizon Agent que no habiliten la compatibilidad con escritorios remotos, no se abrirán los puertos 3389 y 32111, y deberá abrirlos manualmente.

Si cambia el número de puerto RDP tras la instalación, deberá modificar las reglas del firewall asociadas. Si cambia un puerto predeterminado después de la instalación, debe volver a configurar de forma manual las reglas del firewall de Windows para permitir el acceso al puerto actualizado. Consulte "Reemplazar los puertos predeterminados para los servicios de View" en el documento *Instalación de Horizon 7*.

Las reglas de firewall de Windows para View Agent o Horizon Agent en hosts RDS muestran un bloque de 256 puertos UDP contiguos y abiertos para el tráfico entrante. Este bloque de puertos es para uso interno de VMware Blast en View Agent o Horizon Agent. Un controlador especial firmado de Microsoft sobre hosts RDS bloquea el tráfico entrante que llega a estos puertos de fuentes externas. Este controlador causa que el firewall de Windows trate los puertos como cerrados.

Si utiliza una plantilla de máquina virtual como origen de escritorio, las excepciones del firewall solo se aplican en los escritorios implementados si la plantilla es un miembro del dominio de escritorio. Puede utilizar la configuración de directiva de grupo de Microsoft para administrar las excepciones de firewall local. Consulte el artículo 875357 de la Microsoft Knowledge Base (KB) para obtener más información.

Tabla 5-5. Puertos TCP y UDP abiertos durante la instalación de View Agent o de Horizon Agent

Protocolo	Puertos
RDP	Puerto TCP 3389
Redireccionamiento USB y sincronización de la zona horaria	Puerto TCP 32111
MMR (redireccionamiento multimedia) y CDR (redireccionamiento de la unidad cliente)	Puerto TCP 9427
PCoIP	<p>En hosts RDS, PCoIP usa los siguientes números de puerto: puerto TCP 4172 y puerto UDP 4172 (bidireccional).</p> <p>En los escritorios, PCoIP usa números de puerto seleccionados a partir de un rango configurable. De forma predeterminada, puertos TCP de 4172 a 4173 y puertos UDP de 4172 a 4182. Las reglas del firewall para estos no especifican números de puertos, pero siguen dinámicamente los puertos abiertos en cada PCoIP Server. Los números de puertos seleccionados se comunican con el cliente mediante el servidor de conexión.</p>
VMware Blast	<p>Puerto TCP 22443</p> <p>Puerto UDP 22443 (bidireccional)</p> <p>Nota UDP no se utiliza en escritorios Linux.</p>
HTML Access	Puerto TCP 22443
XDMCP	<p>UDP 177</p> <p>Nota Este puerto se abre exclusivamente para acceso a XDMCP en los escritorios Linux que ejecutan Ubuntu 18.04. Las reglas de firewall bloquean todo el acceso externo del host a este puerto.</p>
X11	<p>TCP 6100</p> <p>Nota Este puerto se abre exclusivamente para acceso a XServer en los escritorios Linux que ejecutan Ubuntu 18.04. Las reglas de firewall bloquean todo el acceso externo del host a este puerto.</p>

Reglas del firewall para Active Directory

Si hay un firewall entre el entorno Horizon 7 y el servidor de Active Directory, es necesario asegurarse de que todos los puertos necesarios estén abiertos.

Por ejemplo, el servidor de conexión de View debe poder acceder a los servidores de Active Directory Global Catalog y Lightweight Directory Access Protocol (LDAP). Si los puertos de Global Catalog y LDAP están bloqueados por el software de firewall, los administradores tendrán problemas para configurar las autorizaciones de los usuarios.

Para obtener información sobre los puertos que se deben abrir para que Active Directory funcione correctamente a través de un firewall, consulte la documentación de Microsoft para su versión del servidor de Active Directory.

Descripción general de los pasos para configurar un entorno de Horizon 7

6

Complete estas tareas de alto nivel para instalar Horizon 7 y configurar una implementación inicial.

Tabla 6-1. Lista de tareas para instalar y configurar Horizon 7

Paso	Tarea
1	Configure los grupos y usuarios administradores necesarios en Active Directory. Instrucciones: documentación de vSphere e <i>Instalación de Horizon 7</i> .
2	Si aún no lo ha hecho, instale y configure los hosts de ESXi y vCenter Server. Instrucciones: documentación de VMware vSphere.
3	(Opcional) Si se van a instalar escritorios de clones vinculados, instale View Composer, ya sea en el sistema vCenter Server o en un servidor independiente. Instale también la base de datos de View Composer. Instrucciones: documento de <i>Instalación de Horizon 7</i> .
4	Instale y configure el servidor de conexión de Horizon. Instale también la base de datos de eventos. Instrucciones: documento de <i>Instalación de Horizon 7</i> .
5	Cree una o varias máquinas virtuales que se puedan usar como una plantilla para grupos de escritorios de clones completos o como máquinas principales para grupos de escritorios de clones vinculados o grupos de escritorios de clones instantáneos. Instrucciones: <i>Configurar escritorios virtuales en Horizon 7</i> .
6	(Opcional) Configure un host RDS e instale las aplicaciones remotas para los usuarios finales. Instrucciones: <i>Configurar aplicaciones y escritorios publicados en Horizon 7</i> .
7	Cree grupos de escritorios, grupos de aplicaciones o ambos. Instrucciones: <i>Configurar escritorios virtuales en Horizon 7</i> y <i>Configurar aplicaciones y escritorios publicados en Horizon 7</i> .
8	Control el acceso de los usuarios a los escritorios. Instrucciones: <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
9	Instale Horizon Client en las máquinas de los usuarios finales y permita que estos accedan a sus aplicaciones y escritorios remotos. Instrucciones: documentación de Horizon Client en https://docs.vmware.com/es/VMware-Horizon-Client/index.html .
10	(Opcional) Cree y configure administradores adicionales para permitir diferentes niveles de acceso a configuraciones y objetos del inventario específicos. Instrucciones: documento de <i>Administración de Horizon 7</i> .

Tabla 6-1. Lista de tareas para instalar y configurar Horizon 7 (continuación)

Paso	Tarea
11	(Opcional) Configure directivas para controlar el comportamiento de los componentes de Horizon 7, grupos de aplicaciones y escritorios y usuarios finales. Instrucciones: <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
12	(Opcional) Configure Horizon Persona Management, que proporciona a los usuarios acceso a opciones y datos personalizados cuando inician sesión en un escritorio. Instrucciones: <i>Configurar escritorios virtuales en Horizon 7</i> .
13	(Opcional) Para mayor seguridad, integre la autenticación de tarjetas inteligentes o una solución de autenticación de doble factor RADIUS. Instrucciones: documento de <i>Administración de Horizon 7</i> .