

Configurar escritorios de Horizon 7 for Linux

Diciembre de 2019
VMware Horizon 7 7.11



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2016-2019 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Configurar escritorios Horizon 7 for Linux 6

1 Funciones y requisitos del sistema 7

Funciones de los escritorios de Horizon para Linux 7

Descripción general de los pasos de configuración para los escritorios Horizon 7 for Linux 13

Requisitos del sistema para Horizon 7 for Linux 15

Configuración de máquinas virtuales para gráficos 2D 24

Configurar la función Session Collaboration en escritorios Linux 24

2 Preparar una máquina virtual Linux para implementar escritorios 28

Crear una máquina virtual e instalar Linux 28

Preparar una máquina Linux para la implementación de escritorios remotos 29

Instalar paquetes de dependencia para Horizon Agent 31

3 Configurar la integración de Active Directory para escritorios Linux 33

Integrar Linux con Active Directory 33

Utilizar la autenticación pass-through del servidor OpenLDAP 34

Configurar la autenticación LDAP mediante SSSD en Microsoft Active Directory 34

Utilizar la solución de unión a dominio Winbind 34

Configurar la autenticación PowerBroker Identity Services Open (PBISO) 35

Configurar la unión a dominio sin conexión mediante Samba 36

Usar la solución de unión Realmd en RHEL/CentOS 8.0 38

Configurar Single Sign-On 39

Configurar el redireccionamiento de tarjeta inteligente 40

Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 8.0 42

Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 7.x/6.x 47

Configurar el redireccionamiento de tarjetas inteligentes para escritorios Ubuntu 53

Configurar el redireccionamiento de tarjetas inteligentes para escritorios SLED/SLES 63

Configurar True SSO para escritorios Linux 70

Configurar True SSO en los escritorios RHEL/CentOS 8.0 70

Configurar True SSO para escritorios RHEL/CentOS 7.x 72

Configurar True SSO para escritorios Ubuntu 76

Configurar True SSO para escritorios SLED/SLES 82

4 Configurar gráficos para escritorios Linux 86

Configurar las distribuciones de Linux compatibles con vGPU 86

Instalar el VIB de la tarjeta gráfica NVIDIA GRID vGPU en el host ESXi 87

Configurar un dispositivo PCI compartido para vGPU en la máquina virtual Linux 88

Instalar el controlador de visualización NVIDIA GRID vGPU	89
Verificar que el controlador de pantalla NVIDIA está instalado	90
Configurar RHEL 6.x para vDGA	91
Habilitar DirectPath I/O para NVIDIA GRID en un host	91
Agregar un dispositivo de pass-through vDGA a una máquina virtual con RHEL 6.x	92
Instalar el controlador de visualización NVIDIA para vDGA	93
Verificar que el controlador de pantalla NVIDIA está instalado	94

5 Instalar Horizon Agent 96

Instalar Horizon Agent en una máquina virtual Linux	96
Opciones de la línea de comandos para install_viewagent.sh	97
Configurar el certificado para Linux Agent	99
Actualizar Horizon Agent en una máquina virtual Linux	100
Actualizar Horizon Agent en una máquina virtual Linux	101
Desinstalar máquinas Horizon 7 for Linux	102

6 Opciones de configuración para escritorios Linux 103

Opciones de configuración en los archivos de configuración de un escritorio Linux	103
Usar Directivas de Smart	113
Requisitos de Directivas de Smart	114
Instalar Dynamic Environment Manager	114
Configurar Dynamic Environment Manager	115
Opciones de directivas inteligentes de Horizon	115
Agregar condiciones a las definiciones de directivas de Horizon Smart	116
Crear una directiva de Horizon Smart en Dynamic Environment Manager	116
Ejemplo de configuración de Blast para escritorios Linux	118
Ejemplos de opciones de redireccionamiento de unidades cliente para escritorios Linux	119

7 Crear y administrar grupos de escritorios Linux 121

Crear un grupo de escritorios manual para Linux	122
Administrar grupos de escritorios Linux	123
Cree un grupo de escritorios automatizado de clones completos para Linux	124
Crear un grupo de escritorios flotantes de clones instantáneos para Linux	126
Comandos PowerCLI agente	130

8 Implementación por lotes de Horizon 7 para grupos de escritorios manuales 134

Descripción general de la implementación por lotes de escritorios Linux	134
Descripción general de la actualización por lotes de escritorios Linux	136
Crear una plantilla de máquina virtual para clonar máquinas de escritorios Linux	137
Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux	139
Script de ejemplo para clonar máquinas virtuales Linux	140

Script de ejemplo para unir máquinas virtuales clonadas a un dominio AD	144
Script de ejemplo para unir máquinas virtuales clonadas a un dominio de AD mediante SSH	147
Script de ejemplo para cargar archivos de configuración en máquinas virtuales Linux	151
Script de ejemplo para cargar archivos de configuración en máquinas virtuales de Linux mediante SSH	154
Script de ejemplo de PowerCLI para actualizar Horizon Agent en máquinas de escritorios Linux	158
Script de ejemplo para actualizar Horizon Agent en máquinas virtuales Linux mediante SSH	163
Script de ejemplo para realizar operaciones en máquinas virtuales Linux	169

9 Solucionar los problemas de escritorios Linux 173

Usar Horizon Help Desk Tool en Horizon Console	173
Iniciar Horizon Help Desk Tool en Horizon Console	174
Solucionar los problemas de los usuarios en Horizon Help Desk Tool	174
Detalles de las sesiones para Horizon Help Desk Tool	177
Procesos de las sesiones de Horizon Help Desk Tool	180
Solucionar problemas de sesiones de escritorios de Linux en Horizon Help Desk Tool	181
Recopilar información de diagnóstico de máquinas con Horizon 7 for Linux	182
Se produce un error en Horizon Agent al desconectarse de Horizon Client para iPad Pro	183
El escritorio SLES 12 SP1 no se actualiza automáticamente	183
SSO no puede conectarse a un agente de desconexión	183
No se puede acceder a la máquina virtual después de crear un grupo de escritorios manual para Linux	184

Configurar escritorios Horizon 7 for Linux

El documento *Configurar escritorios de Horizon 7 for Linux* proporciona información sobre la configuración de una máquina virtual Linux que se utilizará como un escritorio de VMware Horizon® 7 for Linux. La información incluye la preparación del sistema operativo invitado de Linux, la instalación de Horizon Agent en la máquina virtual y la configuración de la máquina en Horizon Console para su uso en una implementación de Horizon 7.

Público al que se dirige

Esta información está destinada a cualquier persona que quiera configurar y usar escritorios remotos que se ejecuten en sistemas operativos invitados Linux. La información está destinada a administradores de sistemas Linux con experiencia, que estén familiarizados con la tecnología de máquinas virtuales y operaciones de centros de datos.

Funciones y requisitos del sistema

1

Con Horizon 6.2.x o versiones posteriores, los usuarios pueden conectarse a escritorios remotos que ejecutan el sistema operativo Linux.

Este capítulo incluye los siguientes temas:

- [Funciones de los escritorios de Horizon para Linux](#)
- [Descripción general de los pasos de configuración para los escritorios Horizon 7 for Linux](#)
- [Requisitos del sistema para Horizon 7 for Linux](#)

Funciones de los escritorios de Horizon para Linux

La siguiente lista incluye las principales funciones que admiten los escritorios Linux en Horizon.

Funciones admitidas en escritorios Linux

Integración de Active Directory

Los escritorios de clones instantáneos que ejecuten las siguientes distribuciones de Linux pueden realizar una unión a dominio sin conexión con Active Directory mediante PowerBroker Identity Services Open (PBISO).

- Ubuntu 16.04 y 18.04
- SLED/SLES 12.x

Para obtener más información, consulte la sección de autenticación PowerBroker Identity Services Open (PBISO) en [Integrar Linux con Active Directory](#).

Los escritorios de clones instantáneos que ejecuten las siguientes distribuciones de Linux pueden realizar una unión a dominio sin conexión con Active Directory mediante Samba.

- Ubuntu 16.04 y 18.04

- RHEL 7.3 y 8.0

Entrada de audio

Se admite el redireccionamiento de entrada de audio desde un host de cliente a un escritorio remoto Linux. Esta función no está basada en la función de redireccionamiento USB. Si desea que esta función esté habilitada, debe seleccionarla durante la instalación. Como entrada de audio, desde su aplicación debe seleccionar en el dispositivo PulseAudio server (local) el audio predeterminado del sistema. Las siguientes distribuciones de Linux admiten esta función.

- Ubuntu 16.04 x64 con entornos de escritorio Gnome Fallback (Metacity) o MATE
- Ubuntu 18.04 x64 con entornos de escritorio Gnome Ubuntu o MATE
- RHEL 7.x Workstation x64 con entornos de escritorio Gnome o KDE
- RHEL 8.0 Workstation x64 con entornos de escritorio Gnome
- SLED/SLES 12.x SP3 x64

Salida de audio

Se admite el redireccionamiento de salida de audio. Esta función está habilitada de forma predeterminada. Para deshabilitar esta función, debe establecer la opción `RemoteDisplay.allowAudio` en **false**. Si se accede a través de los navegadores Chrome o Firefox, VMware Horizon HTML Access ofrecerá soporte de salida de audio para escritorios Linux.

Grupo de escritorios automatizado de clones completos

Puede crear grupos de escritorios de clones completos automatizados para escritorios Linux.

Redireccionamiento de unidades cliente

Si habilita la función Redireccionamiento de unidades cliente (CDR), podrá acceder a las unidades y las carpetas compartidas del sistema local. Utilice la carpeta `tsclient` que se encuentra en el directorio de inicio del escritorio remoto Linux. Para usar esta función, debe instalar los componentes de CDR.

Redireccionamiento del portapapeles

Con la función de redireccionamiento del portapapeles, puede copiar y pegar texto enriquecido o texto sin formato de un host cliente a un escritorio remoto Linux y viceversa. Puede establecer la dirección de copiar y pegar y el tamaño máximo del texto si utiliza las opciones de Horizon Agent. Esta función está habilitada de forma predeterminada. Se puede deshabilitar durante la instalación.

Modo FIPS 140-2

Aunque aún no tenga la validación del Programa de validación de módulos criptográficos (CMVP) del NIST, el soporte para el modo Estándar federal de procesamiento de información (FIPS) 140-2 está disponible para escritorios Linux.

Horizon 7 Agent for Linux implementa módulos criptográficos que están diseñados conforme a los requisitos del estándar FIPS 140-2. Estos módulos se validaron en los entornos operativos que aparecen en los certificados CMVP #2839 y #2866, y se trasladaron a esta plataforma. Sin embargo, todavía no se completaron en el plan del producto los requisitos de pruebas de CMVP y de CAVP diseñados para incluir nuevos entornos operativos en los certificados CMVP y CAVP NIST de VMware.

Nota La versión 1.2 del protocolo Seguridad de la capa de transporte (TLS) es obligatoria para que se admita el modo FIPS 140-2.

Herramienta del departamento de soporte técnico

Horizon Help Desk Tool es una aplicación web que permite solucionar problemas con sesiones de escritorios Linux. Puede usar Horizon Help Desk Tool para obtener el estado de las sesiones de los usuarios de Horizon 7 y para realizar operaciones de mantenimiento y de solución de problemas. Consulte [Usar Horizon Help Desk Tool en Horizon Console](#).

Directivas de Horizon Smart

Puede usar VMware Dynamic Environment Manager™ 9.4 o una versión posterior para crear Horizon Directivas de Smart que controlen el comportamiento del redireccionamiento USB, el redireccionamiento del portapapeles y las funciones del redireccionamiento de unidades cliente en escritorios remotos Linux específicos. Consulte [Usar Directivas de Smart](#).

Codificador H.264

H.264 puede mejorar el rendimiento de Blast Extreme para los escritorios de Horizon, particularmente en redes con un ancho de banda bajo. Si el sistema cliente tiene deshabilitado H.264, Blast Extreme volverá automáticamente a la codificación en formato JPEG/PNG.

El codificador de H.264 admite H.264 de hardware y codificadores de software. El H.264 de hardware tiene los siguientes requisitos.

- El procesador vGPU está configurado con una tarjeta gráfica NVIDIA.
- La serie 384 del controlador NVIDIA o una serie posterior se instala en la tarjeta gráfica NVIDIA.

Si el sistema cumple los requisitos anteriores, Horizon 7 for Linux usa el codificador H.264 de hardware. De lo contrario, se utiliza el codificador H.264 de software.

Grupo de escritorios flotantes de clones instantáneos

Puede crear grupos de escritorios flotantes de clones instantáneos para escritorios Linux. Esta función solo se admite en sistemas que tengan instalados las siguientes distribuciones de Linux.

- Ubuntu 16.04 y 18.04
- RHEL 7.1 o posterior
- RHEL 8.0

	<ul style="list-style-type: none"> ■ SLED/SLES 12.x <p>Si desea obtener más información, consulte Crear un grupo de escritorios flotantes de clones instantáneos para Linux.</p>
Entorno de escritorio de K	<p>El entorno de escritorio K (KDE) se admite en las siguientes distribuciones de Linux.</p> <ul style="list-style-type: none"> ■ CentOS 6.x y 7.x ■ RHEL 6.x y 7.x ■ Ubuntu 16.04 y 18.04
Sincronización de configuración regional y distribución del teclado	<p>Esta función especifica si se debe sincronizar la distribución del teclado actual y la configuración regional del sistema cliente con los escritorios Horizon Agent de Linux. Cuando esta opción está habilitada o no está configurada, se permite la sincronización. Cuando esta opción está deshabilitada, no se permite la sincronización.</p> <p>Esta función solo es compatible con VMware Horizon para Windows y para las siguientes configuraciones regionales: alemán, chino simplificado, chino tradicional, coreano, español, francés, inglés y japonés.</p>
PNG sin pérdida	<p>Las imágenes y los vídeos que se generan en un escritorio se representan en el dispositivo cliente de forma exacta, pixel a pixel.</p>
Grupo de escritorios manual	<p>Origen de la máquina.</p> <ul style="list-style-type: none"> ■ Máquina virtual administrada - Origen de la máquina para la máquina virtual vCenter. Se admiten máquinas virtuales administradas para implementar máquinas nuevas y actualizaciones. ■ Máquina virtual sin administrar - Origen de la máquina de otras fuentes. Solo se admiten máquinas virtuales sin administrar cuando la actualización se realiza desde una implementación de una máquina virtual sin administrar. <hr/> <p>Nota Para obtener el mejor rendimiento posible, no use ninguna máquina virtual sin administrar.</p> <hr/>
Entorno de escritorio MATE	<p>El entorno de escritorio MATE se admite en las siguientes distribuciones de Linux.</p> <ul style="list-style-type: none"> ■ Ubuntu 16.04 ■ Ubuntu 18.04
Varios monitores	<ul style="list-style-type: none"> ■ Los escritorios vDGA/vGPU admiten una resolución máxima de 2560 x 1600 en cuatro monitores.

- Los escritorios 2D de VMware vSphere® 6.0 o versiones posteriores admiten una resolución máxima de 2048 x 1536 en cuatro monitores, o bien una resolución máxima de 2560 x 1600 en tres monitores.

En Ubuntu 16.04 y 18.04, debe utilizar el entorno de escritorio MATE, KDE o GNOME para usar la función de varios monitores. Consulte <http://kb.vmware.com/kb/2151294> para obtener más información.

Para SLES 12 SP1, debe usar el paquete predeterminado con nivel de kernel kernel-default 3.12.49-11.1. Si actualizó el paquete, la función de varios monitores no funciona y solo puede visualizar el escritorio en un monitor.

A partir de VMware Horizon HTML Access™ 5.0, los escritorios con Horizon 7 para Linux admiten la función multimonitor.

Soporte de Network Intelligence para VMware Blast

VMware Blast admite Network Intelligence Transport. Esta función está habilitada de forma predeterminada.

Cuando el protocolo de datagramas de usuario (UDP) está habilitado, Blast establece las conexiones de protocolo de control de transmisión (TCP) y UDP. Según las condiciones de red, Blast selecciona de forma dinámica uno de los transporte para transmitir datos y ofrecer así la mejor experiencia de usuario. Por ejemplo, en una red de área local, TCP trabaja mejor que UDP, por lo que Blast selecciona TCP para transportar datos. De forma similar, en una red de área extensa (WAN), el rendimiento de UDP es mejor que el de TCP y Blast selecciona el transporte UDP en ese entorno.

Si uno de los componentes incluidos y usados no admite UDP, Blast solo establece la conexión TCP. Por ejemplo, si su conexión utiliza el componente de la puerta de enlace de seguridad de Blast del servidor de conexión de Horizon o del servidor de seguridad, solo se establece una conexión TCP. Incluso si el cliente y el agente habilitan UDP, la conexión utiliza TCP porque la puerta de enlace de seguridad de Blast no admite UDP. Si los usuarios se conectan desde fuera de la red empresarial, el componente UDP requiere VMware Unified Access Gateway (antes denominado Access Point), que admite UDP.

Utilice la siguiente información para establecer una conexión Blast basada en UDP.

- Si el cliente se conecta a un escritorio Linux, habilite UDP en el cliente y el agente. De forma predeterminada, UDP está habilitado en el cliente y el agente.

- Si el cliente se conecta a un escritorio Linux con Unified Access Gateway, habilite UDP en el cliente, el agente y Unified Access Gateway.

Session Collaboration

La función Session Collaboration le permite invitar a otros usuarios a que se unan a una sesión de escritorio remoto de Linux, o bien unirse a una sesión colaborativa cuando otro usuario le envíe una invitación. Esta función solo se admite en los escritorios remotos Linux con las siguientes distribuciones de Linux instaladas.

- Ubuntu 18.04 con el entorno de escritorios Gnome
- RHEL 7.5 o una versión posterior con el entorno de escritorio Gnome Classic
- RHEL 8.0 con el entorno de escritorios Gnome Classic

Single Sign-On

Single Sign-On (SSO) es compatible con las siguientes distribuciones de Linux.

- RHEL 8.0/7.x/6.x Workstation x64
- CentOS 8.0/7.x/6.x x64
- SLED/SLES 12.x SP3/SP2/SP1
- Ubuntu 18.04/16.04 x64

Redireccionamiento de tarjetas inteligentes

Las siguientes distribuciones de Linux admiten el redireccionamiento de tarjetas inteligentes.

- RHEL 8.0
- RHEL 7.1 y versiones posteriores
- RHEL 6.6 y versiones posteriores
- Ubuntu 18.04/16.04
- SLED/SLES 12.x SP3

Esta función admite las tarjetas de verificación de identidad personal (PIV) y las tarjetas de acceso común (CAC). Si desea obtener más información, consulte [Configurar el redireccionamiento de tarjeta inteligente](#).

Compatibilidad con True SSO

Las siguientes distribuciones de Linux admiten True SSO.

- RHEL 7.x/8.0
- CentOS 7.x/8.0
- SLED/SLES 12.x SP3
- Ubuntu 18.04/16.04

Si desea obtener más información, consulte [Configurar True SSO para escritorios Linux](#).

Redireccionamiento USB

La función Redireccionamiento USB permite acceder desde escritorios remotos Linux a dispositivos USB conectados localmente. Debe instalar los componentes de la función Redireccionamiento USB y el módulo del kernel de la unidad USB VHCI para usar la función USB. Asegúrese de que tenga los privilegios necesarios para usar el dispositivo USB que desee redireccionar.

Mouse de 3Dconnexion

Para empezar a usar un mouse de 3Dconnexion debe instalar el controlador de dispositivo adecuado y vincular el mouse desde el menú Conectar dispositivo USB de su escritorio Linux.

Gráficos 3D

La función Gráficos 3D admite las siguientes combinaciones de versiones Linux y tarjetas gráficas:

- vDGA se admite en RHEL 6.x Workstation x64 con tarjetas gráficas NVIDIA GRID K1 o K2.
- vGPU es compatible con las distribuciones Linux y las tarjetas gráficas NVIDIA especificadas en <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

Limitaciones de los escritorios y grupos de escritorios Linux

Los escritorios y los grupos de escritorios Linux tienen las siguientes limitaciones:

- No se admiten la impresión virtual, la impresión basada en ubicación ni la función de vídeo en tiempo real.
- No se admite la función de transferencia de archivos de VMware HTML Access.

Nota Cuando se usa un servidor de seguridad, el puerto 22443 debe abrirse en el firewall interno para permitir el tráfico entre el servidor de seguridad y el escritorio de Linux.

Descripción general de los pasos de configuración para los escritorios Horizon 7 for Linux

Cuando instale y configure escritorios Horizon 7 for Linux, debe seguir una secuencia de pasos distinta en función de si instala gráficos 2D o 3D en las máquinas virtuales.

Gráficos 2D: Descripción general de los pasos de configuración

Para los gráficos 2D, siga estos pasos:

- 1 Revise los requisitos del sistema para configurar una implementación de Horizon 7 for Linux. Consulte [Requisitos del sistema para Horizon 7 for Linux](#).

- 2 Cree una máquina virtual en vSphere e instale el sistema operativo Linux. Consulte [Crear una máquina virtual e instalar Linux](#).
- 3 Prepare el sistema operativo invitado para su implementación como escritorio en un entorno de Horizon 7. Consulte [Preparar una máquina Linux para la implementación de escritorios remotos](#).
- 4 Configure el sistema operativo Linux invitado para que se autentique con Active Directory. Este paso se implementa con software de terceros, según los requisitos de su entorno. Consulte [Integrar Linux con Active Directory](#) para obtener más información.
- 5 Instalar Horizon Agent en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- 6 Cree un grupo de escritorios que contenga las máquinas virtuales Linux configuradas. Consulte [Crear un grupo de escritorios manual para Linux](#).

Gráficos 3D: Descripción general de los pasos de configuración

Debe completar la configuración de NVIDIA GRID vGPU o vDGA en las máquinas virtuales Linux antes de instalar en ellas Horizon Agent y de implementar un grupo de escritorios en Horizon Console.

- 1 Revise los requisitos del sistema para configurar una implementación de Horizon 7 for Linux. Consulte [Requisitos del sistema para Horizon 7 for Linux](#).
- 2 Cree una máquina virtual en vSphere e instale el sistema operativo Linux. Consulte [Crear una máquina virtual e instalar Linux](#).
- 3 Prepare el sistema operativo invitado para su implementación como escritorio en un entorno de Horizon 7. Consulte [Preparar una máquina Linux para la implementación de escritorios remotos](#).
- 4 Configure el sistema operativo Linux para autenticar con Active Directory. Este paso se implementa con software de terceros, según los requisitos de su entorno. Consulte [Integrar Linux con Active Directory](#) para obtener más información.
- 5 Configure las funciones 3D en sus hosts ESXi y en la máquina virtual Linux. Siga los procedimientos para la función 3D que desee instalar.
 - Consulte [Configurar las distribuciones de Linux compatibles con vGPU](#).
 - Consulte [Configurar RHEL 6.x para vDGA](#).
- 6 Instalar Horizon Agent en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- 7 Cree un grupo de escritorios que contenga las máquinas virtuales Linux configuradas. Consulte [Crear un grupo de escritorios manual para Linux](#).

Implementación por lotes

Con Horizon Console, solo puede implementar máquinas virtuales Linux en un grupo de escritorios manual. Con vSphere PowerCLI, puede desarrollar scripts que automaticen la implementación de un grupo de máquinas de escritorios Linux. Consulte [Capítulo 8 Implementación por lotes de Horizon 7 para grupos de escritorios manuales](#).

Requisitos del sistema para Horizon 7 for Linux

Para instalar Horizon 7 for Linux, el sistema Linux debe cumplir ciertos requisitos de sistema operativo, de Horizon 7 y de la plataforma vSphere.

Versiones de Linux que admiten Horizon Agent

En la siguiente tabla, se muestran los sistemas operativos Linux compatibles con Horizon Agent.

Tabla 1-1. Sistemas operativos Linux que admiten Horizon Agent

Distribución de Linux	Arquitectura
Ubuntu 16.04 y 18.04	x64
Nota Debe aplicar una de las soluciones descritas en el artículo de la base de conocimientos de VMware http://kb.vmware.com/kb/2151294 .	
RHEL 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 y 8.0	x64
CentOS 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 y 8.0	x64
NeoKylin 6 Update 1	x64
SLED 12.x SP1/SP2/SP3	x64
SLES 12.x SP1/SP2/SP3	x64

Nota El agente de Linux tiene paquetes de dependencia en algunas distribuciones de Linux. Consulte [Instalar paquetes de dependencia para Horizon Agent](#) para obtener más información.

Nota En los sistemas RHEL/CentOS 8.0, Horizon Agent solo admite el protocolo de servidor de visualización X11. No se admite el protocolo Wayland.

Plataforma requerida y versiones del software Horizon 7

Para instalar y usar Horizon 7 for Linux, la implementación debe cumplir ciertos requisitos de la plataforma vSphere, de Horizon 7 y del software Horizon Client.

Tabla 1-2. Plataforma requerida y versiones del software Horizon 7

Plataforma y software	Versiones compatibles
Versión de la plataforma de vSphere	<ul style="list-style-type: none"> ■ vSphere 6.0 U2 o una versión posterior ■ vSphere 6.5 U1 o una versión posterior ■ vSphere 6.7 o una versión posterior
Entorno de Horizon	<ul style="list-style-type: none"> ■ Servidor de conexión de Horizon 7.11
Software de Horizon Client	<ul style="list-style-type: none"> ■ Horizon Client 5.3.0 para Android ■ Horizon Client 5.3.0 para Windows ■ Horizon Client 5.3.0 para Linux ■ Horizon Client 5.3.0 para Mac OS X ■ Horizon Client 5.3.0 para iOS (iPad Pro) ■ HTML Access 5.3.0 en Chrome, Firefox e Internet Explorer ■ No se admiten clientes cero.

Puertos TCP/UDP que usan las máquinas virtuales Linux

Horizon Agent y Horizon Client usan puertos TCP o UDP para acceder a la red entre ellos y varios componentes de Horizon Server.

Tabla 1-3. Puertos TCP/UDP que usan las máquinas virtuales Linux

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Horizon Client	*	Agente Linux	22443	TCP/UDP	Blast, si la puerta de enlace segura Blast no se utiliza
Servidor de seguridad, Servidor de conexión de Horizon o dispositivo Access Point	*	Agente Linux	22443	TCP/UDP	Blast, si la puerta de enlace segura Blast se utiliza
Horizon Agent	*	Servidor de conexión de Horizon	4001, 4002	TCP	Tráfico SSL de JMS.

Nota Para obtener más información sobre los puertos TCP y UDP utilizados por los clientes, consulte el documento *Seguridad en Horizon Client y Agent* y la guía [Puertos de red de VMware Horizon 7](#).

Para permitir a los usuarios conectarse a sus escritorios Linux, estos deben ser capaces de aceptar conexiones TCP entrantes desde los dispositivos de Horizon Client, el servidor de seguridad y Horizon Connection Server.

En distribuciones de Ubuntu y Kylin, el firewall iptables está configurado de forma predeterminada con una directiva de entrada de ACCEPTAR.

En distribuciones de RHEL y CentOS, siempre que sea posible, el script del instalador de Horizon Agent configura el firewall iptables con una directiva de entrada de ACCEPTAR.

Asegúrese de que iptables de un sistema operativo invitado con RHEL o CentOS tenga una directiva de entrada que sea ACEPTAR con respecto a las nuevas conexiones procedentes del puerto de Blast, que es el 22443.

Cuando está habilitada la BSG, las conexiones de cliente se dirigen desde un dispositivo de Horizon Client a través de la BSG en un servidor de seguridad o Horizon Connection Server hasta el escritorio Linux. Cuando la BSG no está habilitada, las conexiones se realizan directamente desde el dispositivo de Horizon Client hasta el escritorio Linux.

Verificar la cuenta Linux que usan las máquinas virtuales

[Tabla 1-4. Nombre y tipo de cuenta](#) muestra el nombre y el tipo de las cuentas que usan las máquinas virtuales Linux.

Tabla 1-4. Nombre y tipo de cuenta

Nombre de la cuenta	Tipo de cuenta	Usada por
raíz	Integrada en Linux OS	Java Standalone Agent, mksvchanserver, scripts de shell
vmwblast	Creada por el instalador del agente de Linux	VMwareBlastServer
<usuario con la sesión iniciada>	Linux OS integrado, usuarios de AD o de LDAP	Script python

Entorno de escritorios

Horizon 7 for Linux es compatible con varios entornos de escritorio en distribuciones de Linux diferentes.

[Tabla 1-5. Entornos de escritorio compatibles](#) muestra los entornos de escritorio predeterminados para cada distribución Linux y los entornos de escritorio adicionales que admite Horizon 7 for Linux.

Tabla 1-5. Entornos de escritorio compatibles

Distribución de Linux	Entorno de escritorio predeterminado	Entornos de escritorio compatibles con los escritorios Horizon 7 for Linux
Ubuntu 18.04	Gnome	Gnome Ubuntu, entorno de escritorio de K (K Desktop Environment, KDE), MATE
Ubuntu 16.04	Unity	Gnome Flashback (Metacity), KDE, MATE
RHEL/CentOS 6.x	Gnome	Gnome, KDE
RHEL/CentOS 7.x	Gnome	Gnome, KDE
RHEL/CentOS 8.0	Gnome	Gnome
SLED 12 SP1/SP2/SP3	Gnome	Gnome
SLES 12 SP1/SP2/SP3	Gnome	Gnome
NeoKylin 6 Update 1	Mate	Mate

Para cambiar el entorno de escritorio predeterminado que se usa en una de las distribuciones Linux admitidas, debe usar los pasos y comandos que aparecen a continuación y que son más apropiados para su escritorio Linux.

Nota Single Sign-On (SSO) para KDE y para el entorno de escritorio MATE solo funciona cuando el escritorio Linux utiliza la pantalla de inicio de sesión predeterminada. Debe instalar KDE y MATE con los comandos que aparecen en [Tabla 1-6. Comandos para instalar los entornos de escritorios](#).

Cuando use RHEL/CentOS 7.x y las distribuciones Ubuntu 18.04/16.04, SSO no puede desbloquear una sesión KDE bloqueada. Debe proporcionar manualmente la contraseña para desbloquear la sesión.

- 1 Instale el sistema operativo de la distribución Linux admitida con la opción predeterminada del entorno de escritorio.
- 2 Ejecute los comandos de [Tabla 1-6. Comandos para instalar los entornos de escritorios](#) adecuados para su distribución de Linux.

Tabla 1-6. Comandos para instalar los entornos de escritorios

Distribución de Linux	Nuevo entorno de escritorio predeterminado	Comandos para cambiar el entorno de escritorio predeterminado
RHEL/CentOS 6.x	KDE	<code># yum groupinstall "X Window System" "KDE Desktop"</code>
RHEL/CentOS 7.x	KDE	<code># yum groupinstall "KDE Plasma Workspaces"</code>
Ubuntu 18.04/16.04	KDE	<code># apt install plasma-desktop</code>
Ubuntu 18.04	MATE 1.225	<code># apt install ubuntu-mate-desktop</code>
Ubuntu 16.04	MATE 1.16	<code># apt-add-repository ppa:ubuntu-mate-dev/xenial-mate</code> <code># apt update</code> <code># apt upgrade</code> <code># apt install mate</code> <code># apt install ubuntu-mate-themes</code>
Ubuntu 16.04	Gnome Flashback (Metacity)	<code># apt install gnome-session-flashback</code>

- 3 Reinicie el escritorio para comenzar a usar el nuevo entorno de escritorio predeterminado.

Si habilitó SSO en un escritorio Linux que tuviera instalados varios entornos de escritorio, utilice la siguiente información para seleccionar el entorno de escritorio que se usará en una sesión SSO.

- En Ubuntu 18.04/16.04 y RHEL/CentOS 7.x, use la información que aparece en [Tabla 1-7. Opción SSODesktopType](#) para establecer la opción SSODesktopType en el archivo `/etc/vmware/viewagent-custom.conf` y especificar así el entorno de escritorio que se usará con SSO.

Tabla 1-7. Opción SSODesktopType

Tipo de escritorio	Opción de configuración SSODesktopType
MATE	SSODesktopType=UseMATE
GnomeUbuntu	SSODesktopType=UseGnomeUbuntu
GnomeFlashback	SSODesktopType=UseGnomeFlashback
KDE	SSODesktopType=UseKdePlasma
GnomeClassic	SSODesktopType=UseGnomeClassic

- En RHEL/CentOS 6.x, para que el inicio de sesión SSO use KDE, elimine todos los archivos de inicio de los escritorios, excepto el archivo de inicio KDE, del directorio `/usr/share/xsession`. Use el siguiente conjunto de comandos como ejemplo.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/kde*.desktop ./
```

Después de establecer la configuración inicial, el usuario final debe cerrar sesión o reiniciar el escritorio Linux para que KDE sea el escritorio predeterminado en la siguiente sesión SSO.

- En RHEL/CentOS 8.0, para que el inicio de sesión SSO use Gnome Classic, elimine todos los archivos de inicio de los escritorios, excepto el archivo de inicio Gnome Classic, del directorio `/usr/share/xsession`. Use el siguiente conjunto de comandos como ejemplo.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/gnome-classic.desktop ./
```

Después de establecer la configuración inicial, el usuario final debe cerrar sesión o reiniciar el escritorio Linux para que Gnome Classic sea el escritorio predeterminado en la siguiente sesión SSO.

Si deshabilitó SSO en un escritorio Linux que tenga varios entornos de escritorios instalados, no es necesario que realice los pasos anteriores. Los usuarios finales tienen que seleccionar el entorno de escritorio que quieran utilizar cuando inician sesión en ese escritorio Linux.

Requisitos de red

VMware Blast Extreme admite el protocolo de datagramas de usuario (UDP) y el protocolo de control de transmisión (TCP). Las condiciones de red afectan al rendimiento de UDP y TCP. Para obtener una experiencia de usuario mejorada, seleccione UDP o TCP dependiendo de la condición de red.

- Seleccione TCP si la condición de red es buena, por ejemplo, un entorno de red de área local (Local Area Network, LAN).
- Seleccione UDP si la condición de red es deficiente, por ejemplo, un entorno de red de área extensa (Wide Area Network, WAN) con pérdida de paquetes y retraso temporal.

Utilice una herramienta para analizar la red, como Wireshark, para determinar si VMware Blast Extreme utiliza TCP o UDP. Utilice el siguiente conjunto de pasos, en los que se usa Wireshark, como ejemplo de referencia.

- 1 Descargue e instale Wireshark en la máquina virtual Linux.

Para RHEL/CentOS 6:

```
sudo yum install wireshark
```

Para Ubuntu 18.04/16.04:

```
sudo apt install tshark
```

Para SLED/SLES 12:

```
sudo zypper install wireshark
```

- 2 Conéctese al escritorio Linux usando VMware Horizon Client.
- 3 Abra una ventana de terminal y ejecute el siguiente comando, que muestra el paquete de TCP o el paquete de UDP que usa VMware Blast Extreme.

```
sudo tshark -i any | grep 22443
```

Las condiciones de red afectan a las funciones Redireccionamiento USB y Redireccionamiento de unidades cliente (Client Drive Redirection, CDR). Si la condición de red es deficiente, por ejemplo, un ancho de banda limitado con retrasos y pérdida de paquetes, la experiencia de usuario pierde calidad. En dicha condición, el usuario final puede experimentar una de las siguientes situaciones.

- El proceso de copiar archivos remotos es lento. Por ello, envíe archivos de menor tamaño en su lugar.
- El dispositivo USB no aparece en el escritorio remoto Linux.
- Los datos USB no se envían completamente. Por ejemplo, si copia un archivo de gran tamaño, es posible que el archivo que pegue tenga un tamaño menor al original.

Controlador VHCI para el redireccionamiento USB

La función de redireccionamiento USB depende del controlador del kernel USB Virtual Host Controller Interface (VHCI). Para poder usar USB 3.0 y la función de redireccionamiento USB, debe realizar los siguientes pasos:

- 1 Descargue el código fuente de USB VHCI de <https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/>.
- 2 Para compilar el código fuente del controlador VHCI e instalar el binario resultante en el sistema Linux, use los comandos incluidos en [Tabla 1-8. Compile e instale el controlador USB VHCI](#).

Por ejemplo, si descomprime el archivo de instalación, VMware-horizonagent-linux-x86_64-*<versión>-<número-de-compilación>*.tar.gz del directorio /install_tmp/, la *ruta-completa_del_archivo-de-revisión* es /install_tmp/VMware-horizonagent-linux-x86_64-*<versión>-<número-de-compilación>*/resources/vhci/patch/vhci.patch y el comando patch que se debe usar es

```
# patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-<versión>-<número-de-compilación>/resources/vhci/patch/vhci.patch
```

Nota La instalación del controlador VHCI se debe realizar antes de instalar Horizon for Linux.

Tabla 1-8. Compile e instale el controlador USB VHCI

Distribución de Linux	Pasos para compilar e instalar el controlador USB VHCI
Ubuntu 18.04	<ol style="list-style-type: none"> 1 Instale los paquetes de dependencia. <pre># apt-get install make # apt-get install gcc # apt-get install libelf-dev</pre> 2 Compile e instale los controladores de VHCI. <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < <i>ruta-completa_del_archivo-de-revisión</i> # make clean && make && make install</pre>
Ubuntu 16.04	<p>Compile e instale los controladores de VHCI.</p> <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < <i>ruta-completa_del_archivo-de-revisión</i> # make clean && make && make install</pre>

Tabla 1-8. Compile e instale el controlador USB VHCI (continuación)

Distribución de Linux	Pasos para compilar e instalar el controlador USB VHCI
RHEL/CentOS 6.9/6.10	1 Instale los paquetes de dependencia.
RHEL/CentOS 7.x	<pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r)</pre>
RHEL/CentOS 8.0	<pre># yum install patch # yum install elfutils-libelf-devel</pre>
	2 Compile e instale los controladores de VHCI.
	<pre># tar -xvzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < ruta-completa_del_archivo-de-revisión # make clean && make && make install</pre>
	3 (RHEL/CentOS 8.0) Para garantizar que los controladores de VHCI funcionen correctamente con el redireccionamiento USB, configure las opciones de firma para el controlador USB.
	a Cree un par de claves SSL para el controlador USB.
	<pre>openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/"</pre>
	b Firme el controlador USB.
	<pre>sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-hcd.ko</pre>
	c Registre la clave para el arranque seguro UEFI.
	<pre>sudo mokutil --import MOK.der</pre>
	Nota Este comando envía una solicitud para establecer una contraseña de la clave de propietario de la máquina (MOK) para el arranque seguro UEFI.
	d Para configurar el arranque seguro UEFI en la consola de vSphere, reinicie el sistema. Para obtener más información, consulte https://sourceware.org/systemtap/wiki/SecureBoot .
SLED/SLES 12 SP2	1 Descubra la versión del paquete del kernel actual.
	<pre># rpm -qa grep kernel-default-\$(echo \$(uname -r) cut -d '-' -f 1,2)</pre>
	El resultado es el nombre del paquete de kernel instalado actualmente. Si, por ejemplo, el nombre del paquete es kernel-default-3.0.101-63.1, la versión actual del paquete del kernel será 3.0.101-63.1.
	2 Instale los paquetes kernel-devel, kernel-default-devel, kernel-macros y patch.
	<pre># zypper install --oldpackage kernel-devel-<versión-del-paquete-del-kernel> \ kernel-default-devel-<versión-del-paquete-del-kernel> kernel-macros-revisión <versión-del-paquete-del-kernel></pre>
	Por ejemplo:
	<pre># zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch</pre>

Tabla 1-8. Compile e instale el controlador USB VHCI (continuación)

Distribución de Linux	Pasos para compilar e instalar el controlador USB VHCI
	<p>3 Compile e instale los controladores de VHCI.</p> <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < ruta-completa_del_archivo-de-revisión # mkdir -p linux/\$(echo \$(uname -r) cut -d '-' -f 1)/drivers/usb/core # cp /lib/modules/\$(uname -r)/source/include/linux/usb/hcd.h linux/\$(echo \$(uname -r) cut -d '-' -f 1)/drivers/usb/core # make clean && make && make install</pre>

Además, siga estas directrices:

- Si el kernel de Linux cambia a una nueva versión, deberá volver a compilar e instalar el controlador VHCI, pero no es necesario que vuelva a instalar Horizon for Linux.
- También puede agregar Dynamic Kernel Module Support (DKMS) al controlador VHCI siguiendo pasos similares a los que aparecen en este ejemplo para un sistema Ubuntu 18.04/16.04.
 - a Instale los encabezados del kernel.

```
# apt install linux-headers-$(uname -r)
```

- b Instale dkms mediante el siguiente comando.

```
# apt install dkms
```

- c Extraiga el archivo TAR de VHCI y aplique las revisiones.

```
# tar xzvf vhci-hcd-1.15.tar.gz
# cd vhci-hcd-1.15
# patch -p1 < ruta-completa_al_archivo-revisión>
# cd ..
```

- d Copie los archivos de origen de VHCI extraídos al directorio /usr/src.

```
# cp -r vhci-hcd-1.15 /usr/src/usb-vhci-hcd-1.15
```

- e Cree un archivo llamado dkms.conf y colóquelo en el directorio /usr/src/usb-vhci-hcd-1.15.

```
# touch /usr/src/usb-vhci-hcd-1.15/dkms.conf
```

- f Agregue los siguientes contenidos al archivo dkms.conf.

```
PACKAGE_NAME="usb-vhci-hcd"
PACKAGE_VERSION=1.15
MAKE_CMD_TMPL="make KVERSION=$(kernelver)"

CLEAN="$MAKE_CMD_TMPL clean"
```

```
BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
MAKE[0]="$MAKE_CMD_TMPL"

BUILT_MODULE_NAME[1]="usb-vhci-hcd"
DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
MAKE[1]="$MAKE_CMD_TMPL"

AUTOINSTALL="YES"
```

- g Agregue este controlador VHCI a dkms.

```
# dkms add usb-vhci-hcd/1.15
```

- h Compile el controlador VHCI.

```
# dkms build usb-vhci-hcd/1.15
```

- i Instale el controlador VHCI.

```
# dkms install usb-vhci-hcd/1.15
```

Configuración de máquinas virtuales para gráficos 2D

Cuando cree máquinas virtuales de Horizon 7 para Linux, debe cambiar la configuración de vCPU y la memoria virtual según los requisitos de rendimiento.

Las máquinas virtuales que están configuradas para usar NVIDIA vDGA usan la tarjeta gráfica física de NVIDIA. Las máquinas virtuales que están configuradas para usar NVIDIA GRID vGPU usan la tarjeta gráfica virtual de NVIDIA, que está basada en el acelerador de gráficos físicos NVIDIA. No es necesario cambiar la configuración de vCPU ni la memoria virtual de estas máquinas virtuales.

Las máquinas virtuales que están configuradas para usar gráficos 2D utilizan la tarjeta gráfica virtual de VMware, y deberá cambiar los ajustes de vCPU y memoria virtual para mejorar el rendimiento del escritorio. Utilice las siguientes directrices:

- Para mejorar el rendimiento de un escritorio 2D, configure más vCPU y memoria virtual para la máquina virtual Linux. Por ejemplo, configure 2 vCPU y 2 GB de memoria virtual.
- Para una pantalla más grande con varios monitores, como cuatro monitores, establezca 4 vCPU y 4 GB de memoria virtual para la máquina virtual.
- Para mejorar la reproducción de vídeo en escritorios 2D, establezca 4 vCPU y 4 GB de memoria virtual para la máquina virtual.

Configurar la función Session Collaboration en escritorios Linux

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

Requisitos del sistema para Session Collaboration

Para admitir la función Session Collaboration, la implementación de Horizon debe cumplir ciertos requisitos.

Tabla 1-9. Requisitos del sistema para Session Collaboration

Componente	Requisitos
Sistema cliente	Los propietarios y colaboradores de sesión deben tener instalado Horizon Client 4.10 o una versión posterior para Windows, Mac o Linux en el sistema cliente, o bien usar HTML Access 4.10 o una versión posterior.
Escritorios remotos Linux	En el escritorio virtual Linux debe estar instalado Horizon Agent 7.7 o versiones posteriores. Debe habilitarse la función Session Collaboration en el nivel de grupo de escritorios y VDI.
Servidor de conexión	La instancia del servidor de conexión usa una licencia empresarial.
Protocolo de visualización	VMware Blast

Nota Los escritorios RHEL 8,0 requieren una configuración de sistema adicional para dar soporte a Session Collaboration. Consulte [Configurar un escritorio RHEL 8.0 para Session Collaboration](#).

Para obtener información sobre cómo utilizar la función Session Collaboration, consulte la documentación de Horizon Client.

Configurar las opciones de la función Session Collaboration en los archivos de configuración

Establezca la opción siguiente en el archivo `/etc/vmware/viewagent-custom.conf` para habilitar o deshabilitar la función Session Collaboration.

■ CollaborationEnable

Establezca las opciones siguientes en el archivo `/etc/vmware/config` para configurar las opciones utilizadas durante una sesión colaborativa.

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

Consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#) para obtener más información.

Limitaciones de las funciones de Session Collaboration

Los usuarios no pueden usar las siguientes funciones de escritorio remoto en una sesión de colaboración.

- Redireccionamiento USB

- Redireccionamiento de la entrada de audio
- Redireccionamiento de unidades cliente
- Redireccionamiento de tarjetas inteligentes
- Redireccionamiento del portapapeles

Los usuarios no pueden cambiar la resolución de escritorio remoto en una sesión colaborativa.

No se pueden tener varias sesiones de colaboración en la misma máquina cliente.

Nota Si el icono Session Collaboration de la bandeja del sistema no responde después de que un usuario inicie sesión por primera vez en el escritorio remoto, indique al usuario que cambie el tamaño de la ventana del escritorio remoto. El icono Session Collaboration empezará a responder después de que se cambia el tamaño de la ventana del escritorio.

Configurar un escritorio RHEL 8.0 para Session Collaboration

Para utilizar la función Session Collaboration en un escritorio RHEL 8.0, primero debe descargar e instalar la extensión shell de GNOME 3.28.26.

Procedimiento

- 1 Descargue la extensión shell de GNOME requerida para el sistema RHEL 8.0 de <https://extensions.gnome.org/extension/615/appindicator-support/>. Para la versión de shell, seleccione **3.28** . Para la versión de la extensión, seleccione **26**.
- 2 Descomprima el paquete descargado y cambie el nombre del directorio a `appindicator-support@rgcjonas.gmail.com` (el valor "uuid" en el archivo `metadata.json` del paquete).
- 3 Utilice el comando `mv` para mover el directorio `appindicator-support@rgcjonas.gmail.com` a esta ubicación: `/usr/share/gnome-shell/extensions`.

De forma predeterminada, el archivo `metadata.json` del directorio `appindicator-support@rgcjonas.gmail.com` solo es legible para el usuario raíz. Para admitir la colaboración de la sesión, también debe hacer que este archivo sea legible para otros usuarios.

- 4 Ejecute el comando para hacer que `metadata.json` sea legible para otros usuarios, como se muestra en el siguiente ejemplo.

```
chmod a+r metadata.json
```

- 5 Instale `gnome-tweaks`.
- 6 En el entorno de escritorio, reinicie el shell de GNOME pulsando la siguiente secuencia de teclas en el teclado.

```
Alt+F2
r
Enter
```

- 7 En el entorno de escritorio, ejecute `gnome-tweaks` y, a continuación, habilite **KStatusNotifierItem/ AppIndicator Support**.

Preparar una máquina virtual Linux para implementar escritorios

2

Para configurar un escritorio Linux, es necesario crear una máquina virtual Linux y preparar el sistema operativo para implementar escritorios remotos.

Este capítulo incluye los siguientes temas:

- [Crear una máquina virtual e instalar Linux](#)
- [Preparar una máquina Linux para la implementación de escritorios remotos](#)
- [Instalar paquetes de dependencia para Horizon Agent](#)

Crear una máquina virtual e instalar Linux

Debe crear una nueva máquina virtual en vCenter Server por cada escritorio remoto que se implemente en Horizon 7. Debe instalar su distribución de Linux en la máquina virtual.

Requisitos previos

- Compruebe que su implementación cumpla los requisitos para ser compatible con escritorios Linux. Consulte [Requisitos del sistema para Horizon 7 for Linux](#).
- Familiarícese con los pasos para crear máquinas virtuales en vCenter Server e instalar sistemas operativos invitados. Consulte "Crear y preparar máquinas virtuales" en el documento *Configurar escritorios virtuales en Horizon 7*.
- Familiarícese con los requisitos de configuración de memoria de vídeo (vRAM) para los monitores que desee utilizar con la máquina virtual. Consulte [Requisitos del sistema para Horizon 7 for Linux](#).

Procedimiento

- 1 En vSphere Web Client o vSphere Client, cree una nueva máquina virtual.

2 Configure las opciones de configuración personalizada.

- a Haga clic con el botón secundario en la máquina virtual y haga clic en **Editar configuración**.
- b Especifique el número de vCPU y el tamaño de la vMemory.

Para ver la configuración necesaria, siga las directrices de la guía de instalación de su distribución de Linux.

Por ejemplo, Ubuntu 18.04 especifica que se configuren 2.048 MB para vMemory y 2 vCPU.

- c Seleccione **Tarjeta de vídeo** y especifique el número de pantallas y la memoria de vídeo total (vRAM).

Consulte el tamaño de vRAM en vSphere Web Client para máquinas virtuales que usan 2D, que utilizan el controlador de VMware. El tamaño de vRAM no tiene efecto sobre máquinas con vDGA o NVIDIA GRID vGPU, que usan controladores de NVIDIA.

Para establecer la configuración necesaria, siga las instrucciones incluidas en [Configuración de máquinas virtuales para gráficos 2D](#). No use la Calculadora de memoria virtual.

3 Encienda la máquina virtual e instale la distribución de Linux.

4 Configure el entorno de escritorios que usará para la distribución específica de Linux.

Consulte la sección Entorno de escritorios en [Requisitos del sistema para Horizon 7 for Linux](#) para obtener más información.

5 Asegúrese de que el nombre de host del sistema se pueda resolver en 127.0.0.1.

Preparar una máquina Linux para la implementación de escritorios remotos

Debe realizar algunas tareas a fin de preparar una máquina Linux para usarla como escritorio remoto en una implementación de Horizon 7.

Para preparar una máquina Linux para que sea administrada por Horizon 7, debe habilitar la comunicación entre la máquina y el servidor de conexión. Debe configurar la red de la máquina Linux para que esta pueda hacer ping en la instancia del servidor de conexión usando su FQND (nombre de dominio completo).

Open VMware Tools (OVT) está preinstalado en las máquinas RHEL 8.0/7.x, CentOS 8.0/7.x y SLED/SLES 12.x. Si está preparando alguna de estas máquinas para usarla como escritorio remoto, puede omitir los pasos del 1 al 5 del siguiente procedimiento que describen cómo instalar VMware Tools si ejecuta manualmente el instalador.

Si está usando una máquina Ubuntu 16.04/18.04, instale OVT en ella. Si está preparando esta máquina para usarla como escritorio remoto, puede omitir los pasos del 1 al 5 del siguiente procedimiento e instalar OVT manualmente en su máquina Ubuntu 16.04/18.04 usando el siguiente comando:

```
apt-get install open-vm-tools-desktop
```

Requisitos previos

- Verifique que se haya creado una máquina virtual nueva en vCenter Server y que su distribución de Linux estuviera instalada en la máquina.
- Familiarícese con los pasos para montar e instalar VMware Tools en una máquina virtual Linux. Consulte "Instalar o actualizar VMware Tools manualmente en una máquina virtual Linux" en el documento *Administrar máquinas virtuales de vSphere*.
- Familiarícese con los pasos para configurar su máquina Linux para que el DNS pueda resolverla. Estos pasos varían en las diferentes distribuciones y versiones de Linux. Para obtener instrucciones, consulte la documentación de su distribución y su versión de Linux.

Procedimiento

- 1 En vSphere Web Client o en vSphere Client, monte el disco virtual de VMware Tools en la máquina virtual.
- 2 Haga clic con el botón secundario en el archivo del instalador de VMware Tools, `VMwareTools.x.x.x-xxxx.tar.gz`, haga clic en **Extraer en** y seleccione el escritorio de su distribución de Linux.

La carpeta `vmware-tools-distrib` se extrae en el escritorio.

- 3 En la máquina virtual, inicie sesión en la raíz y abra una ventana de terminal.
- 4 Descomprima el archivo tar del instalador de VMware Tools.

Por ejemplo:

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

- 5 Ejecute el instalador y configure VMware Tools.

Es posible que el comando varíe ligeramente en diferentes distribuciones de Linux. Por ejemplo:

```
cd vmware-tools-distrib
sudo ./vmware-install.pl -d
```

Normalmente, el archivo de configuración `vmware-config-tools.pl` se ejecuta después de que el archivo del instalador termine de ejecutarse.

- 6 Asigne 127.0.0.1 como nombre de host de la máquina Linux en el archivo `/etc/hosts`.

Para RHEL, CentOS, SLES y SLED, debe asignar manualmente 127.0.0.1 como nombre de host porque no está asignado automáticamente. Para Ubuntu, este paso no es necesario, ya que está asignado de forma predeterminada. Este paso tampoco es necesario cuando implementa escritorios por lotes, ya que el proceso de clonación agrega esta asignación.

Nota Si cambia el nombre de host de la máquina Linux después de instalar Horizon Agent, debe asignar 127.0.0.1 como nuevo nombre de host en el archivo `/etc/hosts`. De lo contrario, se seguirá usando el nombre de host antiguo.

- 7 Para RHEL y CentOS, verifique que `virbr0` esté deshabilitado.

```
virsh net-destroy default
virsh net-undefine default
service libvirtd restart
```

- 8 Asegúrese de que las instancias de Horizon Connection Server en el pod puedan resolverse a través del DNS.
- 9 Configure la máquina Linux para que el nivel de ejecución predeterminado sea 5.
- El nivel de ejecución para que funcione el escritorio Linux debe ser 5.

- 10 En una máquina Ubuntu que estuviera configurada para autenticarse con un servidor OpenLDAP, establezca el nombre de dominio completo en la máquina.

Este paso asegura que la información pueda mostrarse correctamente en el campo Usuario de la página Sesiones de Horizon Console. Edite el archivo `/etc/hosts` de la siguiente forma:

- a `# nano /etc/hosts`
- b Agregue el nombre de dominio completo. Por ejemplo: `127.0.0.1 hostname.domainname hostname.`
- c Cierre y guarde el archivo.

- 11 Para SUSE, deshabilite Cambiar nombre de host mediante DHCP. Establezca el nombre de host o de dominio.
- a En Yast, haga clic en **Configuración de red**.
 - b Haga clic en la pestaña **Nombre de host/DNS**.
 - c Desmarque **Cambiar nombre de host mediante DHCP**.
 - d Introduzca el nombre de host y el nombre de dominio.
 - e Haga clic en **Aceptar**.

Después de instalar VMware Tools, si actualiza kernel de Linux, es posible que VMware Tools deje de ejecutarse. Para resolver el problema, consulte <http://kb.vmware.com/kb/2050592>.

Instalar paquetes de dependencia para Horizon Agent

Horizon Agent for Linux tiene algunos paquetes de dependencia exclusivos para las distribuciones de Linux. Debe instalar estos paquetes antes de instalar Horizon Agent for Linux.

Requisitos previos

Verifique que se haya creado una máquina virtual nueva en vCenter Server y su distribución de Linux esté instalada en la máquina.

Procedimiento

- 1 Instale los paquetes obligatorios que no se instalaran o se actualizaran de forma predeterminada. Si algún paquete no cumple el requisito, el instalador detiene la instalación.

Tabla 2-1. Paquetes de dependencia obligatorios

Distribución de Linux	Paquetes
RHEL 7.5	<code>yum install libappindicator-gtk3</code>
SLES 12.x SP1/SLED 12.x SP1 Actualice xf86-video-vmware a una versión posterior a 13.0.2-3.2 desde el repositorio SUSE.	<ol style="list-style-type: none"> 1 Registre SUSE 12.x para habilitar los repositorios SUSE. <code>SUSEConnect -r <i>Código de registro</i> -e <i>Correo electrónico</i></code> 2 Actualice la versión de xf86-video-vmware. <code>zypper update xf86-video-vmware</code>
SLES 12.x	<p>Es necesario instalar python-gobject2 para el escritorio de Linux SLES 12.x cuando esté instalando Horizon Agent.</p> <ol style="list-style-type: none"> 1 Registre SUSE 12.x para habilitar los repositorios SUSE. <code>SUSEConnect -r <i>Código de registro</i> -e <i>Correo electrónico</i></code> 2 Instale python-gobject2. <code>zypper install python-gobject2</code>
Ubuntu 16.04	<code>apt-get install python-dbus python-gobject</code>
Ubuntu 18.04	<code>apt-get install python python-dbus python-gobject</code>

- 2 Instalar paquetes opcionales para Horizon Agent.

- De forma predeterminada, RHEL o CentOS 6.7 tienen glibc-2.12-1.166.el6.x86_64 instalado, lo que puede causar un problema de interbloqueo. Como resultado, la conexión del escritorio se bloquea. Para solucionar este problema, debe instalar la última versión de glibc desde un repositorio conectado.

```
sudo yum install glibc
```


Configurar la integración de Active Directory para escritorios Linux

3

Horizon 7 utiliza la infraestructura existente de Microsoft Active Directory para la administración y autenticación de usuarios. Los escritorios Linux se pueden integrar con Active Directory de forma que los usuarios puedan iniciar la sesión en ellos con sus cuentas de usuario de Active Directory.

Nota Horizon Agent espera que el usuario cliente y el escritorio Linux residan en el mismo dominio de Active Directory. Si el escritorio y el usuario residen en dominios diferentes, Horizon Agent podría identificar incorrectamente el dominio del escritorio como el dominio del usuario.

Este capítulo incluye los siguientes temas:

- [Integrar Linux con Active Directory](#)
- [Configurar Single Sign-On](#)
- [Configurar el redireccionamiento de tarjeta inteligente](#)
- [Configurar True SSO para escritorios Linux](#)

Integrar Linux con Active Directory

Existen varias soluciones para integrar Linux con Microsoft Active Directory (AD) y la solución que se utilice no afecta a los escritorios Horizon 7 for Linux.

Las siguientes soluciones funcionan en un entorno de escritorios Horizon 7 for Linux.

- Autenticación pass-through del servidor OpenLDAP
- Autenticación LDAP mediante System Security Services Daemon (SSSD) en Microsoft Active Directory
- Unión a dominio Winbind
- Autenticación PowerBroker Identity Services Open (PBISO)
- Unión a dominio sin conexión de Samba

Si utiliza soluciones basadas en LDAP, debe establecer la configuración en una máquina virtual de plantilla y no será necesario seguir otros pasos en las máquinas virtuales clonadas.

Nota Para facilitar la implementación, emplee la solución que utilice la autenticación LDAP mediante SSSD en Microsoft Active Directory.

Utilizar la autenticación pass-through del servidor OpenLDAP

Puede configurar un servidor OpenLDAP y utilizar el mecanismo de autenticación pass-through (PTA) para comprobar las credenciales de usuario en Active Directory.

En un nivel alto, es necesario seguir estos pasos para la solución de autenticación pass-through OpenLDAP.

Procedimiento

- 1 Para habilitar LDAPS (Protocolo ligero de acceso a directorios sobre SSL), instale Certificate Services en Active Directory.
- 2 Configurar un servidor OpenLDAP
- 3 Sincronice la información de usuario (excepto la contraseña) de Active Directory al servidor OpenLDAP.
- 4 Configure el servidor OpenLDAP para delegar la verificación por contraseña a un proceso independiente como `saslauthd`, que puede realizar la verificación por contraseña en Active Directory.
- 5 Configure los escritorios Linux para que usen un cliente LDAP para autenticar usuarios con el servidor OpenLDAP.

Configurar la autenticación LDAP mediante SSSD en Microsoft Active Directory

Para utilizar la autenticación LDAP en Windows Active Directory, configure System Security Services Daemon (SSSD) en el escritorio Linux.

Utilice los siguientes pasos de alto nivel para la solución de autenticación LDAP mediante SSSD.

Procedimiento

- 1 Para habilitar LDAPS (Protocolo ligero de acceso a directorios sobre capas de socket seguro), instale Certificate Services en el servidor de Active Directory.
- 2 Para usar la autenticación LDAP directamente en Microsoft Active Directory, configure SSSD en el escritorio Linux.

Utilizar la solución de unión a dominio Winbind

La solución de unión a dominio Winbind, una solución de autenticación basada en Kerberos, es otro método de autenticación de Active Directory.

Utilice los siguientes pasos de alto nivel para configurar la solución de unión a dominio Winbind.

Procedimiento

- 1 Instale los paquetes winbind, samba y Kerberos en el escritorio Linux.
- 2 Conecte el escritorio Linux a Microsoft Active Directory.

Pasos siguientes

Si utiliza la solución de unión a dominio Winbind u otra solución basada en la autenticación Kerberos, una la máquina virtual de plantilla a Active Directory y, a continuación, vuelva a unir la máquina virtual clonada a Active Directory. Por ejemplo, use el siguiente comando:

```
sudo /usr/bin/net ads join -U <domain_user>%<domain_password>
```

Use las siguientes opciones para ejecutar el comando para volver a unir al dominio en una máquina virtual clonada para la solución Winbind:

- Conecte remotamente SSH o vSphere PowerCLI a cada máquina virtual y ejecute el comando. Para obtener más información sobre los scripts, consulte [Capítulo 8 Implementación por lotes de Horizon 7 para grupos de escritorios manuales](#).
- Incluya el comando en un script de shell y defina la ruta del script a la opción de Horizon Agent RunOnceScript en el archivo /etc/vmware/viewagent-custom.conf. Si desea obtener más información, consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#).

Configurar la autenticación PowerBroker Identity Services Open (PBISO)

El método de autenticación PowerBroker Identity Services Open (PBISO) es una de las soluciones admitidas para llevar a cabo una unión a dominio sin conexión.

Los pasos siguientes le permitirán unir un escritorio Linux a Active Directory mediante PBISO.

Procedimiento

- 1 Descargue PBISO 8.5.6 o una versión posterior de <https://www.beyondtrust.com/products/powerbroker-identity-services-open/>.
- 2 Instale PBISO en su máquina virtual Linux.

```
sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- 3 Instale Horizon 7 Agent for Linux.
- 4 Use PBISO para unir el escritorio Linux al dominio de AD.

En el ejemplo siguiente, **lxdc.vdi** es el nombre de dominio y **administrator** es el nombre de usuario del dominio.

```
sudo domainjoin-cli join lxdc.vdi administrator
```

5 Establezca la configuración predeterminada para los usuarios del dominio.

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

6 Edite el archivo /etc/pamd.d/common-session.

- a Busque la línea que dice **session sufficient pam_lsass.so**.
- b Reemplace esa línea con **ssession [success=ok default=ignore] pam_lsass.so**.

Nota Debe repetir este paso después de volver a instalar o actualizar Horizon Agent for Linux.

7 En Ubuntu 16.04, anexe las siguientes líneas al archivo de configuración /usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf.

```
allow-guest=false
greeter-show-manual-login=true
```

Nota Con Ubuntu 18.04, no se requiere ningún cambio en el archivo de configuración lightdm.

8 Reinicie el sistema e inicie sesión.

Pasos siguientes

Nota

- Si la opción /opt/pbis/bin/config AssumeDefaultDomain se establece en **false**, debe actualizar la opción `SSOUserFormat=<username>@<domain>` en el archivo /etc/vmware/viewagent-custom.conf.
- Si utiliza la función de grupo de escritorios flotantes de clones instantáneos de Horizon y no desea perder la configuración del servidor DNS cuando al agregar el nuevo adaptador de red a la máquina virtual clonada, modifique el archivo `resolv.conf` para su sistema Linux. Utilice el siguiente ejemplo en un sistema Ubuntu 16.04 como guía para agregar las líneas necesarias al archivo /etc/resolvconf/resolv.conf.d/head.

```
nameserver 10.10.10.10
search mydomain.org
```

Configurar la unión a dominio sin conexión mediante Samba

Para dar soporte a SSO en una máquina virtual de clon instantáneo en un entorno de escritorio de Horizon 7 para Linux, configure Samba en la máquina virtual principal Linux.

Utilice el siguiente procedimiento como ejemplo para unir los dominios sin conexión de un escritorio Linux de clones instantáneos a Active Directory mediante Samba. Este procedimiento indica los pasos para un sistema Ubuntu.

Procedimiento

- 1 En la máquina virtual principal Linux, instale los paquetes winbind y samba, así como cualquier otra biblioteca dependiente como smbfs y smbclient.
- 2 Instale el paquete Samba tdb-tools mediante el comando siguiente.

```
sudo apt-get install tdb-tools
```

- 3 Instale Horizon 7 Agent for Linux.
- 4 Edite el archivo de configuración /etc/samba/smb.conf de manera que tenga un contenido similar al del ejemplo siguiente.

```
[global]
security = ads
realm = LAB.EXAMPLE.COM
workgroup = LAB
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

- 5 Edite el archivo de configuración /etc/krb5.conf de manera que tenga un contenido similar al del ejemplo siguiente.

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
YOUR-DOMAIN = {
kdc = 10.111.222.33
}

[domain_realm]
your-domain = EXAMPLE.COM
.your-domain = EXAMPLE.COM
```

- 6 Edite el archivo de configuración `/etc/nsswitch.conf`, tal como se muestra en el ejemplo siguiente.

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

- 7 Compruebe que el nombre de host sea correcto y que la fecha y hora del sistema estén sincronizadas con el sistema DNS.
- 8 Para informar a Horizon Agent de que se ha unido el dominio de la máquina virtual Linux mediante el método Samba, configure la siguiente opción en el archivo `/etc/vmware/viewagent-custom.conf`.

```
OfflineJoinDomain=samba
```

- 9 Reinicie el sistema y vuelva a iniciar sesión.

Usar la solución de unión Realmd en RHEL/CentOS 8.0

Para garantizar una correcta operación de funciones como el inicio de sesión único en escritorios RHEL/CentOS 8.0, utilice la solución realmd para unir el escritorio al dominio de Active Directory (AD).

Procedimiento

- 1 Configure un nombre de host completo para el sistema RHEL/CentOS 8.0.

Por ejemplo, si **rhel8** es el nombre de host no completo del sistema y **LXD.VDI** es el dominio de AD, ejecute el siguiente comando.

```
# hostnamectl set-hostname rhel8.lxd.vdi
```

- 2 Compruebe la conexión de red con el dominio de AD, tal y como se muestra en el siguiente ejemplo.

```
# realm discover -vvv LXD.VDI
```

- 3 Instale los paquetes de dependencia necesarios, tal y como se muestra en el siguiente ejemplo.

```
# dnf install -y sssd adcli samba-common-tools oddjob oddjob-mkhomedir
```

- 4 Únase al dominio de AD, tal y como se muestra en el siguiente ejemplo.

```
# realm join -U Administrator LXD.VDI
```

- 5 Edite el archivo de configuración `/etc/sss/sss.conf` de forma que quede parecido a este ejemplo. Agregue `ad_gpo_map_interactive = +gdm-vmwcred` en la sección *[dominio/nombre de dominio]*.

```
[sss]
domains = LXD.VDI
config_file_version = 2
services = nss, pam
```

```
[domain/LXD.VDI]
ad_domain = LXD.VDI
krb5_realm = LXD.VDI
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred
```

- 6 Para asegurarse de que la unión al dominio surta efecto, reinicie el sistema y vuelva a iniciar sesión.
- 7 Compruebe que los usuarios del dominio estén configurados correctamente. En el siguiente ejemplo se muestra cómo utilizar el comando `id` para devolver la salida de configuración desde el usuario de dominio `zyc1`.

```
# id zyc1

uid=1084401403(zyc1) gid=1084400513(domain users) groups=1084400513(domain users)
```

- 8 Con las credenciales de un usuario de dominio, compruebe que puede iniciar sesión correctamente en el escritorio.

Nota Horizon Agent solo admite el protocolo de servidor de visualización X11 en los escritorios RHEL/CentOS 8.0. Para configurar X11 como el protocolo de servidor de visualización predeterminado del sistema, haga clic en el icono configuración de la pantalla de inicio de sesión y seleccione **Classic (X11 display server)** en el menú desplegable.

Configurar Single Sign-On

Para configurar Single Sign-On (SSO), se deben realizar algunos pasos de configuración.

El módulo Single Sign-On de Horizon se comunica con los PAM (módulos de autenticación acoplable) de Linux y no depende del método que use para integrar Linux con Active Directory (AD). El SSO de Horizon funciona con las soluciones OpenLDAP y Winbind que integran Linux con AD.

De forma predeterminada, SSO asume que el atributo `sAMAccountName` de AD es el ID de inicio de sesión. Si usa la solución OpenLDAP o la solución Winbind, debe realizar los siguientes pasos de configuración para asegurar que se use el ID de inicio de sesión correcto para SSO:

- Para OpenLDAP, establezca `sAMAccountName` en `uid`.
- Para Winbind, agregue la siguiente instrucción al archivo de configuración `/etc/samba/smb.conf`.

```
winbind use default domain = true
```

Si los usuarios deben especificar el nombre de dominio para iniciar sesión, debe configurar la opción `SSOUserFormat` en el escritorio Linux. Si desea obtener más información, consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#). SSO siempre usa el nombre de dominio corto en mayúscula. Por ejemplo, si el dominio es `mydomain.com`, SSO usa `MYDOMAIN` como nombre de dominio. Por lo tanto, debe especificar `MYDOMAIN` cuando configure la opción `SSOUserFormat`. En cuanto a los nombres de dominio cortos y largos, se aplican las siguientes reglas:

- Para OpenLDAP, debe usar nombres de dominio cortos en mayúscula.
- Winbind admite nombres de dominio tanto cortos como largos.

AD admite caracteres especiales en los nombres de inicio de sesión, pero Linux no lo hace. Por lo tanto, no use caracteres especiales en los nombres de inicio de sesión cuando configure SSO.

En AD, si el atributo `UserPrincipalName` (UPN) y el atributo `sAMAccount` de un usuario no coinciden y el usuario inicia sesión con el UPN, se producirá un error en SSO. Por ejemplo, si tiene un usuario, `juser` en `mycompany.com` de AD, pero la UPN del usuario está configurada como `juser123@mycompany.com` en lugar de `juser@mycompany.com`, se producirá un error en SSO. Una solución alternativa es que el usuario inicie sesión con el nombre almacenado en `sAMAccount`. Por ejemplo, `juser`.

Horizon 7 no requiere que el nombre de usuario distinga entre mayúsculas y minúsculas. Debe asegurarse de que el sistema operativo Linux admita nombres de usuario que no distingan entre mayúsculas y minúsculas.

- Winbind no distingue entre mayúsculas y minúsculas en el nombre de usuario de forma predeterminada.
- Para OpenLDAP, Ubuntu usa NSCD para autenticar usuarios y distingue entre mayúsculas y minúsculas de forma predeterminada. RHEL y CentOS usan SSSD para autenticar usuarios y distingue entre mayúsculas y minúsculas de forma predeterminada. Para cambiar esta opción, edite el archivo `/etc/sss/sss.conf` y agregue la siguiente línea en la sección `[domain/default]`:

```
case_sensitive = false
```

Si el escritorio Linux tiene varios entornos de escritorio instalado, consulte [Entorno de escritorios](#) para seleccionar el entorno de escritorio que se usará con SSO.

Configurar el redireccionamiento de tarjeta inteligente

Para configurar el redireccionamiento de tarjeta inteligente, se deben realizar algunos pasos de configuración.

Descripción general del redireccionamiento de tarjeta inteligente

El redireccionamiento de tarjetas inteligentes es compatible con escritorios que ejecutan las siguientes distribuciones de Linux con las versiones especificadas de Horizon Agent instaladas.

Tabla 3-1. Requisitos del sistema para el redireccionamiento de tarjetas inteligentes

Distribución de Linux	Horizon Agent
RHEL 8.0	Horizon Agent 7.10 o versiones posteriores
RHEL 7.1 o posterior	Horizon Agent 7.8 o versiones posteriores
RHEL 6.6 o posterior	Horizon Agent 6.2.1 o posterior
Ubuntu 18.04/16.04	Horizon Agent 7.9 o posterior
SLED/SLES 12.x SP3	Horizon Agent 7.9 o posterior

Cuando instale Horizon Agent, primero debe deshabilitar SELinux. También debe seleccionar específicamente el componente de redireccionamiento de tarjetas inteligentes, ya que este no está seleccionado de forma predeterminada. Si desea obtener más información, consulte [Opciones de la línea de comandos para install_viewagent.sh](#).

Si la función de redireccionamiento de tarjetas inteligentes está habilitada en una máquina virtual, el redireccionamiento de USB de vSphere Client no funcionará con la tarjeta inteligente.

El redireccionamiento de tarjetas inteligentes solo admite un lector de tarjetas inteligentes a la vez. Esta opción no funciona si se conectan dos o más lectores al sistema cliente.

El redireccionamiento de tarjeta inteligente solo admite que haya un certificado en la tarjeta. Si hay más de un certificado en la tarjeta, se usará el que esté en la primera ranura y el resto se ignorará. Este comportamiento es una limitación de Linux.

Nota El redireccionamiento de tarjetas inteligentes admite las tarjetas PIV en escritorios Linux. Cuando usa Horizon Client para Linux para autenticar el agente con una tarjeta PIV, debe establecer que la tarjeta inteligente PIV admita TLSv1.2 y evitar que aparezca un error SSL. Use la solución descrita en el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150470>.

Nota El SSO de tarjetas inteligentes está habilitado en la versión 7.0.1 de Horizon 7 o en las versiones posteriores. Los escritorios RHEL 6.x admiten el SSO de tarjetas inteligentes, pero los escritorios RHEL 7.x y RHEL 8.0 no.

Configurar el redireccionamiento de tarjetas inteligentes

Para configurar el redireccionamiento de tarjetas inteligentes, realice las siguientes tareas.

- 1 Configure la tarjeta inteligente de su escritorio siguiendo las instrucciones del distribuidor de Linux y del proveedor de la tarjeta inteligente.
- 2 Integre su escritorio con un dominio de Active Directory, siguiendo el procedimiento de su distribución de Linux.
- 3 Configure el redireccionamiento de tarjetas inteligentes en su escritorio siguiendo el procedimiento de su distribución Linux.

Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 8.0

Para configurar el redireccionamiento de tarjetas inteligentes para un escritorio RHEL 8.0, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas necesarias antes de instalar Horizon Agent.

Integrar escritorios RHEL 8.0 con Active Directory para el redireccionamiento de tarjetas inteligentes

Utilice el siguiente procedimiento para integrar un escritorio RHEL 8.0 con un dominio de Active Directory (AD) para el redireccionamiento de tarjetas inteligentes.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
rhel8sc.rzview2.com	Nombre de host completo de su sistema RHEL 8.0
rhel8sc	Nombre de host no completo de su sistema RHEL 8.0
rzview2.com	Nombre DNS de su dominio de AD
RZVIEW2.COM	Nombre DNS de su dominio de AD, en mayúsculas
RZVIEW2	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
rzviewdns.rzview2.com	Nombre de host del servidor de AD

Procedimiento

- 1 En su sistema RHEL 8.0, haga lo siguiente.
 - a Configure los ajustes DNS y de red según lo requiera su organización.
 - b Deshabilite **IPv6**.
 - c Deshabilite **DNS automático**.
- 2 Edite el archivo de configuración `/etc/hosts` de forma que quede parecido a este ejemplo.

```
127.0.0.1      rhel8sc.rzview2.com rhel8sc localhost localhost.localdomain localhost4
localhost4.localhostdomain4
::1           localhost localhost.localdomain localhost6 localhost6.localhostdomain6

DIRECCIÓN_IP_dns  rzviewdns.rzview2.com
```

- 3 Edite el archivo de configuración `/etc/resolv.conf` de forma que quede parecido a este ejemplo.

```
# Generated by NetworkManager
search rzview2.com
nameserver DIRECCIÓN_ip_dns
```

- 4 Instale los paquetes necesarios para la integración de AD.

```
# yum install -y samba-common-tools oddjob-mkhomedir
```

- 5 Habilite el servicio `oddjobd`.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

- 6 Especifique la identidad del sistema y las fuentes de autenticación.

```
# authselect select sssd with-smartcard with-mkhomedir
```

- 7 Inicie el servicio `oddjobd`.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

- 8 Para dar soporte a la autenticación de tarjetas inteligentes, cree el archivo `/etc/sss/sss.conf`.

```
# touch /etc/sss/sss.conf
# chmod 600 touch /etc/sss/sss.conf
# chown root:root /etc/sss/sss.conf
```

- 9 Añada el contenido necesario a `/etc/sss/sss.conf`, como se muestra en el siguiente ejemplo. En la sección **[pam]**, especifique **pam_cert_auth = True**.

```
[sss]
config_file_version = 2
domains = rzview2.com
services = nss, pam, pac

[domain/RZVIEW2.COM]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
cache_credentials = true

[pam]
pam_cert_auth = True
```

10 Habilite el servicio sssd.

```
# systemctl enable sssd.service
# systemctl start sssd.service
```

11 Edite el archivo de configuración /etc/krb5.conf de forma que quede parecido a este ejemplo.

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = RZVIEW2.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    RZVIEW2.COM = {
        kdc = rzviewdns.rzview2.com
        admin_server = rzviewdns.rzview2.com
        default_domain = rzviewdns.rzview2.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = rzviewdns.rzview2.com
    }

[domain_realm]
    .rzview2.com = RZVIEW2.COM
    rzview2.com = RZVIEW2.COM
```

12 Edite el archivo de configuración /etc/samba/smb.conf de forma que quede parecido a este ejemplo.

```
[global]
    workgroup = RZVIEW2
    security = ads
    passdb backend = tdbsam
    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw
    password server = rzviewdns.rzview2.com
    realm = RZVIEW2.COM
```

```

idmap config * : range = 16777216-33554431
template homedir = /home/RZVIEW2/%U
template shell = /bin/bash
kerberos method = secrets and keytab

[homes]
comment = Home Directories
valid users = %S, %D%w%S
browseable = No
read only = No
inherit acls = Yes

[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775

```

- 13 Únase al dominio de AD, tal y como se muestra en el siguiente ejemplo.

```
# net ads join -U AdminUser
```

Al ejecutar el comando `join`, se obtiene un resultado similar al siguiente ejemplo.

```

Enter AdminUser's password:
Using short domain name -- RZVIEW2
Joined 'RHEL8SC' to dns domain 'rzview2.com'

```

- 14 Compruebe que el escritorio RHEL 8.0 se unió correctamente al dominio de AD.

```

# net ads testjoin

Join is OK

```

Pasos siguientes

[Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 8.0](#)

Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 8.0

Para configurar el redireccionamiento de tarjetas inteligentes en escritorios RHEL 8.0, instale las bibliotecas de las que depende la función, el certificado de CA raíz para dar soporte a la autenticación de confianza de tarjetas inteligentes y la biblioteca PC/SC Lite necesaria.

Requisitos previos**Integrar escritorios RHEL 8.0 con Active Directory para el redireccionamiento de tarjetas inteligentes****Procedimiento**

- 1 Instale las bibliotecas necesarias.

```
# yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
```

- 2 Habilite el servicio pcscd.

```
# systemctl enable pcscd
# systemctl start pcscd
```

- 3 Asegúrese de que el archivo de configuración /etc/sss/sss.conf contenga las siguientes líneas, que habilitan la autenticación de tarjetas inteligente.

```
[pam]
pam_cert_auth = True
```

- 4 Copie el certificado de CA necesario en /etc/sss/pki/sss_auth_ca_db.pem.

```
# openssl x509 -inform der -in certificate.cer -out certificate.pem
# cp certificate.pem /etc/sss/pki/sss_auth_ca_db.pem
```

- 5 Para comprobar el estado de la tarjeta inteligente, ejecute los siguientes comandos pkcs11-tool y confirme que devuelven la salida correcta.

```
# pkcs11-tool -L

# pkcs11-tool --login -0

# pkcs11-tool --test --login
```

- 6 Configure el módulo PKCS11.

```
cp libcmP11.so /usr/lib64/
```

- 7 Cree el archivo /usr/share/p11-kit/modules/libcmP11.module. Agregue el siguiente contenido al archivo.

```
# This file describes how to load the opensc module
# See: http://p11-glue.freedesktop.org/doc/p11-kit/config.html

# This is a relative path, which means it will be loaded from
# the p11-kit default path which is usually $(libdir)/pkcs11.
# Doing it this way allows for packagers to package opensc for
# 32-bit and 64-bit and make them parallel installable
module: /usr/lib64/libcmP11.so
priority: 99
```

8 Actualice PC/SC Lite a la versión 1.8.8.

```
# yum install -y git flex autoconf automake libtool libudev-devel flex
# git clone https://salsa.debian.org/rousseau/PCSC.git
# cd PCSC
# git checkout -b 1.8.8 pcsc-1.8.8
# ./bootstrap
# ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu
    --program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr
    --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share
    --includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec
    --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man
    --infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
# make
# make install
```

9 Instale Horizon Agent 7.10 o una versión posterior, con el redireccionamiento de tarjetas inteligentes habilitado.

10 Reinicie el sistema y vuelva a iniciar sesión.

Configurar el redireccionamiento de tarjetas inteligentes para escritorios RHEL 7.x/6.x

Para configurar el redireccionamiento de tarjetas inteligentes para un escritorio RHEL 7.x/6.x, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas necesarias antes de instalar Horizon Agent.

Integrar escritorios RHEL 7.x/6.x con Active Directory para el redireccionamiento de tarjetas inteligentes

Para admitir el redireccionamiento de tarjetas inteligentes en escritorios RHEL 7.x/6.x, integre el escritorio con un dominio de Active Directory (AD) mediante las soluciones Samba y Winbind.

Utilice el siguiente procedimiento para integrar un escritorio RHEL 7.x/6.x con un dominio de AD para el redireccionamiento de tarjetas inteligentes.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas

Valor del marcador de posición	Descripción
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD

Nota El redireccionamiento de tarjetas inteligentes se admite en escritorios con RHEL 6.0, RHEL 7.1 o versiones posteriores.

Procedimiento

- 1 En su escritorio RHEL 7.x/6.x, instale los paquetes requeridos.

```
# yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients authconfig-gtk
```

- 2 Edite la configuración de red de la conexión del sistema. Abra el panel de control de NetworkManager y desplácese a **Ajustes de IPv4** de la conexión de su sistema. Para el método de IPv4, seleccione **Automático (DHCP)**. En el cuadro de texto **Servidores DNS**, introduzca la dirección IP de su servidor de nombres DNS. A continuación, haga clic en **Aplicar**.
- 3 Ejecute el siguiente comando y compruebe que devuelve el nombre de dominio completo (FQDN) de su escritorio RHEL.

```
# hostname -f
```

- 4 Edite el archivo de configuración `/etc/resolv.conf`, tal y como se muestra en el ejemplo siguiente.

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

- 5 Deshabilite Security-Enhanced Linux (SELinux) en el escritorio RHEL. Edite el archivo de configuración `/etc/selinux/config`, como se muestra en el ejemplo siguiente.

```
SELINUX=disabled
```

- 6 Edite el archivo de configuración `/etc/krb5.conf`, tal y como se muestra en el siguiente ejemplo.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MIDOMINIO.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MIDOMINIO.COM = {
        kdc = nombredelhost-ads
        admin_server = nombredelhost-ads
```



```

        default_domain = nombredelhost-ads
    }

[domain_realm]
    .midominio.com = MIDOMINIO.COM
    midominio.com = MIDOMINIO.COM

```

- 7 Edite el archivo de configuración `/etc/samba/smb.conf`, tal y como se muestra en el siguiente ejemplo.

```

[global]
    workgroup = MIDOMINIO
    password server = nombredelhost-ads
    realm = MIDOMINIO.COM
    security = ads
    idmap config * : range = 16777216-33554431
    template homedir = /home/MIDOMINIO/%U
    template shell = /bin/bash
    kerberos method = secrets and keytab
    winbind use default domain = true
    winbind offline logon = false
    winbind refresh tickets = true

    passdb backend = tdbsam

```

- 8 Abra la herramienta `authconfig gtk` y configure las opciones tal y como se muestra a continuación.
- Seleccione la pestaña **Identidad & Autenticación**. En Base de Datos de Cuentas de Usuarios, seleccione **Winbind**.
 - Seleccione la pestaña **Opciones avanzadas** y seleccione la casilla de verificación **Crear los directorios home (principales) al ingresar la primera vez**.
 - Seleccione la pestaña **Identidad & Autenticación** y, a continuación, haga clic en **Unirse al Dominio**. En la alerta que le solicita que guarde los cambios, haga clic en **Guardar**.
 - Cuando se le solicite, introduzca el nombre de usuario y la contraseña del administrador del dominio y haga clic en **Aceptar**.

Su escritorio RHEL se unió al dominio de AD.

- 9 Configure almacenamiento en caché de ticket en PAM Winbind. Edite el archivo de configuración `/etc/security/pam_winbind.conf` para que incluya las líneas que se muestran en el ejemplo siguiente.

```

[global]

# authenticate using kerberos
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes

```

10 Reinicie el servicio Winbind.

```
# sudo service winbind restart
```

11 Para comprobar que se unió a AD, ejecute los siguientes comandos y asegúrese de que devuelven el resultado correcto.

- net ads testjoin
- net ads info

12 Reinicie el sistema y vuelva a iniciar sesión.**Pasos siguientes**

[Configurar el redireccionamiento de tarjetas inteligentes en un escritorio RHEL 7.x/6.x](#)

Configurar el redireccionamiento de tarjetas inteligentes en un escritorio RHEL 7.x/6.x

Para configurar el redireccionamiento de tarjetas inteligentes en escritorios RHEL 7.x/6.x, instale las bibliotecas de las que depende la función, el certificado de CA raíz necesario para la autenticación y la biblioteca PC/SC Lite necesaria. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Utilice el siguiente procedimiento para configurar el redireccionamiento de tarjetas inteligentes en un escritorio RHEL 7.x/6.x.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD

El redireccionamiento de tarjetas inteligentes se admite en escritorios con RHEL 6.0, RHEL 7.1 o versiones posteriores.

Nota Si utiliza la consola de vSphere para iniciar sesión en un sistema RHEL 7.x. que tiene instalado Horizon Agent y tiene el redireccionamiento de tarjetas inteligentes habilitado, es posible que experimente un retraso de al menos dos minutos al cerrar sesión. Este retraso al cerrar sesión solo se produce desde la consola de vSphere. La experiencia de cierre de sesión de RHEL 7.x desde Horizon Client no se ve afectada.

Requisitos previos

[Integrar escritorios RHEL 7.x/6.x con Active Directory para el redireccionamiento de tarjetas inteligentes](#)

Procedimiento

- 1 Instale las bibliotecas necesarias.

```
yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid authconfig
authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

- 2 Instale un certificado de una entidad de certificación (CA) raíz.

- a Descargue un certificado de CA raíz y guárdelo en su escritorio en /tmp/certificate.cer. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).
- b Busque el certificado de CA raíz que descargó y transfíralo a un archivo .pem.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c El comando certutil le permitirá instalar el certificado CA raíz en la base de datos del sistema /etc/pki/nssdb.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d Copie el certificado de CA raíz en el directorio /etc/pam_pkcs11/cacerts.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 Desplácese hasta **Aplicaciones > Sundry > Autenticación**, marque la casilla de verificación **Habilitar soporte para tarjetas inteligentes** y haga clic en **Aplicar**.
- 4 Copie los controladores de las tarjetas inteligentes y añada la biblioteca de controladores a la base de datos del sistema /etc/pki/nssdb.

```
cp libcmP11.so /usr/lib64/
modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pki/nssdb/
```

- 5 Edite la opción module en el archivo de configuración /etc/pam_pkcs11/pam_pkcs11.conf, tal como se muestra en este ejemplo.

```
pkcs11_module coolkey {
    module = libcmP11.so;
    description = "Cool Key";
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca, signature;
}
```

- 6 Edite el archivo `/etc/pam_pkcs11/cn_map` para que incluya contenido similar al siguiente ejemplo. Para que se incluya el contenido específico, consulte la información del usuario que aparece en el certificado de la tarjeta inteligente.

```
user sc -> user-sc
```

- 7 Edite el archivo de configuración `/etc/krb5.conf/`, tal y como se muestra en el ejemplo siguiente.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MIDOMINIO.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MIDOMINIO.COM = {
        kdc = nombredelhost-ads
        admin_server = nombredelhost-ads
        default_domain = nombredelhost-ads
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = nombredelhost-ads
    }

[domain_realm]
    .midominio.com = MIDOMINIO.COM
    midominio.com = MIDOMINIO.COM
```

- 8 Edite el archivo de configuración `/etc/pam.d/system-auth` para que incluya la línea que se muestra en el ejemplo siguiente.

```
auth optional pam_krb5.so use_first_pass no_subsequent_prompt
    preauth_options=X509_user_identity=PKCS11:/usr/lib64/libcsp11.so
```

- 9 Reinicie el demonio de PC/SC.

```
chkconfig pcscd on
service pcscd start
```

- 10 Instale la versión de PC/SC Lite adecuada para su distribución de RHEL.

- Para RHEL 7.x, instale PC/SC Lite 1.8.8.

```
yum install git flex autoconf automake libtool libudev-devel flex
git clone https://salsa.debian.org/rousseau/PCSC.git
cd PCSC
git checkout -b 1.8.8 pcsc-1.8.8
./bootstrap
./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix=
--disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --
```

```

sbindir=/usr/sbin
--sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64
--libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/
share/man
--infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
make
make install

```

- Para RHEL 6.x, instale PC/SC Lite 1.7.4.

```

yum groupinstall "Development tools"
yum install libudev-devel
service pcscd stop
wget https://alioth.debian.org/frs/download.php/file/3598/pcsc-lite-1.7.4.tar.bz2
tar -xjvf pcsc-lite-1.7.4.tar.bz2
cd ./pcsc-lite-1.7.4
./configure --prefix=/usr/ --libdir=/usr/lib64/ --enable-usbdropdir=/usr/lib64/pcsc/drivers
--enable-confdir=/etc --enable-ipcdir=/var/run --disable-libusb --disable-serial --disable-
usb
--disable-libudev
make
make install
service pcscd start

```

11 Instale el paquete Horizon Agent con el redireccionamiento de tarjetas inteligentes habilitado.

```
sudo ./install_viewagent.sh -m yes
```

Instale el paquete requerido para su distribución de RHEL:

- Para RHEL 7.x, instale Horizon Agent 7.8 o una versión posterior.
- Para RHEL 6.x, instale View Agent 6.2.1 o una versión posterior.

12 Reinicie el sistema y vuelva a iniciar sesión.

Configurar el redireccionamiento de tarjetas inteligentes para escritorios Ubuntu

Para configurar el redireccionamiento de tarjetas inteligentes para un escritorio Ubuntu, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas necesarias antes de instalar Horizon Agent.

Integrar escritorios Ubuntu con Active Directory para el redireccionamiento de tarjetas inteligentes

Para admitir el redireccionamiento de tarjetas inteligentes en un escritorio Ubuntu, integre el escritorio con un dominio de Active Directory (AD) mediante las soluciones Samba y Winbind.

Utilice el siguiente procedimiento para integrar un escritorio Ubuntu con un dominio de AD para el redireccionamiento de tarjetas inteligentes.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD
nombredelhost-ads.midominio.com	Nombre de dominio completo (FQDN) del servidor de AD
miservidordetiempo.miempresa.com	Nombre DNS del servidor de tiempo NTP
AdminUser	Nombre de usuario del administrador del escritorio Linux

Procedimiento

- 1 En el escritorio de Ubuntu, defina el nombre de host del escritorio editando el archivo de configuración `/etc/hostname`.
- 2 Configurar DNS.
 - a Agregue el nombre del servidor DNS y la dirección IP al archivo de configuración `/etc/hosts`.
 - b Agregue la dirección IP del servidor de nombres DNS y el nombre DNS de su dominio de AD al archivo de configuración `/etc/network/interfaces`, tal y como se muestra en el siguiente ejemplo.

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

- 3 Instale el paquete `resolvconf`.
 - a Ejecute el comando de instalación.

```
# apt-get install -y resolvconf
```

Permita que el sistema instale el paquete y se reinicie.

- b Compruebe la configuración de DNS en el archivo `//etc/resolve.conf`, tal y como se muestra en el siguiente ejemplo.

```
# cat /etc/resolve.conf
...
nameserver dns_IP_ADDRESS
search mydomain.com
```

4 Configure la sincronización de hora de red.

- a Instale el paquete de ntpdate.

```
# apt-get install -y ntpdate
```

- b Agregue la información del servidor NTP al archivo de configuración /etc/systemd/timesyncd.conf, tal y como se muestra en el siguiente ejemplo.

```
[Time]
NTP=mytimeserver.mycompany.com
```

5 Reinicie el servicio NTP.

```
sudo service ntpdate restart
```

6 Instale los paquetes de unión de AD necesarios.

- a Ejecute el comando de instalación.

```
# apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
libnss-winbind
```

- b En el mensaje de instalación que solicita el dominio Kerberos predeterminado, introduzca el nombre DNS de su dominio de AD en letras mayúsculas (por ejemplo, MIDOMINIO.COM). A continuación, seleccione **Aceptar**.

7 Edite el archivo de configuración /etc/krb5.conf, tal y como se muestra en el siguiente ejemplo.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MIDOMINIO.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MIDOMINIO.COM = {
        kdc = nombredelhost-ads.midominio.com
        admin_server = nombredelhost-ads.midominio.com
        default_domain = nombredelhost-ads.midominio.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = nombredelhost-ads.midominio.com
    }

[domain_realm]
    .midominio.com = MIDOMINIO.COM
    midominio.com = MIDOMINIO.COM
```

- 8 Para comprobar la certificación Kerberos, ejecute los siguientes comandos.

```
# kinit Administrator@MIDOMINIO.COM

# klist
```

Compruebe que los comandos devuelven un resultado similar al siguiente ejemplo.

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MIDOMINIO.COM Valid starting Expires
Service principal
2019-05-27T17:12:03 2019-05-28T03:12:03 krbtgt/MIDOMINIO.COM@MIDOMINIO.COM
renew until 2019-05-28T17:12:03
```

- 9 Edite el archivo de configuración `/etc/samba/smb.conf`, tal y como se muestra en el siguiente ejemplo.

```
[global]
    workgroup = MIDOMINIO
    realm = MIDOMINIO.COM
    password server = nombredelhost-ads.midominio.com
    security = ads
    kerberos method = secrets only
    winbind use default domain = true
    winbind offline logon = false
    template homedir = /home/%D/%U
    template shell = /bin/bash
    client use spnego = yes
    client ntlmv2 auth = yes
    encrypt passwords = yes
    passdb backend = tdbsam
    winbind enum users = yes
    winbind enum groups = yes
    idmap uid = 10000-20000
    idmap gid = 10000-20000
```

- 10 Únase al dominio de AD y compruebe la integración.

- a Ejecute los comandos de unión de AD.

```
# net ads join -U AdminUser@midominio.com
# systemctl stop samba-ad-dc
# systemctl enable smbd nmbd winbind
# systemctl restart smbd nmbd winbind
```

- b Modifique el archivo de configuración `/etc/nsswitch.conf`, tal como se muestra en el siguiente ejemplo.

```
passwd: compat systemd winbind
group: compat systemd winbind
shadow: compat
gshadow: files
```


- c Para comprobar el resultado de la unión a AD, ejecute los siguientes comandos y verifique que devuelven el resultado correcto.

```
# wbinfo -u

# wbinfo -g
```

- d Para comprobar Winbind Name Service Switch, ejecute los siguientes comandos y compruebe que devuelven el resultado correcto.

```
# getent group|grep 'domain admins'

# getent passwd|grep 'ads-hostname'
```

- 11 Habilite todos los perfiles de PAM.

```
# pam-auth-update
```

En la pantalla de configuración de PAM, seleccione todos los perfiles de PAM, incluido **Crear el directorio del usuario (home) al iniciar sesión** y, a continuación, seleccione **Aceptar**.

- 12 En Ubuntu 16.04, habilite el conmutador de usuario en la pantalla de inicio de sesión. Modifique el archivo `/usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf`, tal y como se muestra en el siguiente ejemplo.

```
user-session=ubuntu
greeter-show-manual-login=true
```

Pasos siguientes

[Configurar el redireccionamiento de tarjetas inteligentes en un escritorio Ubuntu](#)

Configurar el redireccionamiento de tarjetas inteligentes en un escritorio Ubuntu

Para configurar el redireccionamiento de tarjetas inteligentes en un escritorio Ubuntu, instale las bibliotecas de las que depende la función y el certificado de CA raíz para permitir la autenticación de confianza de las tarjetas inteligentes. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas

Valor del marcador de posición	Descripción
MIDDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD
nombredelhost-ads.midominio.com	Nombre de dominio completo (FQDN) del servidor de AD
miservidordetiempo.miempresa.com	Nombre DNS del servidor de tiempo NTP
AdminUser	Nombre de usuario del administrador del escritorio Linux

Requisitos previos

Integrar escritorios Ubuntu con Active Directory para el redireccionamiento de tarjetas inteligentes

Procedimiento

- 1 Instale las bibliotecas necesarias.

```
# apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 opensc
libengine-pkcs11-openssl libnss3-tools
```

- 2 Instale un certificado de una entidad de certificación (CA) raíz.

- a Descargue un certificado de CA raíz y guárdelo en su escritorio en /tmp/certificate.cer. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).
- b Busque el certificado de CA raíz que descargó y transfíralo a un archivo .pem.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c El comando certutil le permitirá instalar el certificado CA raíz en la base de datos del sistema /etc/pki/nssdb.

```
# certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d Copie el certificado de CA raíz en el directorio /etc/pam_pkcs11/cacerts.

```
# mkdir -p /etc/pam_pkcs11/cacerts

# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 Cree un archivo de hash pkcs11.

```
# chmod a+r certificate.pem
# pkcs11_make_hash_link
```

- 4 Copie los controladores requeridos y agregue los archivos de biblioteca necesarios al directorio nssdb.

- a Ejecute los siguientes comandos.

```
# cp libcmP11.so /usr/lib/
# mkdir -p /etc/pki/nssdb
# certutil -N -d /etc/pki/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pki/nssdb
# modutil -dbdir /etc/pki/nssdb/ -add "piv card 2.0" -libfile /usr/lib/libcmP11.so
```

- b Compruebe que el certificado esperado se cargó correctamente.

```
# certutil -L -d /etc/pki/nssdb

Certificate Nickname

rootca
```

- c Compruebe que las bibliotecas esperadas se agregaran correctamente.

```
modutil -dbdir /etc/pki/nssdb -list

Listing of PKCS #11 Modules
-----
1. NSS Internal PKCS #11 Module
   slots: 2 slots attached
   status: loaded

   slot: NSS Internal Cryptographic Services
   token: NSS Generic Crypto Services

   slot: NSS User Private Key and Certificate Services
   token: NSS Certificate DB

2. piv card 2.0
   library name: /usr/lib/libcmP11.so
   slots: There are no slots attached to this module
   status: loaded
-----
```

5 Configure la biblioteca pam_pkcs11.

- a Cree un archivo `pam_pkcs11.conf` con el contenido de ejemplo predeterminado.

```
# mkdir /etc/pam_pkcs11
# zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
tee /etc/pam_pkcs11/pam_pkcs11.conf
```

- b Edite el archivo `/etc/pam_pkcs11/pam_pkcs11.conf`, tal y como se muestra en el siguiente ejemplo.

```
use_pkcs11_module = mysc;

pkcs11_module mysc {
    module = /usr/lib/libcmP11.so;
    description = "LIBCMP11";
    slot_num = 0;
    ca_dir = /etc/pki/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca;
}
...
use_mappers = cn, null;
...
mapper cn {
    debug = false;
    module = internal;
    # module = /lib/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;
    # mapfile = "none";
}
```

- c Edite el archivo `/etc/pam_pkcs11/cn_map` para que incluya la siguiente línea.

```
nombredehost-ads -> nombredehost-ads
```

6 Configure la autenticación de PAM.

- a Edite el archivo de configuración `/etc/pam.d/gdm-password`. Coloque la línea de autorización `pam_pkcs11.so` antes de la línea `common-auth`, tal y como se muestra en el siguiente ejemplo.

```
##PAM-1.0
auth    requisite      pam_nologin.so
auth    required       pam_succeed_if.so user != root quiet_success
auth    sufficient
pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
@include common-account
```

- b En Ubuntu 16.04, edite el archivo de configuración `/etc/pam.d/lightdm`. Coloque la línea de autorización `pam_pkcs11.so` antes de la línea `common-auth`, tal y como se muestra en el siguiente ejemplo.

```
##PAM-1.0
auth    requisite      pam_nologin.so debug
auth    sufficient     pam_succeed_if.so user ingroup nopasswdlogin debug
auth    [success=3 default=ignore]    pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
auth    optional       pam_kwallet.so
```

- c En Ubuntu 16.04, edite el archivo de configuración `/etc/pam.d/unity`. Coloque la línea de autorización `pam_pkcs11.so` antes de la línea `common-auth`, tal y como se muestra en el siguiente ejemplo.

```
auth    [success=3 default=ignore]    pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
```

- 7 Para verificar el hardware de la tarjeta inteligente y los certificados instalados en ella, ejecute los siguientes comandos.

```
# pcsc_scan

# pkcs11_listcerts

# pkcs11_inspect
```

8 Configure el protector de protector de GNOME para que se bloquee cuando se extraiga la tarjeta inteligente.

- a Instale el paquete del protector de pantalla.

```
# apt-get install gnome-screensaver
```

- b Para configurar el protector de pan, edite el archivo `/etc/pam_pkcs11/pkcs11_eventmgr.conf`, tal y como se muestra en el siguiente ejemplo.

```
pkcs11_eventmgr {
    # Run in background? Implies debug=false if true
    daemon = true;

    # show debug messages?
    debug = false;

    # polling time in seconds
    polling_time = 1;

    # expire time in seconds
    # default = 0 ( no expire )
    expire_time = 0;

    # pkcs11 module to use
    pkcs11_module = /usr/lib/libcmP11.so;

    #
    # list of events and actions
    # Card inserted
    event card_insert {
        # what to do if an action fail?
        # ignore : continue to next action
        # return : end action sequence
        # quit : end program
        on_error = ignore ;

        # You can enter several, comma-separated action entries
        # they will be executed in turn
        action = "gnome-screensaver-command --poke";
    }

    # Card has been removed
    event card_remove {
        on_error = ignore;
        action = "gnome-screensaver-command --lock";
    }

    # Too much time card removed
    event expire_time {
```

```

    on_error = ignore;
    action = "/bin/false";
}
}

```

- c Ejecute `pkcs11_eventmgr`.

```
# /usr/bin/pkcs11_eventmgr &
```

- 9 Instale el paquete Horizon Agent con el redireccionamiento de tarjetas inteligentes habilitado.

```
# sudo ./install_viewagent.sh -m yes
```

Nota Debe instalar Horizon Agent 7.9 o una versión posterior.

- 10 Reinicie el sistema y vuelva a iniciar sesión.

Configurar el redireccionamiento de tarjetas inteligentes para escritorios SLED/SLES

Para configurar el redireccionamiento de tarjetas inteligentes para un escritorio SLED/SLES, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas necesarias antes de instalar Horizon Agent.

Integrar escritorios SLED/SLES con Active Directory para el redireccionamiento de tarjetas inteligentes

Para admitir el redireccionamiento de tarjetas inteligentes en un escritorio SLED/SLES, integre el escritorio con un dominio de Active Directory (AD) mediante las soluciones Samba y Winbind.

Utilice el siguiente procedimiento para integrar un escritorio SLED/SLES con un dominio de AD para el redireccionamiento de tarjetas inteligentes.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD
nombredelhost-ads.midominio.com	Nombre de dominio completo (FQDN) del servidor de AD

Valor del marcador de posición	Descripción
miservidordetiempo.miempresa.com	Nombre DNS del servidor de tiempo NTP
AdminUser	Nombre de usuario del administrador del escritorio Linux

Procedimiento

- 1 Configure los ajustes de red para el escritorio SLED/SLES.
 - a Para definir el nombre de host del escritorio, edite los archivos de configuración `/etc/hostname` y `/etc/hosts`.
 - b Configure la dirección IP del servidor DNS y deshabilite **DNS automático**. En SLES 12 SP3, deshabilite también **Cambiar nombre de host mediante DHCP**.
 - c Para configurar la sincronización de hora de red, agregue la información del servidor NTP al archivo `/etc/ntp.conf`, tal y como se muestra en el siguiente ejemplo.

```
server miservidordetiempo.miempresa.com
```

- 2 Instale los paquetes de unión de AD necesarios.

```
# zypper in krb5-client samba-winbind
```


3 Edite los archivos de configuración necesarios.

- a Edite el archivo `/etc/samba/smb.conf`, tal y como se muestra en el siguiente ejemplo.

```
[global]
    workgroup = MIDOMINIO
    usershare allow guests = NO
    idmap gid = 10000-20000
    idmap uid = 10000-20000
    kerberos method = secrets and keytab
    realm = MIDOMINIO.COM
    security = ADS
    template homedir = /home/%D/%U
    template shell = /bin/bash
    winbind use default domain=true
    winbind offline logon = yes
    winbind refresh tickets = yes
[homes]
    ...
```

- b Edite el archivo `/etc/krb5.conf`, tal y como se muestra en el siguiente ejemplo.

```
[libdefaults]
    default_realm = MIDOMINIO.COM
    clocks skew = 300

[realms]
    MIDOMINIO.COM = {
        kdc = nombredelhost-ads.midominio.com
        default_domain = midominio.com
        admin_server = nombredelhost-ads.midominio.com
    }

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[domain_realm]
    .midominio.com = MIDOMINIO.COM
    midominio.com = MIDOMINIO.COM

[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        minimum_uid = 1
    }
```

- c Edite el archivo `/etc/security/pam_winbind.conf`, tal y como se muestra en el siguiente ejemplo.

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

- d Edite el archivo `/etc/nsswitch.conf`, tal y como se muestra en el siguiente ejemplo.

```
passwd: compat winbind
group: compat winbind
```

- 4 Únase al dominio de AD, tal y como se muestra en el siguiente ejemplo.

```
# net ads join -U AdminUser
```

- 5 Habilite el servicio Winbind.

- a Para habilitar e iniciar Winbind, ejecute la siguiente secuencia de comandos.

```
# pam-config --add --winbind
# pam-config -a --mkhomedir
# systemctl enable winbind
# systemctl start winbind
```

- b Para asegurarse de que los usuarios de AD puedan iniciar sesión en el escritorio sin tener que reiniciar el servidor Linux, ejecute la siguiente secuencia de comandos.

```
# systemctl stop nscd
# nscd -i passwd
# nscd -i group
# systemctl start nscd
```

- 6 Para confirmar que se unió correctamente a AD, ejecute los siguientes comandos y compruebe que devuelven el resultado correcto.

```
# wbinfo -u

# wbinfo -g
```

Pasos siguientes

[Configurar el redireccionamiento de tarjetas inteligentes en un escritorio SLED/SLES](#)

Configurar el redireccionamiento de tarjetas inteligentes en un escritorio SLED/SLES

Para configurar el redireccionamiento de tarjetas inteligentes en un escritorio SLED/SLES, instale las bibliotecas de las que depende la función y el certificado de CA raíz para permitir la autenticación de confianza de las tarjetas inteligentes. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD
nombredelhost-ads.midominio.com	Nombre de dominio completo (FQDN) del servidor de AD
miservidordetiempo.miempresa.com	Nombre DNS del servidor de tiempo NTP
AdminUser	Nombre de usuario del administrador del escritorio Linux

Requisitos previos

Integrar escritorios SLED/SLES con Active Directory para el redireccionamiento de tarjetas inteligentes

Procedimiento

1 Instale los paquetes de biblioteca necesarios.

a Instale la biblioteca PAM y otros paquetes.

```
# zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools
pcsc-lite pcsc-ccid opensc coolkey pcsc-tools
```

b Para instalar las herramientas de PC/SC, ejecute la siguiente serie de comandos.

```
# SUSEConnect --list-extensions
# SUSEConnect -p PackageHub/12.3/x86_64
# zypper in pcsc-tools
```

2 Instale un certificado de una entidad de certificación (CA) raíz.

a Descargue un certificado de CA raíz y guárdelo en su escritorio en /tmp/certificate.cer. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).

b Busque el certificado de CA raíz que descargó, transféralo a un archivo .pem y cree un archivo hash.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
# chmod a+r /etc/pam_pkcs11/cacerts/certificate.pem
# cd /etc/pam_pkcs11/cacerts
# pkcs11_make_hash_link
```

- c Instale los anclajes de veracidad en la base de datos de NSS.

```
# mkdir /etc/pam_pkcs11/nssdb
# certutil -N -d /etc/pam_pkcs11/nssdb
# certutil -L -d /etc/pam_pkcs11/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

- d Instale los controladores necesarios.

```
# cp libcmP11.so /usr/lib64/
# modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pam_pkcs11/nssdb/
```

3 Edite el archivo /etc/pam_pkcs11/pam_pkcs11.conf.

- a Elimine la línea `use_pkcs11_module = nss`. En su lugar, agregue la línea `use_pkcs11_module = mysc`.
- b Agregue el módulo `mysc`, tal y como se muestra en el siguiente ejemplo.

```
pkcs11_module mysc {
    module = /usr/lib64/libcmP11.so;
    description = "MY Smartcard";
    slot_num = 0;
    nss_dir = /etc/pam_pkcs11/nssdb;
    cert_policy = ca, ocsp_on, signature, crl_auto;
}
```

- c Actualice la configuración del asignador de nombres comunes, tal y como se muestra en el siguiente ejemplo.

```
# Assume common name (CN) to be the login
mapper cn {
    debug = false;
    module = internal;
    # module = /usr/lib64/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;}
```

- d Elimine la línea `use_mappers = ms`. En su lugar, agregue la línea `use_mappers = cn, null`.

4 Edite el archivo de configuración /etc/pam_pkcs11/cn_map para que incluya la siguiente línea.

```
nombredehost-ads -> nombredehost-ads
```

5 Modifique la configuración PAM.

- a Para poder configurar la autenticación con tarjeta inteligente, deshabilite primero la herramienta `pam_config`.

```
# find /etc/pam.d/ -type l -iname "common-*" -delete
# for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
```

- b Cree un archivo llamado `common-auth-smartcard` en el directorio `/etc/pam.d/`. Agregue el siguiente contenido al archivo.

```
auth    required      pam_env.so
auth    sufficient    pam_pkcs11.so
auth    optional      pam_gnome_keyring.so
auth    [success=1 default=ignore] pam_unix.so nullok_secure try_first_pass
auth    required      pam_winbind.so use_first_pass
```

- c En SLED/SLES 12 SP3, reemplace la línea `auth include common-auth` por la línea `auth include common-auth-smartcard` en los archivos `/etc/pam.d/gdm` y `/etc/pam.d/xscreensaver`.

6 Deshabilite el firewall.

```
# rcSuSEfirewall2 stop
# chkconfig SuSEfirewall2_setup off
# chkconfig SuSEfirewall2_init off
```

Nota A veces se produce un error en el redireccionamiento de tarjetas inteligentes cuando el firewall está habilitado.

7 Instale los paquetes de biblioteca necesarios para el redireccionamiento de tarjetas inteligentes.

- a Para SLED/SLES 12 SP3, ejecute los siguientes comandos de instalación.

```
# SUSEConnect -p sle-sdk/12.3/x86_64
# zypper in git autoconf automake libtool flex libudev-devel gcc
```

- b En SLES 12 SP3, instale `systemd-devel`.

```
# zypper in systemd-devel
```

8 Instale el paquete Horizon Agent con el redireccionamiento de tarjetas inteligentes habilitado.

```
# sudo ./install_viewagent.sh -m yes
```

Nota Debe instalar Horizon Agent 7.9 o una versión posterior.

9 Reinicie el sistema y vuelva a iniciar sesión.

Configurar True SSO para escritorios Linux

La función True Single Sign-on (True SSO) permite a los usuarios acceder a un escritorio virtual Linux o a una aplicación o escritorio publicados después de iniciar sesión por primera vez en VMware Identity Manager. Los usuarios pueden iniciar sesión en VMware Identity Manager mediante una tarjeta inteligente, RSA SecurID o una autenticación RADIUS y, a continuación, acceder a los recursos remotos de Linux sin introducir sus credenciales de Active Directory.

Si un usuario se autentica con las credenciales de Active Directory (AD), la función True SSO no es necesaria. Sin embargo, puede configurar True SSO para que se utilice incluso en este caso, de manera que el escritorio pueda admitir tanto las credenciales de AD como de True SSO.

Cuando se conectan a un escritorio virtual Linux o a una aplicación o un escritorio publicados, los usuarios pueden elegir HTML Access u Horizon Client nativo.

True SSO tiene las siguientes limitaciones:

- La función solo se admite en escritorios con las siguientes distribuciones: RHEL/CentOS 8.0, RHEL/CentOS 7.x, Ubuntu 16.04 y 18.04, y SLED/SLES 12.x SP3.
- En los x escritorios RHEL/CentOS 7.x, la función solo se admite con los siguientes métodos de unión: las herramientas de predeterminadas de unión a dominio, Samba, System Security Services Daemon (SSSD) y el protocolo de autenticación de red de Kerberos.

Para configurar True SSO en su entorno Linux, realice las tareas siguientes.

- 1 Instale y configure True SSO en el entorno de Horizon 7. Consulte "Configuración de True SSO" en el documento *Administración de Horizon 7*.
- 2 Integre su escritorio con un dominio de AD, siguiendo el procedimiento de su distribución de Linux.
- 3 Configurar True SSO en el escritorio, siguiendo el procedimiento de su distribución de Linux.

Configurar True SSO en los escritorios RHEL/CentOS 8.0

Para admitir True SSO en un escritorio RHEL/CentOS 8.0, primero debe integrar el sistema con su dominio de Active Directory (AD). A continuación, debe modificar algunas configuraciones en el sistema para admitir la función True SSO.

Nota True SSO no se admite en escritorios RHEL 8.0 de clones instantáneos.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
MIDOMINIO	Nombre del dominio NetBIOS

Requisitos previos

- Compruebe que el servidor de Active Directory (AD) se puede resolver mediante el DNS en el sistema RHEL/CentOS 8.0.
- Configure el nombre de host del sistema.
- Configure el protocolo de tiempo de redes (NTP) en el sistema.

Procedimiento

- 1 En el sistema RHEL/CentOS 8.0, compruebe la conexión de red con Active Directory.

```
# realm discover midominio.com
```

- 2 Instale los paquetes de dependencia necesarios.

```
# yum install oddjob oddjob-mkhomedir sssd adcli samba-common-tools
```

- 3 Únase al dominio de AD.

```
# realm join --verbose midominio.com -U administrator
```

- 4 Descargue el certificado de CA raíz y cópielo en el directorio requerido como un archivo .pem.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem

# cp /tmp/certificate.pem /etc/sssdpki/sssdpki_auth_ca_db.pem
```

- 5 Modifique el archivo de configuración /etc/sssdpki/sssdpki.conf, tal como se muestra en el siguiente ejemplo.

```
[sssdpki]
domains = midominio.com
config_file_version = 2
services = nss, pam

[domain/mydomain.com]
ad_domain = midominio.com
krb5_realm = IMIDOMINIO.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False      <----- Use short name for user
fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred  <----- Add this line for SSO

[pam]                                <----- Add pam section for certificate logon
pam_cert_auth = True                 <----- Add this line to enable certificate
logon for system
```

```
pam_p11_allowed_services = +gdm-vmwcred <----- Add this line to enable certificate
logon for VMware Horizon Agent

[certmap/midominio.com/truesso] <----- Add this section and following lines
to set match and map rule for certificate user
matchrule = <EKU>msScLogin
maprule = (|(userPrincipal={subject_principal}))(samAccountName={subject_principal.short_name}))
domains = midominio.com
priority = 10
```

- 6 Instale el paquete Horizon Agent con True SSO habilitado.

Nota Debe instalar Horizon Agent 7.11 o una versión posterior.

```
# sudo ./install_viewagent.sh -T yes
```

- 7 Modifique el archivo de configuración `/etc/vmware/viewagent-custom.conf` para que incluya la siguiente línea.

```
NetbiosDomain = MIDOMINIO
```

- 8 Reinicie el sistema y vuelva a iniciar sesión.

Configurar True SSO para escritorios RHEL/CentOS 7.x

Para configurar True SSO para un escritorio RHEL/CentOS 7.x, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas requeridas antes de instalar Horizon Agent.

Integrar un escritorio RHEL/CentOS 7.x con Active Directory para True SSO

Para admitir True SSO en una máquina virtual de clones instantáneos en un entorno de escritorios de Horizon 7 para Linux de un sistema RHEL/CentOS 7.x, configure Samba en la máquina virtual principal Linux.

La función `realmd` de RHEL/CentOS 7.x proporciona una manera sencilla de detectar y unir dominios de identidad. En lugar de conectar el sistema al dominio en sí, `realmd` configura los servicios del sistema Linux subyacentes, como SSSD o Winbind, para que se conecten al dominio. A continuación se indica cómo usar `realmd` y Samba para realizar una unión de dominio sin conexión de un escritorio RHEL/CentOS 7.x a Active Directory.

Requisitos previos

- El sistema RedHat Enterprise Linux (RHEL) está suscrito a Red Hat Network (RHN) o tiene la herramienta yum instalada de forma local.
- El DNS puede resolver el servidor de Active Directory (AD) en el sistema Linux.
- El protocolo de tiempo de redes (NTP) está configurado en el sistema Linux.

Procedimiento

- 1 Compruebe que el sistema RHEL o CentOS puede detectar el servidor de AD. Utilice el siguiente ejemplo, donde *ADdomain.example.com* debe reemplazarse con la información del servidor de AD.

```
sudo realm discover ADdomain.example.com
```

- 2 Instale el paquete Samba `tdb-tools`.

El paquete Samba `tdb-tools` no está disponible para su descarga en el repositorio oficial de Red Hat. Debe descargarlo manualmente. Por ejemplo, puede utilizar el comando siguiente para descargarlo desde un sistema CentOS 7.5 e instalar el paquete descargado en su sistema RHEL.

```
yumdownloader tdb-tools
```

Si no dispone de un sistema CentOS, vaya a <https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+...&system=&arch=>, descargue el paquete `tdb-tools-1.3.15-1.el7.x86_64.rpm` e instálelo en el sistema RHEL.

- 3 Instale Samba y los paquetes de dependencia.

```
sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client krb5-workstation
```

- 4 Ejecute el comando `join` con la ayuda del ejemplo siguiente, donde *DNSdomain.example.com* deberá reemplazarse por la ruta de acceso al dominio DNS específico de su entorno.

```
sudo realm join DNSdomain.example.com -U administrator
```

Cuando el comando de unión se ejecuta correctamente, recibirá el mensaje siguiente.

```
La máquina se inscribió correctamente en realm
```

- 5 Reinicie el sistema y vuelva a iniciar sesión.

Pasos siguientes

[Configurar True SSO en los escritorios RHEL/CentOS 7.x](#)

Configurar True SSO en los escritorios RHEL/CentOS 7.x

Para habilitar la función True SSO en un escritorio RHEL/CentOS 7.x, instale las bibliotecas de las que depende la función True SSO, el certificado de CA raíz para poder usar la autenticación de confianza, y Horizon Agent. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Utilice el siguiente procedimiento para habilitar True SSO en escritorios RHEL 7.x y CentOS 7.x. Para soportar True SSO en estos escritorios, debe instalar Horizon Agent 7.6 o una versión posterior.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de DNS de su dominio de AD. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
servidor_dns	Ruta de acceso a su servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas

Requisitos previos

- Configure True SSO para VMware Identity Manager y Horizon Connection Server.
- [Integrar un escritorio RHEL/CentOS 7.x con Active Directory para True SSO](#)
- Obtenga un certificado raíz firmado por una entidad de certificación y guárdelo en la carpeta /tmp/certificate.cer de su escritorio RHEL/CentOS 7.x. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).

Procedimiento

- 1 Instale el grupo de paquete de soporte PKCS11.

```
yum install -y nss-tools nss-pam-ldapd pam_krb5 krb5-libs krb5-workstation krb5-pkinit
```

- 2 Instale un certificado de una entidad de certificación (CA) raíz.

- a Busque el certificado de CA raíz que descargó y transfíralo a un archivo .pem.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b El comando certutil le permitirá instalar el certificado CA raíz en la base de datos del sistema /etc/pki/nssdb.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Agregue el certificado CA raíz a la lista de certificados CA de confianza del sistema RHEL o CentOS 7.x y actualice la configuración del almacén de confianza de todo el sistema mediante el comando update-ca-trust.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
update-ca-trust
```

- 3 Modifique la sección correspondiente en el archivo de configuración SSSD de su sistema, tal como se muestra en este ejemplo.

```
[domain/midominio.com]
ad_domain = midominio.com
krb5_realm = MIDOMINIO.COM
```

```
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

- 4 Modifique el archivo de configuración de Kerberos `/etc/krb5.conf/`, tal y como se muestra en el ejemplo siguiente.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_ccache_name = KEYRING:persistent:%{uid}
    # Add following line, if the system doesn't add it automatically
    default_realm = MIDOMINIO.COM

[realms]
MIDOMINIO.COM = {
    kdc = servidor_dns
    admin_server = servidor_dns
    # Add the following three lines for pkinit_*
    pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
    pkinit_kdc_hostname = servidor_DNS_de_tu_organización
    pkinit_eku_checking = kpServerAuth
}

[domain_realm]
    midominio.com = MIDOMINIO.COM
    .midominio.com = MIDOMINIO.COM
```

- 5 Instale el paquete Horizon Agent con True SSO habilitado.

```
sudo ./install_viewagent.sh -T yes
```

Nota Debe instalar Horizon Agent 7.6 o una versión posterior.

- 6 Agregue el siguiente parámetro al archivo de configuración personalizada de Horizon Agent `/etc/vmware/viewagent-custom.conf`. Utilice el siguiente ejemplo, donde `NOMBRE_NETBIOS_DEL_DOMINIO` es el nombre de NetBIOS del dominio de su organización.

```
NetbiosDomain=NOMBRE_NETBIOS_DEL_DOMINIO
```

- 7 Reinicie el sistema y vuelva a iniciar sesión.

Configurar True SSO para escritorios Ubuntu

Para configurar True SSO para un escritorio Ubuntu, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas requeridas antes de instalar Horizon Agent.

Integrar escritorios Ubuntu con Active Directory para True SSO

Para admitir True SSO en un escritorio Ubuntu 16.04 o 18.04, integre el escritorio con un dominio de Active Directory mediante las soluciones Samba y Winbind.

Utilice el siguiente procedimiento para integrar un escritorio Ubuntu 16.04 o 18.04 en un dominio AD.

Algunos ejemplos incluidos en el procedimiento utilizan valores de marcador de posición para representar entidades en su configuración de red, como el nombre de host de su escritorio Ubuntu. Reemplace los valores de marcador de posición con información específica de su configuración, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
DIRECCIÓN_IP_dns	Dirección IP del servidor de nombres DNS
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD, en mayúsculas
mihost	Nombre del host de su escritorio Ubuntu
MIDOMINIO	Nombre DNS del grupo de trabajo o el dominio NT que incluye su servidor Samba, en mayúsculas
nombredelhost-ads	Nombre de host del servidor de AD
usuario-admin	Nombre de usuario del administrador del dominio de AD

Requisitos previos

- El DNS puede resolver el servidor de Active Directory (AD) en el sistema Linux.
- El protocolo de tiempo de redes (NTP) está configurado en el sistema Linux.

Procedimiento

- 1 En su escritorio Ubuntu 16.04 o 18.04, instale los paquetes samba y winbind.

```
sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

- 2 Cuando se le solicite, configure las opciones de autenticación de Kerberos tal como se muestra a continuación.
 - a En **Reino predeterminado de la versión 5 de Kerberos**, introduzca el nombre de DNS de su dominio de AD en mayúsculas.

Por ejemplo, si el nombre del dominio de AD es **midominio.com**, introduzca **MIDOMINIO.COM**.
 - b En **Servidores de Kerberos para su reino**, introduzca el nombre de host de su servidor AD (representado como **nombrehost_ads** en los ejemplos de este procedimiento).
 - c En **Servidor administrativo para su reino de Kerberos**, introduzca de nuevo el nombre de host de su servidor AD.

3 Actualice la configuración PAM.

- a Abra la página de configuración de PAM.

```
pam-auth-update
```

- b Seleccione **Crear el directorio del usuario (home) al iniciar sesión** y, a continuación, seleccione **Aceptar**.

4 Edite el archivo de configuración `/etc/nsswitch.conf`, tal como se muestra en el ejemplo siguiente.

```
passwd: compat winbind
group:  compat winbind
shadow: compat
gshadow: files
```

- 5 Para asegurarse de que el archivo generado automáticamente `resolv.conf` hace referencia a su dominio de AD como un dominio de búsqueda, edite la opción NetworkManager con la conexión de su sistema.
 - a Abra el panel de control de NetworkManager y desplácese a **Ajustes de IPv4** de la conexión de su sistema. En Método, seleccione **Solo direcciones automáticas (DHCP)**. En **Servidores DNS**, introduzca la dirección IP de su servidor DNS (representado como `DIRECCIÓN_IP_dns` en los ejemplos de este procedimiento). A continuación, haga clic en **Guardar**.
 - b Edite el archivo de configuración de la conexión de su sistema, que se encuentra en `/etc/NetworkManager/system-connections`. Utilice el siguiente ejemplo.

```
[ipv4]
dns=DIRECCIÓN_IP_dns
dns-search=midominio.com
ignore-auto-dns=true
method=auto
```

Nota Cuando se crea un nuevo escritorio virtual de clones instantáneos, se añade un nuevo adaptador de red virtual. Cualquier ajuste del adaptador de red (por ejemplo, el servidor DNS) que aparezca en la plantilla del escritorio virtual, se perderá cuando se añade el nuevo adaptador de red al escritorio virtual de clones instantáneos. Para evitar que se pierda la configuración del servidor DNS al añadir el nuevo adaptador de red a un escritorio virtual clonado, deberá especificar un servidor DNS en su sistema Linux.

- c Especifique el servidor DNS editando el archivo de configuración `/etc/resolv.conf`, tal y como se muestra en el ejemplo siguiente.

```
nameserver DIRECCIÓN_IP_dns

search midominio.com
```

- d Reinicie el sistema y vuelva a iniciar sesión.

- 6 Edite el archivo de configuración `/etc/hosts`, tal y como se muestra en el ejemplo siguiente.

```
127.0.0.1    localhost
127.0.1.1    mihost.midominio.com mihost
```

- 7 Edite el archivo de configuración `/etc/samba/smb.conf`, tal y como se muestra en el ejemplo siguiente.

```
[global]
security = ads
realm = MIDOMINIO.COM
workgroup = MIDOMINIO
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
```

```
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

8 Reinicie el servicio smbd.

```
sudo systemctl restart smbd.service
```

9 Edite el archivo de configuración /etc/krb5.conf de manera que tenga un contenido similar al del ejemplo siguiente.

```
[libdefaults]
    default_realm = MIDOMINIO.COM
    dns_lookup_realm = true
    dns_lookup_kdc = true

[realms]
    MIDOMINIO.COM = {
        kdc = nombredelhost-ads
        admin_server = nombredelhost-ads
    }

[domain_realm]
    .midominio.com = MIDOMINIO.COMmidominio.com = MIDOMINIO.COM
```

10 Una su escritorio Ubuntu al dominio de AD.

a Inicie un ticket de Kerberos.

```
sudo kinit admin-user
```

Cuando se le solicite, introduzca su contraseña de administrador.

b Compruebe que el ticket se ha creado correctamente.

```
sudo klist
```

Este comando le permitirá consultar información sobre el ticket, incluida la fecha de inicio válida y la fecha de expiración.

c Cree un archivo keytab de Kerberos.

```
sudo net ads keytab create -U admin-user
```

d Únase al dominio de AD.

```
sudo net ads join -U admin-user
```

11 Reinicie y verifique el servicio Winbind.

- a Reinicie el servicio Winbind.

```
sudo systemctl restart winbind.service
```

- b Para verificar el servicio Winbind, ejecute los siguientes comandos y compruebe que devuelven el resultado correcto.

- `wbinfo -u`
- `wbinfo -g`
- `getend passwd`
- `getend group`

12 Reinicie el sistema y vuelva a iniciar sesión.**Pasos siguientes**

[Configurar True SSO en escritorios Ubuntu](#)

Configurar True SSO en escritorios Ubuntu

Para habilitar la función True SSO en un escritorio Ubuntu 16.04 o 18.04, instale las bibliotecas de las que depende la función True SSO, el certificado de CA raíz para poder usar la autenticación de confianza, y Horizon Agent. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Utilice el siguiente procedimiento para habilitar True SSO en escritorios Ubuntu 16.04 y 18.04. Para soportar True SSO en estos escritorios, debe instalar Horizon Agent 7.8 o una versión posterior.

Requisitos previos

- Configure True SSO para VMware Identity Manager y Horizon Connection Server.
- [Integrar escritorios Ubuntu con Active Directory para True SSO](#)
- Obtenga un certificado raíz firmado por una entidad de certificación y guárdelo en la carpeta `/tmp/certificate.cer` de su escritorio. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).

Procedimiento

- 1 En su escritorio Ubuntu 16.04 o 18.04, instale el paquete de soporte pkcs11.

```
sudo apt install libpam-pkcs11
```

- 2 Instale el paquete para libnss3-tools.

```
sudo apt install libnss3-tools
```


3 Instale un certificado de una entidad de certificación (CA) raíz.

- a Busque el certificado de CA raíz que descargó y transfíralo a un archivo .pem.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b El comando certutil le permitirá instalar el certificado CA raíz en la base de datos del sistema /etc/pki/nssdb.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Copie el certificado de CA raíz en el directorio /etc/pam_pkcs11/cacerts.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- d Cree un vínculo hash para el certificado de CA raíz. En el directorio /etc/pam_pkcs11/cacerts, ejecute el siguiente comando.

```
pkcs11_make_hash_link
```

4 Instale el paquete Horizon Agent con True SSO habilitado.

```
sudo ./install_viewagent.sh -T yes
```

Nota Para utilizar la función True SSO, debe instalar Horizon Agent 7.8 o una versión posterior.

- 5 Agregue el siguiente parámetro al archivo de configuración personalizada de Horizon Agent/etc/vmware/viewagent-custom.conf. Utilice el siguiente ejemplo, donde *NOMBRE_NETBIOS_DEL_DOMINIO* es el nombre de NetBIOS del dominio de su organización.

```
NetbiosDomain=NOMBRE_NETBIOS_DEL_DOMINIO
```

6 Edite el archivo de configuración /etc/pam_pkcs11/pam_pkcs11.conf.

- a Si es necesario, cree el archivo de configuración /etc/pam_pkcs11/pam_pkcs11.conf. Busque el archivo de ejemplo en /usr/share/doc/libpam-pkcs11/examples, cópielo en el directorio /etc/pam_pkcs11 y cámbiele el nombre por pam_pkcs11.conf. Añada la información de su sistema al contenido del archivo según sea necesario.
- b Modifique el archivo de configuración /etc/pam_pkcs11/pam_pkcs11.conf para que incluya contenido similar al siguiente ejemplo.

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
    module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
}
```

7 Modifique los parámetros auth en el archivo de configuración PAM.

- a Abra el archivo de configuración PAM.
 - En Ubuntu 16.04, abra /etc/pam.d/lightdm.
 - En Ubuntu 18.04, abra /etc/pam.d/gdm-vimwcred.
- b Edite el archivo de configuración PAM, tal y como se muestra en el ejemplo siguiente.

```
auth requisite pam_vimw_cred.so
auth sufficient pam_pkcs11.so try_first_pass
```

8 Reinicie el sistema y vuelva a iniciar sesión.

Configurar True SSO para escritorios SLED/SLES

Para configurar True SSO para un escritorio SLED/SLES, primero integre el escritorio con un dominio de Active Directory. A continuación, instale el certificado de CA raíz y las bibliotecas requeridas antes de instalar Horizon Agent.

Integrar un escritorio SLED/SLES con Active Directory para True SSO

Para que True SSO se admita en un escritorio SLED 12.x SP3 o SLES 12.x SP3, integre el escritorio con un dominio de Active Directory usando las soluciones Samba y Winbind.

Utilice el siguiente procedimiento para integrar un escritorio SLED/SLES con un dominio de AD.

Requisitos previos

- El DNS puede resolver el servidor de Active Directory (AD) en el sistema Linux.
- El protocolo de tiempo de redes (NTP) está configurado en el sistema Linux.

Procedimiento

1 En el escritorio SLED/SLES, instale los paquetes samba y winbind.

```
zypper install samba-winbind krb5-client samba-winbind-32bit
```

2 Abra la herramienta de configuración YaST y desplácese hasta **Configuración de red > Pertenencia a dominio de Windows**.

3 En la pantalla Pertenencia a dominio de Windows, configure las opciones del siguiente modo.

- a En **Dominio o grupo de trabajo**, escriba el nombre DNS del grupo de trabajo o dominio NT que incluye su servidor Samba, en mayúsculas. Por ejemplo, si el nombre de su grupo de trabajo es **midominio**, introduzca **MIDOMINIO**.
- b Seleccione **Usar la información SMB para la autenticación de Linux**.
- c Seleccione **Crear el directorio del usuario (home) al iniciar sesión**.
- d Seleccione **Autenticación sin conexión**.
- e Seleccione **Single Sign-On para SSH**.

- 4 En el mensaje que pregunta si desea unirse al dominio, seleccione **Sí**.
- 5 Introduzca el nombre del administrador y la contraseña del grupo de trabajo especificado y seleccione **Aceptar**.

Aparecerá un mensaje que confirma que el escritorio SLED/SLES se unió al dominio correctamente. Seleccione **Aceptar**.
- 6 Edite el archivo de configuración de `/etc/samba/smb.conf` para que incluya el siguiente parámetro.

```
[global]
...
winbind use default domain = yes
```

- 7 Reinicie el sistema y vuelva a iniciar sesión.
- 8 Pruebe y verifique la integración de su escritorio SLED/SLES.

Ejecute los siguientes comandos de prueba y compruebe que devuelven el resultado correcto. Sustituya `mydomain` con el nombre del grupo de trabajo de su servidor Samba o dominio NT.
 - `net ads testjoin`
 - `net ads info`
 - `wbinfo --krb5auth=mydomain\\open%open`
 - `ssh localhost -l mydomain\\open`

Pasos siguientes

[Configurar True SSO en escritorios SLED/SLES](#)

Configurar True SSO en escritorios SLED/SLES

Para habilitar la función True SSO en un escritorio SLED/SLES 12.x SP3, instale las bibliotecas de las que depende la función True SSO, el certificado de CA raíz para poder usar la autenticación de confianza, y Horizon Agent. Además, debe editar algunos archivos de configuración para completar la configuración de autenticación.

Utilice el siguiente procedimiento para habilitar True SSO en escritorios SLED 12.x SP3 y SLES 12.x SP3. Para soportar True SSO en estos escritorios, debe instalar Horizon Agent 7.8 o una versión posterior.

Requisitos previos

- Configure True SSO para VMware Identity Manager y Horizon Connection Server.
- [Integrar un escritorio SLED/SLES con Active Directory para True SSO](#)
- Obtenga un certificado raíz firmado por una entidad de certificación y guárdelo en la carpeta `/tmp/certificate.cer` de su escritorio SLED/SLES 12.x SP3. Consulte la sección [Cómo exportar el certificado raíz firmado por una entidad de certificación](#).

Procedimiento

- 1 Para escritorios SLES 12.x SP3, instale los paquetes necesarios ejecutando el siguiente comando.

```
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- 2 Para escritorios SLED 12.x SP3, instale los paquetes necesarios siguiendo estos pasos.

- a Descargue un archivo .iso SLES en el disco local del escritorio SLED (por ejemplo, /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso).

Debe añadir el archivo .iso SLES como origen de paquete de tu escritorio SLED, ya que el paquete necesario `krb5-plugin-preauth-pkinit` solo está disponible para sistemas SLES.

- b Monte el archivo .iso SLES en su escritorio SLED e instale los paquetes necesarios.

```
sudo mkdir -p /mnt/sles
sudo mount -t iso9660 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso /mnt/sles
sudo zypper ar -f /mnt/sles sles
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- c Una vez completada la instalación, desmonte el archivo .iso SLES.

```
sudo umount /mnt/sles
```

- 3 Instale un certificado de una entidad de certificación (CA) raíz.

- a Busque el certificado de CA raíz que descargó y transfíralo a un archivo .pem.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b El comando `certutil` le permitirá instalar el certificado CA raíz en la base de datos del sistema `/etc/pki/nssdb`.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Añada el certificado de CA raíz a `pam_pkcs11`.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

- 4 Edite el archivo de configuración `/etc/krb5.conf` de manera que tenga un contenido similar al del ejemplo siguiente.

```
[libdefaults]
    default_realm = MIDOMINIO.COM
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
```

```

MIDOMINIO.COM = {
    kdc = nombredelhost-ads
    admin_server = nombredelhost-ads
    pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
    pkinit_kdc_hostname = nombredelhost-ads
    pkinit_eku_checking = kpServerAuth
}

[domain_realm]
.midominio.com = MIDOMINIO.COMmidominio.com = MIDOMINIO.COM

```

Reemplace los valores de marcador de posición del ejemplo con información específica de su configuración de red, tal y como se describe en la siguiente tabla.

Valor del marcador de posición	Descripción
midominio.com	Nombre DNS de su dominio de AD
MIDOMINIO.COM	Nombre DNS de su dominio de AD (en mayúsculas)
nombredelhost-ads	Nombre de host del servidor de AD (distingue entre mayúsculas y minúsculas)

5 Instale el paquete Horizon Agent con True SSO habilitado.

```
sudo ./install_viewagent.sh -T yes
```

Nota Para utilizar la función True SSO, debe instalar Horizon Agent 7.8 o una versión posterior.

6 Agregue el siguiente parámetro al archivo de configuración personalizada de Horizon Agent/etc/vmware/viewagent-custom.conf. Utilice el siguiente ejemplo, donde *NOMBRE_NETBIOS_DEL_DOMINIO* es el nombre de NetBIOS del dominio de su organización.

```
NetbiosDomain=NOMBRE_NETBIOS_DEL_DOMINIO
```

7 Reinicie el sistema y vuelva a iniciar sesión.

Configurar gráficos para escritorios Linux

4

Puede configurar las distribuciones admitidas actualmente de Linux para aprovechar las funciones de NVIDIA en el host ESXi o en un sistema operativo invitado.

Requisitos de clonación de máquinas virtuales para configurar gráficos 3D

Debe tener en cuenta los siguientes requisitos para la clonación de máquinas virtuales antes de configurar los gráficos 3D.

- Para vGPU, complete la configuración de gráficos en la máquina virtual de base. Clone las máquinas virtuales. La configuración de gráficos funciona para las máquinas virtuales clonadas y no se necesita otra configuración.
- Para vDGA, complete la configuración de gráficos en la máquina virtual de base. Clone las máquinas virtuales. Sin embargo, antes de encender las máquinas virtuales clonadas, debe eliminar el dispositivo PCI pass-through de NVIDIA existente de la máquina virtual clonada y agregar un nuevo dispositivo PCI pass-through de NVIDIA a la máquina virtual clonada. Las máquinas virtuales no pueden compartir un mismo dispositivo PCI pass-through de NVIDIA. Cada máquina virtual usa un dispositivo PCI pass-through de NVIDIA dedicado.

Este capítulo incluye los siguientes temas:

- [Configurar las distribuciones de Linux compatibles con vGPU](#)
- [Configurar RHEL 6.x para vDGA](#)

Configurar las distribuciones de Linux compatibles con vGPU

Puede configurar una distribución de Linux compatible para aprovechar las funciones de NVIDIA vGPU (aceleración de hardware de GPU compartida) en el host ESXi.

Debe usar el controlador de pantalla para VM Linux de NVIDIA que corresponda al controlador de la GPU del host ESXi (.vib). Visite el sitio web de NVIDIA para obtener información sobre los paquetes de controladores.

Nota Para obtener información sobre las tarjetas gráficas NVIDIA y las distribuciones Linux que admiten vGPU, consulte <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

Precaución Antes de comenzar, compruebe que Horizon Agent no esté instalado en la máquina virtual Linux. Si instala Horizon Agent antes de configurar la máquina para usar NVIDIA vGPU, se sobrescriben los parámetros de configuración del archivo `xorg.conf` y no funciona NVIDIA vGPU. Debe instalar Horizon Agent una vez que se haya completado la configuración de NVIDIA vGPU.

Instalar el VIB de la tarjeta gráfica NVIDIA GRID vGPU en el host ESXi

Debe descargar e instalar el VIB para su tarjeta gráfica NVIDIA GRID en la versión 6.0 U1 o posteriores del host ESXi.

NVIDIA proporciona un paquete de software vGPU con un administrador de vGPU que se instala en el host ESXi en este procedimiento, y un controlador de visualización de Linux, que instalará en una máquina virtual Linux en un procedimiento posterior a este.

Requisitos previos

- Verifique que tenga instalado vSphere 6.0 U1 o una versión posterior en su entorno.
- Compruebe que la tarjeta gráfica de vGPU requerida esté instalada en el host ESXi.

Nota Para obtener información sobre las tarjetas gráficas NVIDIA y las distribuciones Linux que admiten vGPU, consulte <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

Procedimiento

- 1 Descargue el VIB para su tarjeta gráfica NVIDIA GRID vGPU desde el sitio [Descarga de controladores NVIDIA](#).

Seleccione la versión apropiada del VIB de los menús desplegables de NVIDIA.

Opción	Descripción
Tipo de producto	GRID
Serie del producto	Seleccione NVIDIA GRID vGPU .
Producto	Seleccione la versión (por ejemplo: GRID K2) que está instalada en el host ESXi.
Sistema operativo	Seleccione la versión de VMware vSphere ESXi.

- 2 Descomprima el archivo .zip que contiene el paquete de software vGPU.

- 3 Cargue la carpeta del administrador de vGPU en el host ESXi.

Nota Instalará el controlador de visualización de Linux en la máquina virtual Linux en un procedimiento posterior a este.

- 4 Apague o suspenda todas las máquinas virtuales del host ESXi.
- 5 Conecte el host ESXi mediante SSH.
- 6 Detenga el servicio xorg.

```
# /etc/init.d/xorg stop
```

- 7 Instale el VIB de NVIDIA.

Por ejemplo:

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

- 8 Reinicie o actualice el host ESXi.

- ◆ Para un host ESXi instalado, reinicie el host.
- ◆ Para un host ESXi sin cortafuegos, siga los siguientes pasos para actualizar el host. (Estos pasos también funcionan en un host instalado.)

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

- 9 Verifique que el servicio xorg esté ejecutándose después de que el host se reinicie.

Configurar un dispositivo PCI compartido para vGPU en la máquina virtual Linux

Para usar NVIDIA vGPU, debe configurar un dispositivo PCI compartido para la máquina virtual Linux.

Requisitos previos

- Compruebe que la máquina virtual Linux esté preparada para usarse como escritorio. Consulte [Crear una máquina virtual e instalar Linux](#) y [Preparar una máquina Linux para la implementación de escritorios remotos](#).
- Compruebe que Horizon Agent no esté instalado en la máquina virtual Linux.

- Compruebe que esté instalado NVIDIA VIB en el host ESXi. Consulte [Instalar el VIB de la tarjeta gráfica NVIDIA GRID vGPU en el host ESXi](#).
- Familiarícese con los tipos de GPU virtuales disponibles con NVIDIA vGPU, que selecciona con el ajuste **Perfil de GPU**. Los tipos de GPU virtuales proporcionan diversas capacidades en las GPU físicas instaladas en el host ESXi.

Nota Para obtener información sobre las tarjetas gráficas NVIDIA y las distribuciones Linux que admiten vGPU, consulte <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

Procedimiento

- 1 Apague la máquina virtual.
- 2 En vSphere Web Client, seleccione la máquina virtual y en la pestaña **Hardware de VM** haga clic en **Editar configuración**.
- 3 En el menú **Nuevo dispositivo**, seleccione **Dispositivo PCI compartido**.
- 4 Haga clic en **Agregar** y seleccione **NVIDIA GRID vGPU** desde el menú desplegable.
- 5 Para la opción **Perfil de GPU**, seleccione un tipo de GPU virtual desde el menú desplegable.
- 6 Haga clic en **Reservar toda la memoria** y haga clic en **Aceptar**.

Debe reservar toda la memoria de máquina virtual para que la GPU sea compatible con NVIDIA GRID vGPU.

- 7 Encienda la máquina virtual.

Instalar el controlador de visualización NVIDIA GRID vGPU

Para instalar el controlador de visualización NVIDIA GRID vGPU, debe deshabilitar el controlador NVIDIA predeterminado, descargar los controladores de visualización NVIDIA y configurar el dispositivo PCI en la máquina virtual.

Requisitos previos

- Verifique que descargó el paquete de software vGPU del sitio de descargas de NVIDIA, descomprimió el paquete y tiene listo el controlador de visualización de Linux (un componente del paquete). Consulte [Instalar el VIB de la tarjeta gráfica NVIDIA GRID vGPU en el host ESXi](#).

Verifique también que se agregó un dispositivo PCI compartido a la máquina virtual. Consulte [Configurar un dispositivo PCI compartido para vGPU en la máquina virtual Linux](#).

Procedimiento

- 1 Copie el controlador de visualización de Linux de NVIDIA a la máquina virtual.
- 2 Abra un terminal remoto a la máquina virtual o cambie a una consola de texto pulsando Control+Alt+F2, inicie sesión en la raíz y ejecute el comando `init 3` para deshabilitar Windows X.

- 3 Instale los componentes adicionales necesarios para el controlador NVIDIA.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 4 Agregue un marcador ejecutable al paquete de controladores NVIDIA GRID vGPU.

```
chmod +x NVIDIA-Linux-x86_64-versión-grid.run
```

- 5 Inicie el programa instalador de NVIDIA GRID vGPU.

```
sudo ./NVIDIA-Linux-x86_64-versión-grid.run
```

- 6 Acepte el contrato de licencia del software NVIDIA y seleccione **Sí** para actualizar automáticamente las opciones de configuración X.

Pasos siguientes

Instalar Horizon Agent en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).

Cree un grupo de escritorios que contenga las máquinas virtuales Linux configuradas. Consulte [Crear un grupo de escritorios manual para Linux](#).

Verificar que el controlador de pantalla NVIDIA está instalado

Puede verificar que el controlador de pantalla NVIDIA esté instalado en una máquina virtual Linux si muestra la salida del controlador NVIDIA de una sesión de escritorio de Horizon.

Requisitos previos

- Verifique que instaló el controlador de pantalla NVIDIA.
- Compruebe que Horizon Agent esté instalado en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- Verifique que la máquina virtual Linux esté implementada en un grupo de escritorios. Consulte [Crear un grupo de escritorios manual para Linux](#).

Procedimiento

- 1 Reinicie la máquina virtual Linux.

El script de inicio de Horizon Agent inicia el servidor X y muestra la topología.

Ya no podrá ver la máquina virtual en la consola vSphere.

- 2 Desde Horizon Client, conéctese al escritorio Linux.
- 3 En la sesión del escritorio Linux, verifique que el controlador de pantalla NVIDIA esté instalado.

Abra una ventana de terminal y ejecute el comando `glxinfo | grep NVIDIA`.

Aparece la salida del controlador NVIDIA. Por ejemplo:

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

El usuario puede acceder a las funciones de los gráficos NVIDIA en el escritorio remoto.

Después de verificar la instalación del controlador de pantalla NVIDIA, realice las siguientes tareas para que la instalación se realice correctamente.

- Si actualiza el kernel de Linux, es posible que Horizon Agent no pueda comunicarse con el servidor de conexión de Horizon. Para solucionar el problema, vuelva a instalar el controlador NVIDIA.
- Configure la licencia NVIDIA GRID en la máquina virtual Linux. Para obtener más información, consulte la documentación de NVIDIA. El escritorio Linux no funcionará correctamente si la licencia no está configurada. Por ejemplo, el ajuste automático no funciona.

Configurar RHEL 6.x para vDGA

Puede configurar un sistema operativo invitado RHEL 6.x para que los escritorios Horizon 7 para Linux puedan aprovechar las funciones de vDGA en el host ESXi.

Precaución Antes de comenzar, compruebe que Horizon Agent no esté instalado en la máquina virtual Linux. Si instala Horizon Agent antes de configurar la máquina para usar vDGA, se sobrescriben los parámetros de configuración requeridos del archivo `xorg.conf` y no funciona vDGA. Debe instalar Horizon Agent una vez que se haya completado la configuración de vDGA.

Habilitar DirectPath I/O para NVIDIA GRID en un host

Antes de configurar una máquina virtual Linux para usar vDGA, los dispositivos PCI de GPU NVIDIA GRID deben estar disponibles para la transmisión DirectPath I/O en el host ESXi.

Requisitos previos

- Verifique que tenga instalado vSphere 6.0 o una versión posterior en su entorno.
- Verifique que tenga instalada una tarjeta gráfica NVIDIA GRID K1 o K2 en el host ESXi.

Procedimiento

- 1 En vSphere Web Client, diríjase hasta el host ESXi.
- 2 Haga clic en la pestaña **Administrar** y haga clic en **Configuración**.
- 3 En la sección Hardware, haga clic en **Dispositivos PCI**.

- 4 Para habilitar la transmisión DirectPath I/O para las GPU NVIDIA GRID, haga clic en **Editar**.

Icono	Descripción
Icono verde	El dispositivo PCI está activo y puede habilitarse.
Icono naranja	El estado del dispositivo cambió. Debe reiniciar el host para poder usar el dispositivo.

- 5 Seleccione las GPU NVIDIA GRID y haga clic en **Aceptar**.

Los dispositivos PCI se agregan a la tabla DirectPath I/O Dispositivos PCI disponibles para las máquinas virtuales.

- 6 Reinicie el host para que los dispositivos estén disponibles para que las máquinas virtuales Linux los usen.

Agregar un dispositivo de pass-through vDGA a una máquina virtual con RHEL 6.x

Para configurar una máquina virtual con RHEL 6.x para que use vDGA, debe agregar el dispositivo PCI a la máquina virtual. Con este paso, el dispositivo físico en el host ESXi se puede pasar a través para utilizarlo en la máquina virtual.

Requisitos previos

- Compruebe que la máquina virtual Linux esté preparada para usarse como escritorio. Consulte [Crear una máquina virtual e instalar Linux](#) y [Preparar una máquina Linux para la implementación de escritorios remotos](#).
- Compruebe que Horizon Agent no esté instalado en la máquina virtual Linux.
- Compruebe que el dispositivo PCI NVIDIA GRID GPU se haya puesto a disposición para el pass-through de E/S de DirectPath en el host. Consulte [Habilitar DirectPath I/O para NVIDIA GRID en un host](#).

Procedimiento

- 1 Inicie sesión en el sistema operativo invitado RHEL 6.x como usuario local configurado con derechos sudo.
- 2 En vSphere Web Client, seleccione la máquina virtual y en la pestaña **Hardware de VM** haga clic en **Editar configuración**.
- 3 En el menú **Nuevo dispositivo**, seleccione **Dispositivo PCI**.
- 4 Haga clic en **Agregar** y seleccione el dispositivo PCI desde el menú desplegable.
- 5 Haga clic en **Reservar toda la memoria** y haga clic en **Aceptar**.
Debe reservar toda la memoria de máquina virtual para que la GPU sea compatible con vDGA.
- 6 Encienda la máquina virtual y abra la consola de vSphere para conectarse a la máquina.

- 7 Compruebe que el dispositivo NVIDIA GRID se pase a través hasta la máquina virtual.

Abra una ventana de terminal y ejecute el siguiente comando:

```
lspci | grep NVIDIA
```

Se muestra el controlador compatible con VGA XX:00.0. Por ejemplo:

```
NVIDIA Corporation GK104GL [GRID K2]
```

Instalar el controlador de visualización NVIDIA para vDGA

Para instalar el controlador de visualización NVIDIA para vDGA, debe deshabilitar el controlador NVIDIA predeterminado, descargar los controladores de visualización NVIDIA y configurar el dispositivo PCI en la máquina virtual.

Requisitos previos

- Verifique que el dispositivo PCI se agregó a la máquina virtual RHEL 6 x. Consulte [Agregar un dispositivo de pass-through vDGA a una máquina virtual con RHEL 6.x](#).

Procedimiento

- 1 Deshabilite y ponga en la lista negra el controlador NVIDIA Nouveau predeterminado.

- a Edite el archivo `grub.conf`.

Para RHEL 6.x, el archivo es `/boot/grub/grub.conf`.

Versión de RHEL	Comando
6.x	<code>sudo vi /boot/grub/grub.conf</code>

- b Agregue la línea `rdblacklist=nouveau` al final de las opciones de kernel.
- c Edite el archivo `blacklist.conf`.

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d Agregue la siguiente línea en cualquier lugar del archivo `blacklist.conf`.

```
blacklist nouveau
```

- 2 Reinicie la máquina virtual.

La visualización cambió de aspecto.

- 3 (opcional) Verifique que el controlador Nouveau esté deshabilitado.

```
/sbin/lsmmod | grep nouveau
```

Si la búsqueda `grep` no devuelve ningún resultado, el controlador Nouveau está deshabilitado.

- 4 Descargue el controlador NVIDIA del sitio [Descarga de controladores NVIDIA](#).

Seleccione la versión apropiada del controlador de los menús desplegables de NVIDIA:

Opción	Descripción
Tipo de producto	GRID
Serie del producto	GRID Series
Producto	Seleccione la versión (por ejemplo: GRID K2) que está instalada en el host ESXi.
Sistema operativo	Linux 64-bits o Linux 32-bits

- 5 Para conectarse a la máquina virtual, abra un terminal remoto o utilice una consola de texto pulsando Ctrl-Alt-F2, inicie sesión en la raíz y ejecute el comando `init 3` para deshabilitar Windows X.
- 6 Instale los componentes adicionales necesarios para el controlador NVIDIA.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 Agregue un marcador ejecutable al paquete del controlador NVIDIA para vDGA.

```
chmod +x NVIDIA-Linux-x86_64-versión.run
```

- 8 Ejecute el programa instalador de NVIDIA.

```
sudo ./NVIDIA-Linux-x86_64-versión.run
```

- 9 Acepte el contrato de licencia del software NVIDIA y seleccione **Sí** para actualizar las opciones de configuración X.

Pasos siguientes

Instalar Horizon Agent en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).

Cree un grupo de escritorios que contenga las máquinas virtuales Linux configuradas. Consulte [Crear un grupo de escritorios manual para Linux](#).

Verificar que el controlador de pantalla NVIDIA está instalado

Puede verificar que el controlador de pantalla NVIDIA esté instalado en una máquina virtual Linux si muestra la salida del controlador NVIDIA de una sesión de escritorio de Horizon.

Requisitos previos

- Verifique que instaló el controlador de pantalla NVIDIA.
- Compruebe que Horizon Agent esté instalado en la máquina virtual Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).

- Verifique que la máquina virtual Linux esté implementada en un grupo de escritorios. Consulte [Crear un grupo de escritorios manual para Linux](#).

Procedimiento

- 1 Reinicie la máquina virtual Linux.

El script de inicio de Horizon Agent inicia el servidor X y muestra la topología.

Ya no podrá ver la máquina virtual en la consola vSphere.

- 2 Desde Horizon Client, conéctese al escritorio Linux.
- 3 En la sesión del escritorio Linux, verifique que el controlador de pantalla NVIDIA esté instalado.

Abra una ventana de terminal y ejecute el comando `glxinfo | grep NVIDIA`.

Aparece la salida del controlador NVIDIA. Por ejemplo:

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

El usuario puede acceder a las funciones de los gráficos NVIDIA en el escritorio remoto.

Después de verificar la instalación del controlador de pantalla NVIDIA, realice las siguientes tareas para que la instalación se realice correctamente.

- Si actualiza el kernel de Linux, es posible que Horizon Agent no pueda comunicarse con el servidor de conexión de Horizon. Para solucionar el problema, vuelva a instalar el controlador NVIDIA.
- Configure la licencia NVIDIA GRID en la máquina virtual Linux. Para obtener más información, consulte la documentación de NVIDIA. El escritorio Linux no funcionará correctamente si la licencia no está configurada. Por ejemplo, el ajuste automático no funciona.

Instalar Horizon Agent

5

Debe instalar Horizon Agent en los escritorios Linux para que Horizon Connection Server pueda comunicarse con los escritorios y administrarlos.

Este capítulo incluye los siguientes temas:

- [Instalar Horizon Agent en una máquina virtual Linux](#)
- [Configurar el certificado para Linux Agent](#)
- [Actualizar Horizon Agent en una máquina virtual Linux](#)
- [Desinstalar máquinas Horizon 7 for Linux](#)

Instalar Horizon Agent en una máquina virtual Linux

Para poder implementar una máquina virtual Linux como escritorio remoto, es necesario instalar Horizon Agent en ella.

A partir de la versión 7.0.1 de Horizon, Horizon Agent for Linux utiliza máquinas virtuales administradas por vCenter. Las máquinas virtuales administradas ofrecen las siguientes mejoras.

- vCenter es un requisito obligatorio para la implementación de escritorios Linux.
- La instalación de Horizon Agent en Linux no requiere registro.
- Para implementaciones que afecten a muchos escritorios Linux, puede instalar Horizon Agent en la máquina virtual base.

Precaución Si se va a utilizar NVIDIA GRIDvGPU o vDGA, se deben configurar estas funciones 3D en la máquina virtual Linux antes de instalar Horizon Agent. Si se instala primero Horizon Agent, se sobrescribirán los parámetros requeridos en el archivo `xorg.conf` y no funcionarán las características de gráficos 3D.

Consulte [Configurar las distribuciones de Linux compatibles con vGPU](#) o [Configurar RHEL 6.x para vDGA](#). Instale Horizon Agent después de completar la configuración de gráficos 3D.

En la configuración de gráficos 2D, se puede instalar Horizon Agent después de completar los pasos indicados en [Preparar una máquina Linux para la implementación de escritorios remotos](#).

Requisitos previos

- Compruebe que el sistema operativo invitado Linux esté preparado para su uso como escritorio. Consulte [Preparar una máquina Linux para la implementación de escritorios remotos](#).
- Familiarícese con el script del instalador de Horizon Agent for Linux. Consulte [Opciones de la línea de comandos para install_viewagent.sh](#).

Procedimiento

- 1 Descargue el archivo del instalador de Horizon Agent for Linux desde el sitio de descarga de VMware en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y computación de usuario final, seleccione los componentes de descarga de View para VMware Horizon. En Horizon 7 for Linux, seleccione la página de descargas de VMware Horizon 7 para sistemas Linux de 64 bits.

El nombre del archivo del instalador es `VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz` para Linux de 64 bits, donde `y.y.y` es el número de versión y `xxxxxxx` el número de compilación.

- 2 Descomprima el archivo tar correspondiente a su distribución Linux en el sistema operativo invitado.
Por ejemplo:

```
tar -xzf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
```

- 3 Acceda a la carpeta del archivo tar.
- 4 Ejecute el script de `install_viewagent.sh` como superusuario.

Consulte una lista de las opciones de la línea de comandos en [Opciones de la línea de comandos para install_viewagent.sh](#).

Por ejemplo:

```
sudo ./install_viewagent.sh
```

- 5 Escriba **Sí** para aceptar el EULA si ejecuta `install_viewagent.sh` sin especificar la opción `-A`.
El instalador no se ejecutará si no se acepta el EULA.

- 6 Reinicie Linux para que los cambios tengan efecto.

Después de la instalación, se inicia el servicio `viewagent`. Compruebe que el servicio se inicie utilizando `sudo service viewagent status`.

Pasos siguientes

Implemente la máquina virtual en un grupo de escritorios. Consulte [Crear un grupo de escritorios manual para Linux](#).

Opciones de la línea de comandos para install_viewagent.sh

El script `install_viewagent.sh` instala Horizon Agent en un sistema operativo invitado Linux.

Utilice el formato siguiente del script `install_viewagent.sh` en una ventana de comandos en el entorno de escritorio de gnome.

```
install_viewagent.sh argumento opción_comando [argumento opción_comando] . . .
```

El script `install_viewagent.sh` incluye parámetros opcionales y obligatorios.

Tabla 5-1. Parámetro obligatorio pero opcional de `install_viewagent.sh`

Parámetro opcional (información obligatoria)	Descripción
-A yes no	Acepte o rechace la declaración del Estándar federal de procesamiento de información (FIPS) y el Contrato de licencia de usuario final (EULA). Debe especificar yes para que la instalación continúe.

Tabla 5-2. Parámetros opcionales de `install_viewagent.sh`

Parámetros opcionales	Descripción
-a yes no	Instala u omite el soporte del redireccionamiento de entrada de audio. La opción predeterminada es yes .
-f yes no	Instala u omite el soporte de los módulos criptográficos diseñados para el Estándar federal de procesamiento de información (FIPS) 140-2. La opción predeterminada es no . Para obtener más información, consulte la descripción del modo FIPS 140-2 en Funciones de los escritorios de Horizon para Linux .
-j	Contraseña de almacén de claves de SSL de JMS. De forma predeterminada, el instalador genera una cadena aleatoria.
-m yes no	Instala u omite la compatibilidad con el redireccionamiento de tarjetas inteligentes. La opción predeterminada es no .
-r yes no	Reinicia el sistema automáticamente tras la instalación. La opción predeterminada es no .
-s	Nombre distintivo (DN) de asunto de certificado autofirmado. De forma predeterminada, el instalador utiliza Blast.
-C yes no	Instala u omite la compatibilidad con la función Redireccionamiento del portapapeles. La opción predeterminada es yes .
-F yes no	Instala u omite la compatibilidad con CDR. La opción predeterminada es yes .
-M yes no	Actualiza Linux Agent a un agente administrado o sin administrar. La opción predeterminada es yes .
-S yes no	Instala u omite el soporte para Single Sign-On (SSO). La opción predeterminada es yes .
-T yes no	Instala u omite el soporte para True Single Sign-On (True SSO). La opción predeterminada es no .
-U yes no	Instala u omite la compatibilidad USB. La opción predeterminada es no .

Tabla 5-3. Ejemplos de parámetros deinstall_viewagent.sh

Condición	Ejemplos
Instalación nueva	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>Para una instalación nueva, siempre es necesario crear un nuevo grupo de escritorios.</p>
Actualice desde una máquina virtual sin administrar y mantenga su estilo	<pre>sudo ./install_viewagent.sh -A yes-M no</pre> <p>Este tipo de actualización no requiere la creación de un nuevo grupo de escritorios. Puede volver a utilizar el grupo de escritorios existente.</p> <p>Nota Para obtener el mejor rendimiento posible, no use ninguna máquina virtual sin administrar.</p>
Actualice desde una implementación de máquina virtual sin administrar y conviértala en una máquina virtual administrada. La actualización requiere la creación de un grupo de escritorios en el agente	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>Este tipo de actualización requiere la creación de un nuevo grupo de escritorios. Debe eliminar el grupo de escritorios existente.</p>

Configurar el certificado para Linux Agent

Cuando instala Linux Agent, el instalador genera un certificado autofirmado para VMwareBlastServer.

- Cuando la puerta de enlace de seguridad de Blast está deshabilitada en el agente, VMwareBlastServer presenta este certificado al explorador que utiliza HTML Access para conectarse con el escritorio Linux.
- Cuando está habilitada en el agente la puerta de enlace de seguridad de Blast, el certificado de la puerta de enlace de seguridad de Blast presenta el certificado al explorador.

Para cumplir con las normativas de seguridad o del sector, puede reemplazar el certificado autofirmado por un certificado firmado por una Entidad de certificación (Certificate Authority, CA.)

Procedimiento

- 1 Instale la clave privada y el certificado en VMwareBlastServer.
 - a Cambie el nombre de la clave privada a rui.key y el del certificado a rui.crt.
 - b Ejecute `sudo chmod 550 /etc/vmware/ssl`.

- c Copie las claves rui.crt y rui.key en /etc/vmware/ssl.
 - d Ejecute `chmod 440 /etc/vmware/ssl`.
- 2 Instale la Entidad de certificación raíz e intermedia en el almacén de entidades de certificación del SO Linux.

Nota Consulte la documentación de distribución de Linux para el cambio de ajustes del sistema Linux.

Actualizar Horizon Agent en una máquina virtual Linux

Puede actualizar Horizon Agent en una máquina virtual Linux si instala la versión más reciente de Horizon Agent.

Máquina virtual sin administrar: el instalador de agentes registra la máquina en el agente que requiere la información del administrador del agente. El asistente **Creación de grupo de escritorios** usa **Otros orígenes** de la página Origen de la máquina para seleccionar la máquina virtual registrada.

Máquina virtual administrada: el instalador no se comunica con el agente. El asistente **Creación de grupo de escritorios** usa **Máquinas virtuales de vCenter** de la página Origen de la máquina para seleccionar las máquinas virtuales a través de vCenter. La implementación de la máquina virtual admite las siguientes funciones.

- Directiva de alimentación de máquinas remotas
- Permitir a los usuarios restablecer sus máquinas

Nota Horizon Agent for Linux 7.0.0 y versiones anteriores funcionaban como máquinas virtuales sin administrar. Horizon Agent for Linux 7.0.1 funciona como máquina virtual administrada.

Puede usar los siguientes métodos para actualizar de una implementación de máquina virtual sin administrar a una administrada.

- Conserve la implementación de máquina virtual sin administrar y actualice a la versión necesaria. Este tipo de actualización no requiere ninguna modificación de configuración en Horizon Connection Server.
- Actualice de una implementación de máquina virtual sin administrar a una implementada con cualquier versión. Este tipo de actualización requiere la creación de un nuevo grupo de escritorios en Horizon Connection Server.

Nota En la actualización desde una implementación de máquina virtual administrada, puede conservar la implementación de la máquina virtual y actualizar a la versión necesaria. Sin embargo, no es posible convertir la implementación de la máquina virtual administrada en una sin administrar durante una actualización.

Los siguientes parámetros están disponibles para la actualización.

Tabla 5-4. Parámetros opcionales para actualizar Horizon Agent

Parámetro	Descripción
-A yes	Aceptación del contrato de licencia de usuario final (EULA) y de la declaración de normas FIPS. Debe especificar yes para que se realice la instalación. Si este parámetro no se especifica, el script de instalación solicita el valor.
-a yes no	Instala u omite el soporte del redireccionamiento de entrada de audio.
-f yes no	Instala u omite el soporte de los módulos criptográficos diseñados para el Estándar federal de procesamiento de información (FIPS) 140-2. La opción predeterminada es no . Para obtener más información, consulte la descripción del modo FIPS 140-2 en Funciones de los escritorios de Horizon para Linux .
-m yes no	Instala u omite la compatibilidad con el redireccionamiento de tarjetas inteligentes. La opción predeterminada es no .
-r yes no	Reinicia el sistema operativo después de la instalación. El valor predeterminado es no .
-C yes no	Instala u omite la compatibilidad con la función Redireccionamiento del portapapeles. La opción predeterminada es yes .
-F yes no	Instala u omite la compatibilidad con CDR. La opción predeterminada es yes .
-M yes no	Actualiza el agente de Linux a un agente administrado no administrado. El valor predeterminado es yes .
-S yes no	Instala u omite la compatibilidad con Single Sign-On (SSO). La opción predeterminada es yes .
-U yes no	Instala u omite la compatibilidad con USB. La opción predeterminada es no .

Actualizar Horizon Agent en una máquina virtual Linux

Puede actualizar Horizon Agent en una máquina Linux instalando la versión más reciente de Horizon Agent.

Requisitos previos

- Compruebe que no se esté ejecutando el proceso VMwareBlastServer.

Para detener este proceso, asegúrese de que el usuario cierre la sesión en la máquina y de que no haya ninguna sesión de escritorio activa, o bien reinicie la máquina.

Procedimiento

- 1 Descargue el archivo del instalador más reciente de Horizon Agent for Linux en el sitio de descargas de VMware: <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y computación de usuario final, seleccione la descarga de VMware Horizon 7, que incluye el instalador de Horizon Agent for Linux.

El nombre del archivo del instalador es VMware-viewagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz para Linux de 64 bits, donde y.y.y es el número de versión y xxxxxxx es el número de compilación.

- 2 Descomprima el archivo tar correspondiente a su distribución Linux en el sistema operativo invitado.

Por ejemplo:

```
tar -xzf <Archivo tar comprimido (.gz) de Horizon Agent>
```

- 3 Acceda a la carpeta del archivo tar.
- 4 Ejecute el script `install_viewagent.sh` para actualizar máquinas virtuales no administradas como se indica en uno de los siguientes escenarios de implementación:

Opción	Descripción
Actualizar la implementación de la máquina virtual sin administrar y conservar su implementación	<pre>sudo ./install_viewagent.sh -A yes -M no</pre> <p>Nota Para obtener el mejor rendimiento posible, no use ninguna máquina virtual sin administrar.</p>
Actualizar la implementación de la máquina virtual sin administrar y cambiarla a la implementación de la máquina virtual administrada	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>Nota En Horizon Console, borre el grupo de escritorios existente de la implementación de la máquina virtual no administrada y cree un grupo de escritorios para una implementación de la máquina virtual administrada. Para obtener más información, consulte Crear un grupo de escritorios manual para Linux.</p>
Actualizar una implementación de máquina virtual administrada	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>Nota Después de la actualización, se podrá reutilizar el grupo de escritorios existente.</p>

Desinstalar máquinas Horizon 7 for Linux

Para desinstalar Horizon 7 for Linux de una máquina virtual, debe desinstalar Horizon Agent y eliminar los archivos de configuración.

Requisitos previos

Verifique que el proceso `VMwareBlastServer` no se esté ejecutando. Para detener este proceso, asegúrese de cerrar la sesión en la máquina y de que ninguna sesión de escritorio esté activa, o bien reinicie la máquina.

Procedimiento

- 1 Abra una ventana de terminal en la máquina virtual y ejecute el script para desinstalar Horizon Agent.

```
sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh
```

El script detiene los procesos de Horizon Agent, elimina el servicio de Horizon Agent y el software del directorio de instalación `/usr/lib/vmware/viewagent`.

- 2 De forma manual, elimine los archivos de configuración de Horizon 7 for Linux que aparecen en el directorio `/etc/vmware`.

Opciones de configuración para escritorios Linux

6

Puede configurar varias opciones para personalizar la experiencia de usuario mediante archivos de configuración.

Este capítulo incluye los siguientes temas:

- [Opciones de configuración en los archivos de configuración de un escritorio Linux](#)
- [Usar Directivas de Smart](#)
- [Ejemplo de configuración de Blast para escritorios Linux](#)
- [Ejemplos de opciones de redireccionamiento de unidades cliente para escritorios Linux](#)

Opciones de configuración en los archivos de configuración de un escritorio Linux

Puede configurar determinadas opciones agregando entradas a los archivos `/etc/vmware/config` o `/etc/vmware/viewagent-custom.conf`.

Durante la instalación de Horizon Agent, el instalador copia dos archivos de plantilla de configuración, `config.template` y `viewagent-custom.conf.template`, en `/etc/vmware`. Además, si `/etc/vmware/config` y `/etc/vmware/viewagent-custom.conf` no existen, el instalador copia `config.template` en `config` y `viewagent-custom.conf.template` en `viewagent-custom.conf`. En los archivos de plantilla, se enumeran y documentan todas las opciones de configuración. Para establecer una opción, tan solo tiene que eliminar el comentario y cambiar el valor según corresponda.

Por ejemplo, la siguiente línea de `/etc/vmware/config` habilita la compilación del modo PNG sin pérdida.

```
RemoteDisplay.buildToPNG=TRUE
```

Después de hacer cambios de configuración, reinicie Linux para que los cambios surtan efecto.

Opciones de configuración en /etc/vmware/config

VMwareBlastServer y sus complementos asociados utilizan el archivo de configuración /etc/vmware/config.

Nota La siguiente tabla incluye la descripción de cada opción de directiva aplicada por el agente para las conexiones USB en el archivo de configuración de Horizon Agent. Horizon Agent usa la configuración para decidir si un USB se puede reenviar al equipo del host. Horizon Agent también envía las opciones a Horizon Client para que las interprete y las aplique. Esta aplicación se basa en si desea especificar el modificador merge (**m**) para aplicar la opción de la directiva de filtro de Horizon Agent, además de la opción de directiva de filtro de Horizon Client, o reemplazar el modificador (**o**) para usar la opción de la directiva de filtro de Horizon Agent en lugar de la opción de la directiva de filtro de Horizon Client.

Tabla 6-1. Opciones de configuración en /etc/vmware/config

Opción	Valor/Formato	Predeterminado	Descripción
Clipboard.Direction	0, 1, 2, o 3	2	<p>Utilice esta opción para especificar la directiva de redireccionamiento del portapapeles. Los valores válidos son los siguientes:</p> <ul style="list-style-type: none"> ■ 0 - Deshabilitar el redireccionamiento del portapapeles. ■ 1 - Habilitar el redireccionamiento del portapapeles en ambas direcciones. ■ 2 - Habilitar el redireccionamiento del portapapeles solo del cliente al escritorio remoto. ■ 3 - Habilitar el redireccionamiento del portapapeles solo de escritorio remoto a cliente.
RemoteDisplay.allowAudio	true o false	true	Establezca esta opción para habilitar o deshabilitar la salida de audio.
RemoteDisplay.allowH264	true o false	true	Establezca esta opción para habilitar o deshabilitar la codificación H.264.
RemoteDisplay.buildToPNG	true o false	false	<p>Las aplicaciones gráficas y en especial las aplicaciones de diseño gráfico requieren una representación exacta de los píxeles de las imágenes en la pantalla de cliente de un escritorio Linux. Puede configurar la compilación de un modo PNG sin pérdida para la reproducción de vídeos e imágenes que se generan en un escritorio Linux y que se representan en el dispositivo cliente. Esta función utiliza ancho de banda adicional entre el cliente y el host ESXi. Al habilitar esta opción se deshabilita la codificación H.264.</p>
RemoteDisplay.enableNetworkContinuity	true o false	true	Establezca esta opción para habilitar o deshabilitar la función Network Continuity en Horizon Agent for Linux.
RemoteDisplay.enableNetworkIntelligence	true o false	true	Establezca esta opción para habilitar o deshabilitar la función Network Intelligence en Horizon Agent for Linux.

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
RemoteDisplay.enableStats	true o false	false	Habilita o deshabilita las estadísticas de protocolo de visualización VMware Blast en el registro de mks, como ancho de banda, FPS, RTT, etc.
RemoteDisplay.enableUDP	true o false	true	Establezca esta opción para habilitar o deshabilitar que Horizon Agent for Linux admita el protocolo UDP.
RemoteDisplay.maxBandwidthKbps	Un número entero	1000000	Especifica el ancho de banda máximo en kilobits por segundo (kbps) para una sesión de VMware Blast. El ancho de banda incluye todo el tráfico de control de VMware Blast y de las imágenes, el audio y el canal virtual. El valor válido debe ser inferior a 4 Gbps (4096000).
RemoteDisplay.minBandwidthKbps	Un número entero	256	Especifica el ancho de banda mínimo en kilobits por segundo (kbps) para una sesión de VMware Blast. El ancho de banda incluye todo el tráfico de control de VMware Blast y de las imágenes, el audio y el canal virtual.
RemoteDisplay.maxFPS	Un número entero	30	Especifica la velocidad máxima de actualizaciones de pantalla. Utilice esta opción para administrar el ancho de banda medio que consumen los usuarios. Un valor válido debe estar entre 3 y 60. El valor predeterminado es de 30 actualizaciones por segundo.
RemoteDisplay.maxQualityJPEG	rango disponible de valores: 1-100	90	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. Las opciones de alta calidad se proporcionan para las áreas más estáticas de la pantalla, lo que ofrece una mejor calidad de la imagen.
RemoteDisplay.midQualityJPEG	rango disponible de valores: 1-100	35	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. Utilice esta opción para establecer las opciones de calidad media de la pantalla del escritorio.
RemoteDisplay.minQualityJPEG	rango disponible de valores: 1-100	25	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. Las opciones de baja calidad se proporcionan para las áreas de la pantalla que cambian a menudo, como, por ejemplo, cuando se produce el desplazamiento.
RemoteDisplay.qpmaxH264	rango disponible de valores: 0-51	36	Use esta opción para establecer el parámetro de cuantificación de H264minQP, que especifica la mejor calidad de imagen para la pantalla remota configurada para utilizar la codificación H.264. Establezca el valor en un valor superior al establecido para RemoteDisplay.qpminH264.

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
RemoteDisplay.qpminH264	rango disponible de valores: 0-51	10	Use esta opción para establecer el parámetro de cuantificación de H264maxQP, que especifica la calidad de imagen más baja para la pantalla remota configurada para utilizar la codificación H.264. Establezca el valor en un valor inferior al establecido para RemoteDisplay.qpmaxH264.
UsbRedirPlugin.log.logLevel	error, warn, info, debug, trace o verbose	info	Utilice esta opción para establecer el nivel de registro del complemento Redireccionamiento USB.
UsbRedirServer.log.logLevel	error, warn, info, debug, trace o verbose	info	Utilice esta opción para establecer el nivel de registro del servidor Redireccionamiento USB.
VMWPKcs11Plugin.log.enable	true o false	false	Establezca esta opción para habilitar o deshabilitar el modo de registro de la función True SSO.
VMWPKcs11Plugin.log.logLevel	error, warn, info, debug, trace o verbose	info	Utilice esta opción para establecer el nivel de registro de la función True SSO.
VVC.RTAV.Enable	true o false	true	Establezca esta opción para habilitar o deshabilitar la entrada de audio.
VVC.ScRedir.Enable	true o false	true	Establezca esta opción para habilitar o deshabilitar el redireccionamiento de tarjetas inteligentes.
VVC.logLevel	fatal error, warn, info, debug o trace	info	Utilice esta opción para establecer el nivel de registro del nodo proxy VVC.
cdserver.cacheEnable	true o false	true	Establezca esta opción para habilitar o deshabilitar la función de caché de escritura en el agente a través del lado del cliente.
cdserver.customizedSharedFolderPath	ruta_carpeta	/home/	<p>Utilice esta opción para cambiar la ubicación de la carpeta compartida de Redireccionamiento de unidades cliente (CDR) del directorio /home/usuario/tsclient predeterminado a un directorio personalizado.</p> <p>Por ejemplo, si el usuario test desea colocar la carpeta compartida de CDR en /mnt/test/tsclient en lugar de /home/test/tsclient, el usuario puede especificar</p> <p>cdserver.customizedSharedFolderPath=/mnt/.</p> <p>Nota Para que se aplique esta opción, la carpeta especificada debe existir y tener los permisos de usuario adecuados.</p>
cdserver.forcedByAdmin	true o false	false	Establezca esta opción para controlar si el cliente puede compartir carpetas adicionales que no se especificaron en la opción cdserver.shareFolders.

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
cdserver.logLevel	error, warn, info, debug, trace o verbose	info	Utilice esta opción para establecer el nivel de registro para el archivo vmware-CDRserver.log.
cdserver.permissions	R	RW	<p>Utilice esta opción para aplicar los permisos de lectura o de escritura que Horizon Agent tenga en las carpetas que comparte Horizon Client. Por ejemplo:</p> <ul style="list-style-type: none"> ■ Si la carpeta que comparte Horizon Client tiene los permisos read y write y establece cdserver.permissions=R, entonces Horizon Agent solo tiene permisos read de acceso. ■ Si la carpeta que comparte Horizon Client solo tiene los permisos read y establece cdserver.permissions=RW, entonces Horizon Agent solo tiene derechos de acceso read. Horizon Agent no puede cambiar el atributo de solo read establecido por Horizon Client. Horizon Agent solo puede eliminar los derechos de acceso de escritura. <p>A continuación, aparecen usos típicos:</p> <ul style="list-style-type: none"> ■ cdserver.permissions=R ■ #cdserver.permissions=R (por ejemplo, puede agregar un comentario o eliminar la entrada)
cdserver.sharedFolders	<i>ruta_archivo1,R</i> ; <i>ruta_archivo2,;</i> <i>ruta_archivo3,R</i> ; ...	no definida	<p>Especifique una o varias rutas a las carpetas que el cliente pueda compartir con el escritorio Linux. Por ejemplo:</p> <ul style="list-style-type: none"> ■ Para un cliente Windows: C:\spreadsheets,;D:\ebooks,R ■ Para un cliente que no sea Windows: /tmp/spreadsheets;/tmp/ebooks,;/home/finance,R
collaboration.logLevel	error, info o debug	info	Utilice esta opción para establecer el nivel de registro que se utilizará para la sesión de colaboración. Si el nivel de registro es debug, se registran todas las llamadas realizadas a las funciones collabui y el contenido de la lista collabor.
collaboration.maxCollabors	Un número entero menor que 10	5	Especifica el número máximo de colaboradores que puede invitar a unirse a una sesión.
collaboration.enableEmail	true o false	true	Establezca esta opción para habilitar o deshabilitar el envío de invitaciones de colaboración mediante una aplicación de correo electrónico instalada. Si esta opción está deshabilitada, no puede usar el correo electrónico para invitar a colaboradores, aunque se instale una aplicación de correo electrónico.
collaboration.serverUrl	[URL]	no definida	Especifica las URL del servidor que se incluyen en las invitaciones de colaboración.

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
collaboration.enableControlPassing	true o false	true	Establezca esta opción para permitir o no que los colaboradores tengan el control del escritorio Linux. Para especificar una sesión de colaboración de solo lectura, establezca el valor false en esta opción.
mksVNCServer.useUIInputButtonMapping	true o false	false	Establezca esta opción para habilitar la compatibilidad con un mouse para zurdos en Ubuntu o RHEL 7.x. CentOS y RHEL 6.x admiten un mouse para zurdos y no es necesario que configure esta opción.
mksvhan.clipboardSize	Un número entero	1024	Utilice esta opción para especificar el tamaño máximo del portapapeles para copiar y pegar.
vdpservice.log.logLevel	fatal error, warn, info, debug o trace	info	Utilice esta opción para establecer el nivel de registro del vdpService.
viewusb.AllowAudioIn	{m o}: {true false}	no definida, lo que es igual a true	Utilice esta opción para permitir o no el redireccionamiento de dispositivos de entrada de audio. Ejemplo: o:false
viewusb.AllowAudioOut	{m o}: {true false}	no definida, lo que es igual a false	Establezca esta opción para permitir o no el redireccionamiento de dispositivos de salida de audio.
viewusb.AllowAutoDeviceSplitting	{m o}: {true false}	no definida, lo que es igual a false	Establezca esta opción para permitir o no la división de un dispositivo USB compuesto. Ejemplo: m:true
viewusb.AllowDevDescFailsafe	{m o}: {true false}	no definida, lo que es igual a false	Establezca esta opción para permitir o no que se redireccionen los dispositivos, aunque Horizon Client no pueda obtener la configuración o los descriptores del dispositivo. Para admitir un dispositivo, aunque no se pueda obtener su configuración o sus descriptores, inclúyalo en los filtros de inclusión como IncludeVidPid o IncludePath .
viewusb.AllowHIDBootable	{m o}: {true false}	no definida, lo que es igual a true	Utilice esta opción para permitir o no el redireccionamiento de los dispositivos de entrada que no sean los dispositivos de teclado o de mouse disponibles en el momento de arranque, también conocidos como dispositivos con arranque HID.
viewusb.AllowKeyboardMouse	{m o}: {true false}	no definida, lo que es igual a false	Utilice esta opción para permitir o no el redireccionamiento de teclados con dispositivos de señalización (como un mouse, una bola de seguimiento o un panel táctil).
viewusb.AllowSmartcard	{m o}: {true false}	no definida, lo que es igual a false	Utilice esta opción para permitir o no el redireccionamiento de dispositivos de tarjetas inteligentes.
viewusb.AllowVideo	{m o}: {true false}	no definida, lo que es igual a true	Use esta opción para permitir o no el redireccionamiento de dispositivos de vídeo.

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
viewusb.DisableRemoteConfig	{m o}: {true false}	no definida, lo que es igual a false	Establezca esta opción para habilitar o deshabilitar el uso de la configuración de Horizon Agent cuando realice el filtrado de dispositivos USB.
viewusb.ExcludeAllDevices	{true false}	no definida, lo que es igual a false	Utilice esta opción para excluir o incluir el redireccionamiento de todos los dispositivos USB. Si está configurado como true , puede usar otras opciones de directivas para permitir el redireccionamiento de dispositivos o familias de dispositivos específicas. Si está configurado como false , puede usar otras opciones de directivas para evitar el redireccionamiento de dispositivos o familias de dispositivos específicas. Si establece el valor de ExcludeAllDevices en true en Horizon Agent y esta configuración se envía a Horizon Client, la configuración de Horizon Agent sustituirá la de Horizon Client.
viewusb.ExcludeFamily	{m o}: <i>nombre_familia_1</i> [: <i>nombre_familia_2</i> ;...]	no definida	<p>Use esta opción para excluir el redireccionamiento de familias de dispositivos. Por ejemplo: m:bluetooth;smart-card</p> <p>Si habilitó la división automática del dispositivo, Horizon examinará la familia de dispositivos de cada interfaz de un dispositivo USB compuesto para decidir cuál debe excluir. Si deshabilitó la división automática de dispositivos, Horizon examinará la familia del dispositivo de todo el dispositivo USB compuesto.</p> <p>Nota El teclado y el mouse se excluyen del redireccionamiento de forma predeterminada y no es necesario excluirlos mediante esta opción.</p>
viewusb.ExcludePath	{m o}: <i>bus-x1</i> [/ <i>y1</i>].../ <i>port-z1</i> [: <i>bus-x2</i> [/ <i>y2</i>].../ <i>port-z2</i> ;...]	no definida	<p>Utilice esta opción para excluir el redireccionamiento de dispositivos de rutas de puertos o de un concentrador específicos. Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta.</p> <p>Por ejemplo: m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff</p>
viewusb.ExcludeVidPid	{m o}: <i>vid-xxx1</i> <i>pid-yyy1</i> [: <i>vid-xxx2</i> <i>pid-yyy2</i> ;...]	no definida	<p>Establezca esta opción para excluir el redireccionamiento de dispositivos con los ID de producto y de proveedor especificados. Debe especificar los números de ID en hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: o:vid-0781_pid- ****;vid-0561_pid-554c</p>
viewusb.IncludeFamily	{m o}: <i>nombre_familia_1</i> [: <i>nombre_familia_2</i>]...	no definida	<p>Establezca esta opción para incluir familias de dispositivos que se pueden redireccionar.</p> <p>Por ejemplo: o:storage; smart-card</p>

Tabla 6-1. Opciones de configuración en /etc/vmware/config (continuación)

Opción	Valor/Formato	Predeterminado	Descripción
viewusb.IncludePath	<code>{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../portz2;...]</code>	no definida	<p>Utilice esta opción para incluir el redireccionamiento de dispositivos en rutas de puertos o en un concentrador específicos. Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta.</p> <p>Por ejemplo: m:bus-1/2_port- 02;bus-1/7/1/4_port-0f</p>
viewusb.IncludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	no definida	<p>Establezca esta opción para incluir el redireccionamiento de dispositivos con los ID de producto y de proveedor especificados. Debe especificar los números de ID en hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: o:vid-***_pid-0001;vid-0561_pid-554c</p>
viewusb.SplitExcludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	no definida	<p>Utilice esta opción para incluir un dispositivo USB compuesto y especificado en la división por ID de producto o de proveedor, o bien para excluirlo. El formato de la configuración es vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]. Debe especificar los números del ID en formato hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Ejemplo: m:vid-0f0f_pid-55**</p>
viewusb.SplitVidPid	<code>{m o}: vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])[;...]</code>	no definida	<p>Establezca esta opción para tratar los componentes de un dispositivo USB compuesto y especificado según los ID del producto y del proveedor como dispositivos independientes. El formato de la opción es vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]). Puede usar la palabra clave exintf para excluir componentes del redireccionamiento al especificar el número de interfaz. Debe especificar números ID de forma hexadecimal. Además, los números de interfaz en decimales deben incluir un cero a la izquierda. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Ejemplo: o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</p> <p>Nota Horizon no incluye automáticamente los componentes que no ha excluido explícitamente. Debe especificar una directiva de filtrado, como Incluir dispositivo VidPid para incluir estos componentes.</p>

Opciones de configuración en /etc/vmware/viewagent-custom.conf

Java Standalone Agent utiliza el archivo de configuración /etc/vmware/viewagent-custom.conf.

Tabla 6-2. Opciones de configuración en /etc/vmware/viewagent-custom.conf

Opción	Valor	Predeterminado	Descripción
CDREnable	true o false	true	Use esta opción para habilitar o deshabilitar la función Redireccionamiento de unidades cliente (CDR).
CollaborationEnable	true o false	true	Utilice esta opción para habilitar o deshabilitar la función Session Collaboration en los escritorios Linux.
EndpointVPNEnable	true o false	false	Establezca esta opción para especificar si la dirección IP de VPN o la dirección IP de la tarjeta de red física del cliente se deben usar cuando se evalúe la dirección IP del endpoint en el rango de direcciones IP del endpoint usado en Dynamic Environment Manager Console. Si la opción se configura como false, se usa la dirección IP de la tarjeta de red física del cliente. De lo contrario, se usa la dirección IP de VPN.
HelpDeskEnable	true o false	true	Establezca esta opción para habilitar o deshabilitar la función de la herramienta del departamento de soporte técnico.
KeyboardLayoutSync	true o false	true	<p>Utilice esta opción para especificar si desea sincronizar una lista de configuración regional del sistema del cliente y la distribución del teclado actual con escritorios de Horizon Agent for Linux.</p> <p>Cuando esta opción está habilitada o no está configurada, se permite la sincronización. Cuando esta opción está deshabilitada, no se permite la sincronización.</p> <p>Esta función solo es compatible con Horizon Client para Windows y para las siguientes configuraciones regionales: alemán, chino simplificado, chino tradicional, coreano, español, francés, inglés y japonés.</p>
LogCnt	Un número entero	-1	<p>Use esta opción para establecer el número de archivos de registro que se conservan en /tmp/vmware-root.</p> <ul style="list-style-type: none"> ■ -1: conservar todos ■ 0: eliminar todos ■ > 0: número de registros que se conservan.
NetbiosDomain	Una cadena de texto, todo en mayúsculas		Al configurar True SSO, utilice esta opción para establecer el nombre de NetBIOS del dominio de la organización.
OfflineJoinDomain	pbis o samba	pbis	Utilice esta opción para establecer la unión a dominio sin conexión de los clones instantáneos. Los métodos disponibles para realizar una unión a dominio sin conexión son la autenticación PowerBroker Identity Services Open (PBISO) y la unión a dominio sin conexión mediante Samba. Si esta propiedad tiene un valor distinto a pbis o samba, se ignorará la unión a dominio sin conexión.

Tabla 6-2. Opciones de configuración en /etc/vmware/viewagent-custom.conf (continuación)

Opción	Valor	Predeterminado	Descripción
RunOnceScript			<p>Utilice esta opción para volver a unir la máquina virtual clonada a Active Directory.</p> <p>Establezca la opción RunOnceScript después de que cambie el nombre del host. El script especificado solo se ejecuta una vez después del primer cambio de nombre de host. El script se ejecuta con el permiso de raíz cuando se inicia el servicio de agente y el nombre de host cambió después de que se instalase el agente.</p> <p>Por ejemplo, para la solución winbind, debe unir la máquina virtual base a Active Directory con winbind y establecer esta opción en una ruta de acceso de script. El script debe contener el comando de unirse de nuevo al dominio /usr/bin/net ads join -U <ADUserName> %<ADUserPassword>. Tras la clonar la máquina virtual, la personalización del sistema operativo cambia el nombre del host. Cuando se inicia el servicio de agente, se ejecuta el script para unir la máquina virtual clonada a Active Directory.</p>
RunOnceScriptTimeout		120	<p>Utilice esta opción para establecer el tiempo de espera en segundos de la opción RunOnceScript.</p> <p>Por ejemplo, establezca RunOnceScriptTimeout=120</p>
SSLCiphers	Una cadena de texto	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	<p>Use esta opción para especificar la lista de cifrados. Debe utilizar el formato que se define en https://www.openssl.org/docs/manmaster/man1/ciphers.html.</p>
SSLProtocols	Una cadena de texto	TLSv1_1:TLSv1_2	<p>Use esta opción para especificar los protocolos de seguridad. Los protocolos compatibles son TLSv1.0, TLSv1.1 y TLSv1.2.</p>
SSODesktopType	UseGnomeClassic, UseGnomeFlashback, UseGnomeUbuntu, UseMATE o UseKdePlasma	No disponible	<p>Esta opción especifica el entorno de escritorio que se usará, en lugar del entorno de escritorio predeterminado, cuando SSO está habilitado.</p> <p>En primer lugar, debe asegurarse de que el entorno de escritorio seleccionado esté instalado en el escritorio antes de especificar su uso. Después de configurar esta opción en un escritorio Ubuntu 16.04/18.04, la opción se aplica independientemente de si la función SSO está habilitada. Si esta opción se especifica en un escritorio RHEL/CentOS 7.x, el entorno del escritorio seleccionado se usa solo si SSO está habilitado.</p> <p>Nota Esta opción no es compatible con los escritorios RHEL/CentOS 8.0 y RHEL/CentOS 6.x. Horizon 7 solo admite el entorno de escritorio GNOME en escritorios RHEL/CentOS 8.0. Consulte Entorno de escritorios para obtener más información sobre cómo configurar KDE como el entorno de escritorio predeterminado cuando SSO está habilitado en los escritorios RHEL/CentOS 6.x.</p>

Tabla 6-2. Opciones de configuración en /etc/vmware/viewagent-custom.conf (continuación)

Opción	Valor	Predeterminado	Descripción
SSOEnable	true o false	true	Establezca esta opción para habilitar o deshabilitar Single Sign-On (SSO).
SSOUserFormat	Una cadena de texto	[nombredeusuario]	<p>Utilice esta opción para especificar el formato del nombre de inicio de sesión para Single Sign-On. El valor predeterminado es el nombre del usuario solamente. Establezca esta opción si también se requiere el nombre del dominio. Por lo general, el nombre de inicio de sesión es el nombre de dominio más un carácter especial seguido por el nombre de usuario. Si el carácter especial es la barra diagonal inversa, debe escapar con otra barra diagonal inversa. A continuación aparecen ejemplos de formatos del nombre de inicio de sesión:</p> <ul style="list-style-type: none"> ■ SSOUserFormat=[dominio]\\[nombredeusuario] ■ SSOUserFormat=[dominio]+[nombredeusuario] ■ SSOUserFormat=[nombredeusuario]@[dominio]
Subred	Un valor con formato de dirección IP de CIDR	[subred]	Establezca esta opción para una subred que las otras máquinas puedan utilizar para conectarse a Horizon Agent for Linux. Si hay más de una dirección IP local con distintas subredes, se utilizará la dirección IP local de la subred configurada para conectarse a Horizon Agent for Linux. Debe especificar el valor con el formato de dirección IP de CIDR. Por ejemplo, Subred=123.456.7.8/24.
UEMEnable	true o false	false	Establezca esta opción para habilitar o deshabilitar las directivas de Smart de Dynamic Environment Manager. Si la opción está habilitada y se cumple la condición de la directiva de Smart de Dynamic Environment Manager, se aplican estas directivas.
UEMNetworkPath	Una cadena de texto		Esta opción debe estar habilitada en la misma ruta de red que está establecida en la consola de Dynamic Environment Manager. La ruta debe tener un formato similar a //10.111.22.333/view/LinuxAgent/UEMConfig.

Nota Las tres opciones de seguridad, SSLCiphers, SSLProtocols y SSLCipherServerPreference, son para el proceso VMwareBlastServer. Cuando se inicia el proceso VMwareBlastServer, Java Standalone Agent pasa estas opciones como parámetros. Si está habilitada la puerta de enlace segura de Blast (BSG), estas opciones afectan a la conexión entre BSG y el escritorio Linux. Si BSG está deshabilitada, estas opciones afectan a la conexión entre el cliente y el escritorio Linux.

Usar Directivas de Smart

Puede usar Directivas de Smart para crear directivas que controlen el comportamiento del redireccionamiento USB, el redireccionamiento del portapapeles y las funciones de redireccionamiento de la unidad cliente en escritorios remotos Linux específicos.

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.

Requisitos de Directivas de Smart

Para usar Directivas de Smart, su entorno de Horizon 7 tiene que cumplir algunos requisitos.

- Debe instalar Horizon Agent 7.5 o versiones posteriores y VMware Dynamic Environment Manager 9.4 y versiones posteriores en los escritorios remotos que desee administrar con Directivas de Smart.
- Los usuarios deben usar Horizon Client 4.8 o versiones posteriores para conectarse a los escritorios remotos de Linux que administre con Directivas de Smart.
- La opción `DEMEEnable` debe estar habilitada y la opción `DEMNetworkPath` debe establecerse en el archivo `/etc/vmware/viewagent-custom.conf`. Consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#).
- Debe instalar los paquetes de cliente para acceder al almacenamiento compartido de red. En sistemas Ubuntu 18.04, por ejemplo, instale el paquete `nfs-common` para el almacenamiento compartido con NFS habilitado y el paquete `cifs-utils` para el almacenamiento con Samba habilitado.

Instalar Dynamic Environment Manager

Si quiere usar Directivas de Smart de Horizon para controlar el comportamiento de las funciones de escritorios remotos en un escritorio remoto de Linux, debe instalar Dynamic Environment Manager 9.4 o una versión posterior en el escritorio Windows remoto.

Puede descargar el programa instalador de Dynamic Environment Manager desde la página de descargas de VMware. Puede instalar el componente Consola de administración de Dynamic Environment Manager en cualquier escritorio Windows desde el que quiera administrar el entorno de Dynamic Environment Manager. Desde la Consola de administración de Dynamic Environment Manager en un escritorio Windows, puede controlar el comportamiento de las funciones de escritorio remoto de un escritorio remoto Linux.

En un grupo de escritorios RDS, instale Dynamic Environment Manager en el host RDS que proporcione las sesiones publicadas de escritorios.

Para conocer los requisitos del sistema y las instrucciones de instalación completas de Dynamic Environment Manager, consulte el documento de *Instalar y configurar VMware Dynamic Environment Manager*.

Configurar Dynamic Environment Manager

Debe configurar Dynamic Environment Manager antes de poder usarlo para crear directivas inteligentes para funciones de escritorios remotos.

Para configurar Dynamic Environment Manager, siga las instrucciones de configuración en el *Guía de administración de VMware Dynamic Environment Manager*.

Opciones de directivas inteligentes de Horizon

Para controlar el comportamiento de las funciones remotas en Dynamic Environment Manager, cree una directiva inteligente de Horizon.

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. Consulte la lista completa de directivas en el tema "Configurar directivas inteligentes de Horizon para la configuración del entorno de usuario" en la *Guía de administración de VMware Dynamic Environment Manager*.

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. Consulte la lista completa de directivas en el tema "Configurar directivas inteligentes de Horizon para la configuración del entorno de equipos" en la *Guía de administración de VMware Dynamic Environment Manager*.

En general, las opciones de directivas inteligentes de Horizon que configure para funciones remotas en Dynamic Environment Manager anulan cualquier opción de directivas de grupo y cualquier clave de registro equivalentes.

Agregar condiciones a las definiciones de directivas de Horizon Smart

Al definir una directiva de Horizon Smart en Dynamic Environment Manager, puede agregar condiciones que se deben cumplir para que la directiva tenga efecto. Por ejemplo, puede agregar una condición que deshabilite la función de redireccionamiento de unidad cliente solo en el caso de que un usuario se conecte al escritorio remoto desde fuera de la red corporativa.

Importante Debe agregar las siguientes condiciones a una definición de directiva de Horizon Smart para que la configuración de directiva admitida se aplique a un escritorio remoto de Linux. Estas son las únicas condiciones que se admiten actualmente. Si se establecen otras condiciones, el resultado final de la evaluación de condiciones es falso.

Tabla 6-3. Condiciones necesarias para los escritorios remotos de Linux

Condición	Descripción
Operating System Architecture	Comprueba la arquitectura del sistema operativo. El valor debe establecerse en Linux.
Endpoint IP address	Comprueba si la dirección IP del endpoint está dentro del rango especificado. Los campos vacíos del principio del rango se interpretan como 0 y los del final como 255.

Sin embargo, puede establecer varias condiciones de Endpoint IP address, como aparece en el siguiente ejemplo.

```
Operating system is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 – 11.22.33.77
```

Para obtener información detallada sobre cómo agregar y editar condiciones en la Consola de administración de Dynamic Environment Manager, consulte la *Guía de administración de VMware Dynamic Environment Manager*.

Crear una directiva de Horizon Smart en Dynamic Environment Manager

La Consola de administración de Dynamic Environment Manager se utiliza para crear una directiva de Horizon Smart en Dynamic Environment Manager. Al definir una directiva de Horizon Smart, puede agregar condiciones que se deben cumplir para que la directiva de Smart tenga efecto.

Requisitos previos

- Instalar y configurar Dynamic Environment Manager. Consulte [Instalar Dynamic Environment Manager](#) y [Configurar Dynamic Environment Manager](#).
- Familiarícese con las condiciones que puede agregar a las definiciones de directivas de Horizon Smart. Consulte [Agregar condiciones a las definiciones de directivas de Horizon Smart](#).

- Habilite la opción `DEMEnable` y configure la opción `DEMNetworkPath` en el archivo `/etc/vmware/viewagent-custom.conf`. Consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#).

Nota En una red de alta latencia, después de guardar la directiva nueva o actualizada, espere al menos un minuto para que Dynamic Environment Manager termine de procesar los cambios antes de notificar a los usuarios finales que se conecten a los escritorios afectados.

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, configure 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.

Para obtener información completa sobre el uso de la Consola de administración de Dynamic Environment Manager, consulte el documento *Guía de administración de VMware Dynamic Environment Manager*.

Procedimiento

- 1 En Dynamic Environment Manager Management Console, seleccione **Entorno de usuario** para crear una directiva para la configuración del entorno de usuario o la pestaña **Entorno de equipo** para crear una directiva para la configuración del entorno del equipo.

Si hubiese definiciones de directivas de Horizon Smart existentes, se mostrarían en el panel Directivas de Horizon Smart.

- 2 Seleccione **Directivas inteligentes de Horizon** y haga clic en **Crear** para crear una nueva directiva inteligente.
- 3 Seleccione la pestaña **Configuración** y defina los ajustes de directiva de Smart.

- a En la sección Configuración general, introduzca un nombre para la directiva de Smart en el cuadro de texto **Nombre**.

Por ejemplo, si la directiva de Smart afectará a la función de redireccionamiento de unidades cliente, puede darle a la directiva de Smart el nombre de CDR.

- b En la sección Configuración de directivas de Horizon Smart, seleccione los ajustes y las funciones de escritorio remoto que se deben incluir en la directiva de Smart.

Puede seleccionar varias funciones de escritorio remoto.

4 Agregue las condiciones necesarias para usar la nueva directiva Smart con los escritorios remotos de Linux.

- a Seleccione la pestaña **Condiciones**, haga clic en **Agregar** y seleccione la condición **Arquitectura de sistema operativo**.
- b Establezca el valor en **Linux**.

```
Operating System is Linux
```

- c Haga clic en **Agregar** y seleccione la condición **Dirección IP de endpoint**.

El operador **AND** se agrega de forma predeterminada.

- d En el cuadro de diálogo Dirección IP de endpoint, establezca el rango de direcciones IP de endpoint y haga clic en **Aceptar**.

A continuación se indica un ejemplo de la sintaxis correcta.

```
Operating System is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
```

5 Haga clic en **Guardar** para guardar la directiva de Smart.

Dynamic Environment Manager procesa la directiva de Horizon Smart cada vez que un usuario se conecta o reconecta al escritorio remoto.

Dynamic Environment Manager procesa varias directivas de Smart en orden alfabético basándose en el nombre de la directiva de Smart. Las directivas de Horizon Smart aparecen en orden alfabético en el panel Directivas de Horizon Smart. Si las directivas de Smart entran en conflicto, tiene precedencia la última directiva de Smart que se procesó. Por ejemplo, si tiene una directiva de Smart denominada Sue que habilite el redireccionamiento USB para el usuario denominado Sue y otra directiva de Smart denominada Pool que deshabilite el redireccionamiento USB del grupo de escritorios denominado Ubuntu1604, la función de redireccionamiento USB se habilita cuando Sue se conecta a un escritorio remoto en el grupo de escritorios Ubuntu1604.

Ejemplo de configuración de Blast para escritorios Linux

Es posible ajustar la calidad de la imagen de la pantalla del escritorio remoto para mejorar la experiencia del usuario. La mejora de la calidad de la imagen es útil para mantener la uniformidad en la experiencia del usuario en caso de que la conexión de red sea mala.

Ejemplo de configuración del protocolo VMware Blast Extreme

VMwareBlastServer y sus complementos asociados utilizan el archivo de configuración `/etc/vmware/config`.

Tabla 6-4. Ejemplo de opciones de configuración en /etc/vmware/config

Nombre de la opción	Parámetro	LAN de alta velocidad	LAN	WAN dedicada	WAN de banda ancha	WAN de baja velocidad	Velocidad extremadamente lenta
Configuración del ancho de banda	RemoteDisplay.maxBandwidthKbps	1000000 (1 Gbps)	1000000 (1 Gbps)	1000000 (1 Gbps)	5000 (5 Mbps)	2000 (2 Mbps)	1000 (1 Mbps)
FPS máx.	RemoteDisplay.maxFPS	60	30	30	20	15	5
Reproducción de audio	RemoteDisplay.allowAudio	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE
Calidad de visualización (JPEG/PNG)	RemoteDisplay.maxQualityJPEG	90	90	90	70	60	50
Calidad de visualización (JPEG/PNG)	RemoteDisplay.midQualityJPEG	35	35	35	35	35	35
Calidad de visualización (JPEG/PNG)	RemoteDisplay.minQualityJPEG	25	25	25	20	20	20
Calidad de visualización (H.264)	RemoteDisplay.qpmaxH264	28	36	36	36	36	42
Calidad de visualización (H.264)	RemoteDisplay.qpminH264	10	10	10	10	10	10

Ejemplos de opciones de redireccionamiento de unidades cliente para escritorios Linux

Configure las opciones del redireccionamiento de unidades cliente (CDR) para determinar si los escritorios Linux remotos pueden acceder a las unidades y a las carpetas compartidas de un sistema local.

Para configurar las opciones CDR, agregue entradas en el archivo /etc/vmware/config.

El siguiente ejemplo de configuración comparte las carpetas d:\ebooks y C:\spreadsheets, hace que ambas sean de solo lectura y no permite que el cliente comparta más carpetas.

```
cdserver.forcedByAdmin=true
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdserver.permissions=R
```

En el ejemplo anterior, es obligatorio colocar la coma "," después de **ebooks** y de **spreadsheets** para que se analicen las opciones correctamente.

Cualquier "R" incluida en la opción `cdserver.sharedFolders` podría afectar a todas las carpetas que aparecen en esta opción. En el siguiente ejemplo, las carpetas **ebooks** y **spreadsheets** son de solo lectura, aunque el valor **R** solo aparezca tras la ruta de la carpeta **/home/jsmith**.

```
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```


Crear y administrar grupos de escritorios Linux

7

Para configurar máquinas virtuales Linux para usarlas como escritorios remotos, debe crear un grupo de escritorios con máquinas virtuales Linux.

Horizon for Linux es compatible con los siguientes tipos de grupos de escritorios:

- Grupo de escritorios manual con máquina virtual vCenter
- Grupo de escritorios automatizado de clones completos
- Grupo de escritorios flotantes de clones instantáneos

Para crear un grupo de escritorios manual con una máquina virtual de vCenter, debe instalar Horizon Agent en todas las máquinas virtuales. A continuación, use el asistente para la creación de grupos de escritorios del Servidor de conexión para agregar las máquinas virtuales al grupo de escritorios. Para clonar un número elevado de máquinas virtuales, consulte [Descripción general de la implementación por lotes de escritorios Linux](#).

Para crear un grupo de escritorios de clones completos automatizado, debe instalar Horizon 7 Agent en una plantilla de máquina virtual Linux. A continuación, use el asistente para la creación de grupos de escritorios del Servidor de conexión para clonar las máquinas virtuales completas.

Para crear un grupo de escritorios flotantes de clones instantáneos, debe instalar Horizon 7 Agent en una máquina virtual Linux con la configuración de entorno PBIS Open y crear una plantilla a partir de la máquina. A continuación, use el asistente de creación de grupos de escritorios del servidor de conexión para crear el grupo de escritorios flotantes de clones instantáneos.

Este capítulo incluye los siguientes temas:

- [Crear un grupo de escritorios manual para Linux](#)
- [Administrar grupos de escritorios Linux](#)
- [Cree un grupo de escritorios automatizado de clones completos para Linux](#)
- [Crear un grupo de escritorios flotantes de clones instantáneos para Linux](#)
- [Comandos PowerCLI agente](#)

Crear un grupo de escritorios manual para Linux

Puede crear un grupo de escritorios manual para máquinas virtuales Linux.

A continuación se indica cómo configurar los ajustes obligatorios de un grupo de escritorios manual basado en Linux. Para obtener más información sobre cómo crear grupos de escritorios manuales, consulte *Configurar escritorios virtuales en Horizon Console*.

Requisitos previos

- Compruebe que Horizon Agent esté instalado en el sistema operativo invitado de Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- Compruebe que VMware vCenter Server se agregó a Horizon Connection Server.

Procedimiento

- 1 En Horizon Console, agregue un grupo de escritorios manual.

Seleccione **Inventario > Escritorios > Agregar**.

Nota No cree máquinas virtuales Windows y Linux en el mismo grupo de escritorios.

- 2 Seleccione **Grupo de escritorios manual**.
- 3 Seleccione máquinas virtuales administradas o no administradas por vCenter Server y haga clic en **Siguiente**.
- 4 Seleccione asignaciones de usuario dedicadas o flotantes para las máquinas del grupo de escritorios y haga clic en **Siguiente**.
- 5 Siga los mensajes del asistente para crear el grupo.

En la página Configuración del grupo de escritorios, configure las siguientes opciones.

Opción	Descripción
Protocolo de visualización predeterminado	VMware Blast
Permitir que los usuarios elijan el protocolo	No
Representador 3D	Administrar mediante vSphere Client para escritorios con 2D o vDGA y NVIDIA GRID vGPU para escritorios con vGPU

Nota La configuración del grupo es obligatoria. De lo contrario, es posible que no pueda conectarse al escritorio y obtenga un error de protocolo o una pantalla en negro.

- 6 Una vez creado el grupo de escritorios, autorice a los usuarios en las máquinas del grupo de escritorios. En Horizon Console, seleccione el grupo de escritorios y, a continuación, seleccione **Autorizaciones > Agregar autorización** y agregue usuarios o grupos.

Las máquinas virtuales Linux están listas para ser usadas como escritorios remotos en una implementación de Horizon 7.

Administrar grupos de escritorios Linux

Cuando crea un grupo de escritorios y agrega máquinas Linux al grupo, puede administrar los grupos de escritorios manuales si configura las opciones. Debe agregar solo los sistemas operativos invitados Linux al grupo de escritorios manual. Si el grupo contiene tanto sistemas operativos Windows como sistemas operativos Linux, se considerará un grupo Windows y no podrá conectar los escritorios Linux.

Compatibilidad de las operaciones de administración

- Deshabilitar o habilitar grupo de escritorios
- Grupo de escritorios automatizado de clonación
- Eliminar grupo de escritorios

Puede eliminar máquinas virtuales desde Horizon 7 o bien desde el disco.

Compatibilidad de la configuración remota

Tabla 7-1. Configuración remota

Opción remota	Opciones
Directiva de alimentación de máquinas remotas	<ul style="list-style-type: none"> ■ No realizar ninguna acción de alimentación ■ Asegurarse de que las máquinas siempre estén encendidas ■ Suspende ■ Apagar
Cerrar sesión automáticamente tras desconectarse	<ul style="list-style-type: none"> ■ Inmediatamente ■ Nunca ■ Después de n minutos
Permitir a los usuarios restablecer o reiniciar sus máquinas	<ul style="list-style-type: none"> ■ Sí ■ No
Permitir que los usuarios inicien sesiones independientes desde dispositivos cliente diferentes	<ul style="list-style-type: none"> ■ Sí ■ No
"Eliminar máquina después de cerrar sesión" para grupos de escritorios automatizados flotantes y clones completos	<ul style="list-style-type: none"> ■ Sí ■ No

Soporte para las operaciones de Horizon Console

- Desconectar sesión
- Cerrar sesión
- Restablecer/reiniciar un escritorio
- Enviar mensaje

Para grupos de escritorios dedicados, puede agregar o eliminar una asignación de usuario de cada máquina virtual. Cuando realice un gran número de operaciones, debe utilizar los cmdlets de Horizon PowerCLI.

- Actualizar-PropiedadDelUsuario
- Eliminar-PropiedadDelUsuario

Nota No cambie las opciones del **protocolo de visualización remota**. Esta configuración debe ser la misma que la especificada cuando se creó el grupo de escritorios.

Configuración	Opción
Protocolo de visualización predeterminado	VMware Blast
Permitir que el usuario elija el protocolo	No
Representador 3D	<ul style="list-style-type: none"> ■ Administrar mediante vSphere Client para 2D o vDGA ■ NVIDIA GRID vGPU

Para obtener más información, consulte la documentación de *Administración de VMware Horizon Console*.

Cree un grupo de escritorios automatizado de clones completos para Linux

Puede crear un grupo de escritorios automatizado de clones completos para máquinas virtuales Linux. Después de crear el grupo de escritorios automatizado de clones completos, puede usar las máquinas virtuales Linux como escritorios remotos en una implementación de Horizon 7.

A continuación se indica cómo configurar los ajustes obligatorios de un grupo de escritorios automatizado de clones completos basado en Linux. Para obtener más información sobre cómo crear grupos automatizados de clones completos, consulte *Configurar escritorios virtuales en Horizon Console*.

Requisitos previos

- Compruebe que Horizon Agent esté instalado en el sistema operativo invitado de Linux. Consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- Antes de realizar la clonación de máquinas virtuales, debe crear una plantilla de máquina virtual en la que estarán basados los clones. Consulte [Crear una plantilla de máquina virtual para clonar máquinas de escritorios Linux](#).
- Si usa la solución Winbind para unir la máquina virtual Linux a Active Directory, debe terminar de configurar dicha solución en la plantilla de máquina virtual.
- Si usa la solución Winbind, debe ejecutar el comando de unión a un dominio en la máquina virtual. Incluya el comando en un script del shell y especifique la ruta de acceso del script a la opción de Horizon Agent RunOnceScript en `/etc/vmware/viewagent-custom.conf`. Si desea obtener más información, consulte [Opciones de configuración en los archivos de configuración de un escritorio Linux](#).

- Compruebe que vCenter Server se haya añadido al servidor de conexión de Horizon.

Procedimiento

- 1 Cree una especificación de personalización de invitado.

Consulte "Crear una especificación de personalización para Linux en vSphere Web Client" en el documento *Administrar máquinas virtuales de vSphere*. Cuando cree la especificación, asegúrese de que especifica la siguiente configuración correctamente.

Configuración	Valor
SO de la máquina virtual de destino	Linux
Nombre del equipo	Use el nombre de la máquina virtual.
Dominio	Especifique el dominio del entorno de Horizon 7.
Ajustes de red	Use los ajustes de red estándar.
DNS primario	Especifique una dirección válida.

Nota Para obtener más información sobre la matriz de compatibilidad de personalización del SO invitado, consulte <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

- 2 En Horizon Console, agregue un grupo de escritorios automatizado.
Seleccione **Inventario > Escritorios > Agregar**.
- 3 Seleccione **Grupo de escritorios automatizado** y haga clic en **Siguiente**.
- 4 Seleccione **Máquinas virtuales completas**, a continuación seleccione la instancia de vCenter Server y haga clic en **Siguiente**.

5 Siga los mensajes del asistente para crear el grupo.

- a En la página Configuración del grupo de escritorios, configure las siguientes opciones.

Opción	Descripción
Protocolo de visualización predeterminado	VMware Blast
Permitir que los usuarios elijan el protocolo	No
Representador 3D	Administrar mediante vSphere Client para escritorios con 2D o vDGA y NVIDIA GRID vGPU para escritorios con vGPU

- b Cuando se le solicite, establezca las opciones de **Nombre de máquina virtual**.

Opción	Descripción
Especificar nombres de forma manual	Introduzca los nombres de forma manual.
Patrón de nombres	<p>Por ejemplo, especifique LinuxVM-{n}.</p> <p>También debe especificar las siguientes opciones de tamaño de grupo de escritorios:</p> <ul style="list-style-type: none"> ■ Número máximo de máquinas ■ Número de máquinas de reserva encendidas

- c Cuando se le solicite, seleccione los ajustes de vCenter Server en secuencia.

No se puede omitir ninguno de los ajustes de vCenter Server:

- 1 Plantilla
 - 2 Ubicación de la carpeta de la máquina virtual
 - 3 Host o clúster
 - 4 Grupo de recursos
 - 5 Almacenes de datos
- 6 Una vez creado el grupo de escritorios, autorice a los usuarios en las máquinas del grupo de escritorios. En Horizon Console, seleccione el grupo de escritorios y, a continuación, seleccione **Autorizaciones > Agregar autorización** y agregue usuarios o grupos.
- 7 Espere a que queden disponibles todas las máquinas virtuales Linux en el grupo de escritorios.

Crear un grupo de escritorios flotantes de clones instantáneos para Linux

Puede crear un grupo de escritorios flotantes de clones instantáneos para máquinas virtuales Linux con el asistente **Agregar grupo de escritorios**. Después de crear un grupo de escritorios flotantes de clones instantáneos, puede utilizar las máquinas virtuales Linux como escritorios remotos en una implementación de Horizon 7.

Horizon 7 Agent for Linux admite los grupos de escritorios de clones instantáneos solo en sistemas con Ubuntu 18.04/16.04, RHEL 7.1 o versiones posteriores, RHEL 8.0 o SLED/SLES 12.x.

Nota Las funcionalidades de gráficos vGPU no se admiten en los grupos de escritorios de clones instantáneos creados a partir de escritorios Linux.

A continuación se indica cómo configurar los ajustes obligatorios de un grupo de escritorios de clones instantáneos basado en Linux. Para obtener más información sobre cómo crear grupos de escritorios de clones instantáneos, consulte *Configurar escritorios virtuales en Horizon Console*.

Requisitos previos

- Familiarícese con los pasos para crear máquinas virtuales en vCenter Server e instalar sistemas operativos Linux. Si desea obtener más información, consulte [Crear una máquina virtual e instalar Linux](#).
- Consulte los pasos para la integración de AD usando la solución de autenticación PBISO o la solución de unión sin conexión Samba Winbind. Para obtener más información, consulte [Configurar la autenticación PowerBroker Identity Services Open \(PBISO\)](#) o [Configurar la unión a dominio sin conexión mediante Samba](#).

Nota Para crear un grupo de escritorios de clones instantáneos desde una máquina virtual Linux que ejecuta RHEL 8.0, realice la integración de AD usando la solución de unión sin conexión Samba Winbind. Los grupos de escritorios de clones instantáneos no admiten máquinas virtuales RHEL 8.0 que usan la autenticación PBISO.

- Familiarícese con los pasos de instalación de Horizon 7 Agent for Linux. Si desea obtener más información, consulte [Instalar Horizon Agent en una máquina virtual Linux](#).
- Debe saber cómo tomar una snapshot de una máquina virtual Linux apagada usando VMware vSphere Web Client. Consulte la sección sobre cómo tomar una snapshot en VMware Host Client de *Administrar un host único de vSphere: VMware Host Client*.
- Compruebe que vCenter Server esté agregado al servidor de conexión de Horizon.

Procedimiento

- 1 Cree una máquina virtual Linux que tenga instalado Ubuntu 18.04/16.04, RHEL 7.1 o versiones posteriores, RHEL 8.0 o SLED/SLES 12.x.

Si desea obtener más información, consulte [Crear una máquina virtual e instalar Linux](#).

- 2 Use el siguiente comando para instalar manualmente Open VMware Tools (OVT) en su equipo con Ubuntu 18.04/16.04:

```
# apt-get install open-vm-tools
```

Consulte [Preparar una máquina Linux para la implementación de escritorios remotos](#) para obtener más información.

- 3 Instale cualquier paquete de dependencia obligatorio para la distribución de Linux.

Consulte [Instalar paquetes de dependencia para Horizon Agent](#) para obtener más información.

- 4 Instale Horizon Agent for Linux en la máquina virtual Linux.

```
# sudo ./install_viewagent.sh -A yes
```

Consulte [Instalar Horizon Agent en una máquina virtual Linux](#) para obtener más detalles.

- 5 Integre su máquina virtual Linux con Active Directory.

- Para utilizar la solución de autenticación PBISO, siga estos pasos:

- a Descargue PBIS Open 8.5.6 o una versión posterior desde <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> e instálelo en su máquina virtual Linux.

```
# sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- b Integre su máquina virtual Linux con Active Directory usando la información en la sección de autenticación PowerBroker Identity Services Open (PBISO) en [Integrar Linux con Active Directory](#).

- Para usar la solución de unión sin conexión Samba Winbind, asigne a `OfflineJoinDomain` el valor **samba** en el archivo `/etc/vmware/viewagent-custom.conf`.

Nota Debe utilizar Samba Winbind para integrar una máquina virtual RHEL 8.0 con Active Directory. De lo contrario, no se podrá crear el grupo de escritorios flotante de clones instantáneos.

- Si desea deshabilitar la solución de unión a dominio sin conexión, debe asignar a `OfflineJoinDomain` el valor **none** en el archivo `/etc/vmware/viewagent-custom.conf`. De lo contrario, no se podrá crear el grupo de escritorios flotante de clones instantáneos.

- 6 Si el servidor DHCP no transmite a un servidor DNS, especifique un servidor DNS para el sistema Linux.

Cuando se crea una máquina virtual de clon instantáneo, se agrega un nuevo adaptador de red virtual. Cualquier ajuste del adaptador de red (por ejemplo, el servidor DNS) que aparezca en la plantilla de la máquina virtual, se pierde cuando se agrega el nuevo adaptador de red a la máquina virtual de clon instantáneo. PBIS requiere un servidor DNS válido y no se acepta la asignación de FQDN en `/etc/hosts`. Para evitar que se pierda la configuración de servidor DNS cuando se agrega el nuevo adaptador de red a la máquina virtual clonada, debe especificar un servidor DNS en su sistema Linux. Por ejemplo, en un sistema Ubuntu 16.04, especifique el servidor DNS agregando las siguientes líneas en el archivo `/etc/resolvconf/resolv.conf.d/head`.

```
nameserver 10.10.10.10
search mydomain.org
```


- 7 (Opcional) Si desea agregar un montaje NFS en el archivo `/etc/fstab` del agente maestro de clones instantáneos de VDI de Linux, utilice uno de los siguientes métodos.

- Agregue una marca "soft" en `/etc/fstab`, como:

```
10.111.222.333:/share    /home/nfsmount    nfs
size=8192,wsiz=8192,timeo=14,soft,intr,tcp
```

- Si no quiere usar la marca "soft" en `/etc/fstab`, no podrá configurar `/etc/fstab` en la imagen principal de la máquina virtual Linux. Puede escribir un script de desconexión para configurar el archivo `/etc/fstab` y, a continuación, especificar este mismo script para la herramienta ClonePrep. Para obtener más información, consulte el documento *Administración de VMware Horizon Console*.
- 8 Apague la máquina virtual Linux y cree una imagen principal con una snapshot de la máquina virtual Linux desconectada. Para ello, utilice VMware vSphere® Web Client.
- Consulte la sección sobre cómo tomar una snapshot en VMware Host Client de *Administrar un host único de vSphere: VMware Host Client* para obtener más información.
- 9 En Horizon Console, agregue un grupo de escritorios automatizado.
- Seleccione **Inventario > Escritorios > Agregar**.
- 10 Seleccione **Grupo de escritorios automatizado** y haga clic en **Siguiente**.
- 11 Seleccione **Clones instantáneos**; a continuación, seleccione la instancia de vCenter Server y haga clic en **Siguiente**.

12 Siga los mensajes del asistente para crear el grupo.

- a Cuando se le solicite, establezca las opciones de **Nombre de máquina virtual**.

Opción	Descripción
Habilitar aprovisionamiento	Seleccione esta opción.
Detener aprovisionamiento en error	Seleccione esta opción.
Patrón de nombres	Especifique un patrón que Horizon 7 use como un prefijo en todos los nombres de las máquinas virtuales de escritorio, seguido por un número único. Por ejemplo, especifique LinuxVM-{n} .
Número máximo de máquinas	Especifique el número total de máquinas en el grupo.
Número de máquinas de reserva (encendidas)	Especifique el número de máquinas virtuales de escritorio que estarán disponibles para los usuarios.
Aprovisionar todas las máquinas por adelantado	Seleccione esta opción para que Horizon 7 aprovisiona el número de máquinas virtuales especificado en Número máximo de máquinas .

- b Cuando se le solicite, seleccione **Usar VMware Virtual SAN** para la directiva de administración de almacenamiento.
- c Cuando se le solicite, especifique las opciones Dominio, Contenedor de AD y cualquier otro script de personalización que se deba ejecutar después de clonar la máquina virtual.

Importante Cuando utilice los scripts de desconexión o postsincronización de ClonePrep, asegúrese de que estos se encuentren en la carpeta `/var/userScript`, propiedad del usuario raíz, y de que tengan los permisos de archivo establecidos en 700.

En Horizon Console, puede ver las máquinas virtuales de escritorio cuando se agregan al grupo. Para ello, seleccione **inventario > Escritorios**.

Después de crear el grupo, no elimine la imagen principal ni la quite del inventario de vCenter Server mientras el grupo siga existiendo. Si elimina por error la máquina virtual de imagen principal del inventario de vCenter Server, debe volver a agregarla y, a continuación, realizar una imagen de inserción usando la imagen actual.

Pasos siguientes

Autorice a los usuarios a acceder al grupo. Consulte "Agregar autorizaciones a grupos de escritorios" en *Configurar escritorios virtuales en Horizon Console*.

Comandos PowerCLI agente

Los cmdlets de Horizon PowerCLI, que se usan para realizar varias tareas de administración en el servidor de conexión y en un escritorio de Windows, también se pueden usar en escritorios de Linux.

Crear un grupo de escritorios manual

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc|vgpu -
Pool_id <pool id> [more parameters]
```

Las siguientes opciones y valores son obligatorias para el escritorio de Linux.

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threedRender usevc|vgpu. Para un escritorio vGPU, use -threedRender vgpu, y para un escritorio 2D/DGA, use -threedRender usevc.

Ejemplos

- Cree un grupo de escritorios Linux flotante llamado LinuxDesktop con una máquina virtual, LinuxVM-01.

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc -Pool_id
LinuxDesktop -Id (Get-DesktopVM -Name LinuxVM-01).id -Persistence NonPersistent -Vc_name
myvc.myorg.org
```

- Cree un grupo de escritorios Linux vGPU dedicado llamado LinuxDesktop con todas las máquinas virtuales cuyo nombre empiece por LinuxVM-.

```
Get-DesktopVM | Where-Object {$_.Name.StartsWith("LinuxVM-")} | Add-ManualPool -DefaultProtocol
Blast -AllowProtocolOverride $false -Persistence Persistent -threedRender vgpu -Pool_id
LinuxDesktop
```

- Cree un grupo de escritorios Linux flotante LinuxDesktop con la primera máquina virtual de RHEL 6 x64.

```
Get-DesktopVM | Where-Object {$_.GuestID -eq "rhel6_64Guest"} | Select-Object -Index 0 | Add-
ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -Persistence NonPersistent -
threedRender usevc -Pool_id LinuxDesktop
```

Cree un grupo de escritorios automatizado de clones completos

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc|vgpu `
-Pool_id <pool id> -Vc_id <vCenter id> `
-NamePrefix <VM Name Prefix>" `
-templatePath <Virtual Machine Template Path> `
-VmFolderPath <Virtual Machine Folder Path> `
-ResourcePoolPath <Resource Pool Path> `
-dataStorePaths <Datastore Path> `
-customizationSpecName <Customization Specification Name> `
[more parameters]
```

Las siguientes opciones y valores son obligatorios para los escritorios de Linux.

- DefaultProtocol Blast

- `AllowProtocolOverride $false`
- `threadRender usevc|vgpu` Para un escritorio vGPU, use `-threadRender vgpu`, y para un escritorio 2D, use `-threadRender usevc`.

Ejemplo

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadrender usevc `
-pool_id FullClone-Linux `
-Vc_id (Get-ViewVC -serverName myvc.myorg.org).vc_id `
-NamePrefix "FullClone-{n:fixed=3}" `
-Persistence NonPersistent -deletePolicy DeleteOnUse `
-VmFolderPath "/LinuxVDI/vm/FullClone" `
-ResourcePoolPath "/LinuxVDI/host/LinuxVDICluster/Resources" `
-templatePath "/LinuxVDI/vm/LinuxTemplate" `
-dataStorePaths "/LinuxVDI/host/LinuxVDICluster/datastore" `
-customizationSpecName "linux-spec" `
-maximumCount 100
```

Agregar o retirar autorización a un grupo de escritorios

- Autorice a un grupo de usuarios de dominio del dominio mydomain.org para que puedan acceder a LinuxDesktop.

```
Add-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

- Elimine la autorización del dominio mydomain.org de LinuxDesktop para el grupo de usuarios de dominio.

```
Remove-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

Asignar o eliminar usuario de la máquina virtual del grupo de escritorios dedicado

- Asigne **myuser** a la máquina virtual LinuxVM-01 que está en un grupo de escritorios dedicado.

```
Update-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id -Sid (Get-User -
Name "myuser" | Where-Object {$_.cn -eq "myuser"}).sid
```

- Elimine el usuario **myuser** de la máquina virtual LinuxVM-01 que está en un grupo de escritorios dedicado.

```
Remove-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id
```

Desconéctese del escritorio

- Cierre la sesión del escritorio de myuser.

```
Get-RemoteSession -Username "mydomain.org\myuser" | Send-SessionLogoff
```

Si desea obtener más información sobre los cmdlet de PowerCLI relacionados con agentes, consulte "Usar el módulo Horizon PowerCLI" en *Integración de Horizon 7*.

Implementación por lotes de Horizon 7 para grupos de escritorios manuales

8

Con Horizon Console puede crear automáticamente un grupo de máquinas de escritorios Windows, pero no Linux. Sin embargo, puede desarrollar scripts que automaticen la implementación de un grupo de máquinas de escritorios Linux.

Los scripts de ejemplo proporcionados solo tienen fines ilustrativos. VMware no se hace responsable de ningún problema que pueda surgir cuando use los scripts de ejemplo.

Este capítulo incluye los siguientes temas:

- [Descripción general de la implementación por lotes de escritorios Linux](#)
- [Descripción general de la actualización por lotes de escritorios Linux](#)
- [Crear una plantilla de máquina virtual para clonar máquinas de escritorios Linux](#)
- [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#)
- [Script de ejemplo para clonar máquinas virtuales Linux](#)
- [Script de ejemplo para unir máquinas virtuales clonadas a un dominio AD](#)
- [Script de ejemplo para unir máquinas virtuales clonadas a un dominio de AD mediante SSH](#)
- [Script de ejemplo para cargar archivos de configuración en máquinas virtuales Linux](#)
- [Script de ejemplo para cargar archivos de configuración en máquinas virtuales de Linux mediante SSH](#)
- [Script de ejemplo de PowerCLI para actualizar Horizon Agent en máquinas de escritorios Linux](#)
- [Script de ejemplo para actualizar Horizon Agent en máquinas virtuales Linux mediante SSH](#)
- [Script de ejemplo para realizar operaciones en máquinas virtuales Linux](#)

Descripción general de la implementación por lotes de escritorios Linux

Implementar escritorios manuales para Linux por lotes requiere seguir ciertos pasos. Si piensa implementar bastantes escritorios, puede automatizar alguno de estos pasos mediante scripts de PowerCLI.

Para algunas operaciones, puede decidir si va a ejecutar con PowerCLI o con SSH los comandos en la máquina Linux. En la tabla siguiente, se describe las diferencias entre los dos enfoques.

PowerCLI	SSH
No es necesario instalar herramientas adicionales.	<ul style="list-style-type: none"> ■ Para Ubuntu, es necesario instalar el servidor SSH con el comando <code>sudo apt-get install openssh-server</code>. <code>openssh-server</code> está instalado de forma predeterminada en RHEL y en CentOS, pero necesita asegurarse de que la configuración del firewall permita SSH. ■ Es necesario descargar las aplicaciones cliente de SSH <code>pscp.exe</code> y <code>plink.exe</code> y ponerlas en la misma carpeta que los scripts de PowerCLI.
La carga de archivos y la ejecución de comandos son más lentas.	La carga de archivos y la ejecución de comandos son más rápidas.
Es necesario proporcionar las credenciales de administrador del host ESXi.	No es necesario proporcionar las credenciales de administrador del host ESXi.
No admite caracteres especiales en la contraseña del administrador cuando ejecuta el script para instalar Horizon Agent o en la contraseña de usuario del AD cuando ejecuta el script para unirse al dominio.	Admite caracteres especiales en la contraseña del administrador cuando ejecuta el script para instalar Horizon Agent o en la contraseña de usuario de AD cuando ejecuta el script para unirse al dominio.

Nota Tanto los scripts basados en PowerCLI como los scripts basados en SSH admiten caracteres especiales en la contraseña del administrador de vCenter Server y del administrador de Linux. Los scripts basados en PowerCLI también admiten caracteres especiales en la contraseña del administrador del host ESXi. En todos estos casos, no se necesitan caracteres de escape.

Para obtener más información sobre vSphere PowerCLI, consulte <https://www.vmware.com/support/developer/PowerCLI>.

Para implementar por lotes un grupo de escritorios Linux, es necesario seguir estos pasos:

- 1 Cree una plantilla de máquina virtual e instale Horizon Agent en la máquina virtual.

Consulte [Crear una plantilla de máquina virtual para clonar máquinas de escritorios Linux](#).

- 2 Cree una especificación de personalización de invitado.

Consulte "Crear una especificación de personalización para Linux en vSphere Web Client" en el documento *Administrar máquinas virtuales de vSphere*. Cuando cree la especificación, asegúrese de que especifica la siguiente configuración correctamente.

Configuración	Valor
SO de la máquina virtual de destino	Linux
Nombre del equipo	Use el nombre de la máquina virtual.
Dominio	Especifique el dominio del entorno de Horizon 7.

Configuración	Valor
Ajustes de red	Use los ajustes de red estándar.
DNS primario	Especifique una dirección válida.

Nota Para obtener más información sobre la matriz de compatibilidad de personalización del SO invitado, consulte <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

3 Máquinas virtuales clonadas.

Consulte [Script de ejemplo para clonar máquinas virtuales Linux](#).

4 Una las máquinas virtuales clonadas al dominio de Active Directory (AD) si va a utilizar la solución Winbind. Puede ejecutar el comando para unir las al dominio con los scripts de ejemplo que aparecen a continuación o bien con la opción RunOnceScript en /etc/vmware/viewagent-custom.conf, configurada en la plantilla de máquina virtual.

Consulte [Script de ejemplo para unir máquinas virtuales clonadas a un dominio AD](#) o [Script de ejemplo para unir máquinas virtuales clonadas a un dominio de AD mediante SSH](#).

5 Actualizar las opciones de configuración de máquinas virtuales.

Consulte [Script de ejemplo para cargar archivos de configuración en máquinas virtuales Linux](#) o [Script de ejemplo para cargar archivos de configuración en máquinas virtuales de Linux mediante SSH](#).

6 Cree un grupo de escritorios.

Consulte [Crear un grupo de escritorios manual para Linux](#).

Para un script de ejemplo que realice operaciones como encendido, apagado, reinicio o eliminación de máquinas virtuales, consulte [Script de ejemplo para realizar operaciones en máquinas virtuales Linux](#). El script puede eliminar máquinas virtuales de vCenter Server.

Descripción general de la actualización por lotes de escritorios Linux

La actualización por lotes de escritorios manuales para Linux requiere seguir ciertos pasos. Puede automatizar algunos de estos pasos mediante scripts de PowerCLI.

Actualizar por lotes escritorios no administrados

Para actualizar por lotes la máquina virtual no administrada a una máquina virtual administrada o no administrada, debe usar el script de ejemplo de actualización para cargar el nuevo Horizon Agent en las máquinas virtuales existentes y ejecutar el comando de actualización.

- Si conserva la máquina virtual no administrada, su grupo de escritorios existente podrá volver a usarse.

- Si actualiza de una máquina virtual no administrada a una máquina virtual administrada, debe eliminar el grupo de escritorios existente y crear uno nuevo. Si desea obtener más información, consulte [Actualizar Horizon Agent en una máquina virtual Linux](#).

Actualizar por lotes escritorios administrados

Para actualizar por lotes la máquina virtual no administrada, seleccione uno de los siguientes métodos.

Método	Descripción
En la plantilla de máquina virtual, instale o actualice el nuevo Horizon Agent y cree una snapshot.	<ul style="list-style-type: none"> ■ Como las máquinas virtuales existentes se eliminan, se pierden todos los datos y perfiles de usuario excepto los que se encuentren en un servidor compartido como el servidor NFS. ■ Después de sustituir la máquina virtual, es posible que el estado de la máquina virtual no aparezca en View Administrator. Deberá reiniciar el servicio agente para solucionar el problema.
Use el script de ejemplo de actualización para cargar el nuevo Horizon Agent en las máquinas virtuales existentes y ejecute el comando de actualización.	Los datos y los perfiles de usuario se conservan.

Crear una plantilla de máquina virtual para clonar máquinas de escritorios Linux

Antes de realizar la clonación de máquinas virtuales, debe crear una plantilla de máquina virtual en la que se basen los clones.

Requisitos previos

- Compruebe que su implementación cumpla los requisitos para ser compatible con escritorios Linux. Consulte [Requisitos del sistema para Horizon 7 for Linux](#).
- Familiarícese con los pasos para crear máquinas virtuales en vCenter Server e instalar sistemas operativos invitados. Consulte "Crear y preparar máquinas virtuales" en el documento *Configurar escritorios virtuales en Horizon 7*.
- Familiarícese con los valores de memoria de vídeo (vRAM) necesarios para los monitores que debe usar con la máquina virtual. Consulte [Configuración de máquinas virtuales para gráficos 2D](#).
- Familiarícese con los pasos para la integración de AD. Consulte [Capítulo 3 Configurar la integración de Active Directory para escritorios Linux](#).
- Familiarícese con los pasos para instalar Horizon Agent en Linux. Consulte [Capítulo 5 Instalar Horizon Agent](#).
- Si fuera necesario, familiarícese con los pasos para configurar las opciones mediante los archivos de configuración de Horizon 7. Consulte [Capítulo 6 Opciones de configuración para escritorios Linux](#).
- Si planea configurar los gráficos, familiarícese con los pasos. Consulte [Capítulo 4 Configurar gráficos para escritorios Linux](#).

Procedimiento

- 1 En vSphere Web Client o vSphere Client, cree una nueva máquina virtual.
- 2 Configure las opciones de configuración personalizada.
 - a Haga clic con el botón secundario en la máquina virtual y haga clic en **Editar configuración**.
 - b Especifique el número de vCPU y el tamaño de la vMemory.

Siga las directrices de tamaño de vCPU y vMemory de la guía de instalación para su distribución de Linux.

Por ejemplo, Ubuntu 18.04 especifica que se configuren 2.048 MB para vMemory y 2 vCPU.
 - c Seleccione **Tarjeta de vídeo** y especifique el número de pantallas y la memoria de vídeo total (vRAM).

Consulte el tamaño de vRAM en vSphere Web Client para máquinas virtuales que usan 2D, que utilizan el controlador de VMware. El tamaño de vRAM no tiene efecto sobre máquinas con vDGA o NVIDIA GRID vGPU, que usan controladores de NVIDIA.

Siga las directrices de [Configuración de máquinas virtuales para gráficos 2D](#). No use la Calculadora de memoria virtual.
- 3 Encienda la máquina virtual e instale la distribución de Linux.
- 4 Cree un usuario con privilegios de usuario raíz, como ViewUser. Este usuario se utiliza para instalar y desinstalar solamente Horizon Agent.
- 5 Edite /etc/sudoers y agregue la línea ViewUser ALL=(ALL) NOPASSWD:ALL.

Con esta línea en /etc/sudoers, no se requiere ninguna contraseña para ejecutar sudo como ViewUser. Al ejecutar el script de muestra para instalar Horizon Agent que se proporciona en este capítulo, especifica ViewUser como entrada.
- 6 Si la distribución de Linux es RHEL, CentOS o NeoKylin, edite /etc/sudoers y ponga marcas de comentarios a las siguientes líneas:


```
Defaults requiretty
Defaults !visiblepw
```
- 7 Si la distribución de Linux no es RHEL/CentOS 8.x, RHEL/CentOS 7.x o SLED/SLES 12.x, instale VMware Tools.

RHEL/CentOS 8.0, RHEL/CentOS 7.x y SLED/SLES 12.x tiene Open VM Tools instalado de forma predeterminada.

8 Instale y configure los paquetes de dependencia.

- a Si la distribución de Linux ejecuta una versión de Open VM Tools anterior a la 9.10, instale el complemento deployPkg.

Encontrará las instrucciones en <http://kb.vmware.com/kb/2075048>.

- b Si la distribución de Linux es Ubuntu, consulte los siguientes artículos de la base de conocimientos para determinar qué paquetes de dependencia se deben instalar y configurar en la máquina virtual.

- Consulte los artículos de la base de conocimientos <https://kb.vmware.com/s/article/2051469> y <https://kb.vmware.com/s/article/59687> para Ubuntu 18.04 y 16.04.
- Para Ubuntu 18.04, consulte también el artículo de la base de conocimientos <https://kb.vmware.com/s/article/56409>.

9 Para RHEL y CentOS, habilite el ajuste de la conexión de red **Conectar automáticamente**.**10** Realice las tareas de integración de AD.**11** Realice los pasos necesarios para configurar los gráficos.**12** Instale Horizon Agent.

```
sudo ./install_viewagent.sh -A yes
```

Consulte [Capítulo 5 Instalar Horizon Agent](#).

13 Realice configuraciones adicionales mediante los archivos de configuración de Horizon 7.**14** Apague la máquina virtual y cree una snapshot.

Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux

Los scripts PowerCLI de ejemplo para implementar escritorios Linux leen un archivo de entrada que contiene información sobre las máquinas de escritorios.

El archivo de entrada es de tipo csv y contiene la siguiente información:

- Nombre de la máquina virtual de escritorio
- Nombre de la máquina virtual principal
- Especificación de personalización de invitado
- Almacén de datos donde reside la máquina del escritorio clonado
- Servidor ESXi que aloja la máquina de escritorios
- Snapshot de la máquina virtual principal que se usa para la clonación
- Marcador que indica si se puede borrar la máquina virtual de escritorios (en caso de que exista)

El siguiente ejemplo muestra lo que podría contener el archivo de entrada.

```
VMName,Parentvm,CustomSpec,Datastore,Host,FromSnapshot,DeleteIfPresent
linux-001,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-002,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-003,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-004,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-005,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
```

Los scripts de ejemplo asumen que el nombre del archivo de entrada es `CloneVMs.csv` y que el archivo se encuentra en la misma carpeta que los scripts.

Script de ejemplo para clonar máquinas virtuales Linux

Puede personalizar y usar el siguiente script de ejemplo para clonar el número de máquinas virtuales que desee.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en <https://docs.vmware.com/es/VMware-Horizon-7/index.html>.

Entrada del script

Este script lee un archivo de entrada que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Tipo de clon, que solo puede ser completo
- Deshabilitar o no una consola de máquina virtual de vSphere

Contenido del script

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone from Master VM.
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
```

```

        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ()
{
    Param($VMExists)
    Write-Host "Checking if the VM $VMExists already Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
        }
    }
    return $Exists
}

function Disable_VM_Console()
{
    Param($VMToDisableConsole)
    $vmConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
    $extra = New-Object VMware.Vim.optionvalue
    $extra.Key="RemoteDisplay.maxConnections"
    $extra.Value="0"
    $vmConfigSpec.extraconfig += $extra
    $vm = Get-VM $VMToDisableConsole | Get-View
    $vm.ReconfigVM($vmConfigSpec)
}

function Delete_VM()
{
    Param($VMToDelete)
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Main Script -----

$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false

```

```

$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
$cloneType = GetInput -prompt 'Clone Type ("full")' -IsPassword $false
$disableVMConsole = GetInput -prompt 'Disable vSphere VM Console ("yes" or "no", recommend "yes")' -
IsPassword $false
"-----"
$csvFile = '.\CloneVMs.csv'

# Check that user passed only full clone
if (($CloneType.length > 0) -and ($CloneType -ne "full"))
{
    write-host -ForegroundColor Red "Clone type supports only 'full' (case sensitive)"
    exit
}
if (($disableVMConsole.length > 0) -and ($disableVMConsole -ne "yes" -or $disableVMConsole -ne "no"))
{
    write-host -ForegroundColor Red "Disable vSphere VM Console supports only 'yes' or 'no' (case
sensitive)"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File $CSVFile not found"
    exit
}

# Connect to the VC (Parameterize VC)
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile
#$csvData = Import-CSV $csvFile -
header("VMName","Parentvm","CustomSpec","Datastore","Host","FromSnapshot","DeleteIfPresent")
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $destVMName=$line.VMName
    $srcVM = $line.Parentvm
    $cSpec = $line.CustomSpec
    $targetDSName = $line.Datastore

```

```

$destHost = $line.Host
$srcSnapshot = $line.FromSnapshot
$deleteExisting = $line.DeleteIfPresent
if (IsVMExists ($destVMName))
{
    Write-Host "VM $destVMName Already Exists in VC $vcAddress"
    if($deleteExisting -eq "TRUE")
    {
        Delete_VM ($destVMName)
    }
    else
    {
        Write-Host "Skip clone for $destVMName"
        continue
    }
}
$vm = get-vm $srcvm -ErrorAction Stop | get-view -ErrorAction Stop
$cloneSpec = new-object VMware.VIM.VirtualMachineCloneSpec
$cloneSpec.Location = new-object VMware.VIM.VirtualMachineRelocateSpec
Write-Host "Using Datastore $targetDSName"
$newDS = Get-Datastore $targetDSName | Get-View
$cloneSpec.Location.Datastore = $newDS.summary.Datastore
Set-VM -vm $srcVM -snapshot (Get-Snapshot -vm $srcVM -Name $srcSnapshot) -confirm:$false
$cloneSpec.Snapshot = $vm.Snapshot.CurrentSnapshot
$cloneSpec.Location.Host = (get-vmhost -Name $destHost).Extensiondata.MoRef
$cloneSpec.Location.Pool = (Get-ResourcePool -Name Resources -Location (Get-VMHost -Name
$destHost)).Extensiondata.MoRef
# Start the Clone task using the above parameters
$task = $vm.CloneVM_Task($vm.parent, $destVMName, $cloneSpec)
# Get the task object
$task = Get-Task | where { $_.id -eq $task }
#Wait for the taks to Complete
Wait-Task -Task $task

$newvm = Get-vm $destVMName
$customSpec = Get-OSCustomizationSpec $cSpec
Set-vm -OSCustomizationSpec $cSpec -vm $newvm -confirm:$false
if ($disableVMConsole -eq "yes")
{
    Disable_VM_Console($destVMName)
}
# Start the VM
Start-VM $newvm
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```
PowerCLI C:\scripts> .\CloneVMs.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
Clone Type<"Full"> : Full
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes
```

El tiempo que tarde el proceso de clonación depende del número de máquinas de escritorio y puede variar de unos minutos a varias horas. Para verificar que el proceso se completó, acceda a vSphere Client y asegúrese de que la última máquina virtual de escritorio esté encendida, que tenga un nombre de host único y que VMware Tools se esté ejecutando.

Script de ejemplo para unir máquinas virtuales clonadas a un dominio AD

Para unir máquinas virtuales (VM) clonadas a un dominio de Active Directory (AD), se puede personalizar y utilizar el siguiente script de ejemplo.

Es necesario ejecutar este script si se usa la solución Winbind para la integración de AD ya que el paso para unirse al dominio fallará en las máquinas virtuales clonadas. Este script ejecuta un comando para unirse al dominio en cada máquina virtual. No es necesario ejecutar este script si se usa la solución OpenLDAP.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de administrador para el host ESXi
- Contraseña de administrador para el host ESXi
- Nombre de inicio de sesión de usuario para la máquina virtual Linux
- Contraseña de usuario para la máquina virtual Linux
- Nombre de inicio de sesión de un usuario de AD con autorización para unir máquinas al dominio

■ Contraseña del usuario de AD autorizado

Contenido del script

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join"

.DESRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux to AD

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#----- Handle input -----
"-----"
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"
Please type the AD user password."
"Plase note that special character in password may not work with the script"
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"
```

```

# $csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain.ps1

-----

Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----

Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****

-----

Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

```
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character in password may not work with the script.
Your AD user password: *****
```

Script de ejemplo para unir máquinas virtuales clonadas a un dominio de AD mediante SSH

Puede personalizar y usar el siguiente script de ejemplo para unir máquinas virtuales clonadas a un dominio de Active Directory (AD). Este script usa SSH para ejecutar comandos en las máquinas virtuales de Linux.

Es necesario ejecutar este script si se usa la solución Winbind para la integración de AD ya que el paso para unirse al dominio fallará en las máquinas virtuales clonadas. Este script ejecuta un comando para unirse al dominio en cada máquina virtual. No es necesario ejecutar este script si se usa la solución OpenLDAP.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de usuario para la máquina virtual Linux
- Contraseña de usuario para la máquina virtual Linux
- Nombre de inicio de sesión de un usuario de AD con autorización para unir máquinas al dominio
- Contraseña del usuario de AD autorizado

Contenido del script

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join" via SSH

.DESRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux machine to AD via SSH

.NOTES
```

```
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}
}
```

```

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $false
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
""
Please type the AD user password."
[Console]::ForegroundColor = "Yellow"
"Plase note that special character should be escaped. For example, $ should be \$\"
[Console]::ResetColor()
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

```

```

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain_SSH.ps1
-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character should be escaped. For example, $ should be \$
Your AD user password: *****

```

Script de ejemplo para cargar archivos de configuración en máquinas virtuales Linux

Puede personalizar y usar el siguiente script de ejemplo para cargar los archivos de configuración config y viewagent-custom.conf en varias máquinas virtuales Linux.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de administrador para el host ESXi
- Contraseña de administrador para el host ESXi
- Nombre de inicio de sesión de usuario para la máquina virtual Linux
- Contraseña de usuario para la máquina virtual Linux

Contenido del script

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }
}
```

```

[Console]::ResetColor()
return $input
}

#----- Handle Input -----
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword

```



```

if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $config_File

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $customConf_File

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }
}

```

```

    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

Script de ejemplo para cargar archivos de configuración en máquinas virtuales de Linux mediante SSH

Puede personalizar y usar el siguiente script de ejemplo para cargar los archivos de configuración config y viewagent-custom.conf en varias máquinas virtuales Linux. Este script usa SSH para ejecutar comandos en las máquinas virtuales de Linux.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de usuario para la máquina virtual Linux
- Contraseña de usuario para la máquina virtual Linux

Contenido del script

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs using SSH
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}
```

```

    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle Input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists

```

```

if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

```

```

if ($setConfig)
{
    Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$config_File -DestPath $destFolder

    $cmd = "sudo mv ./ $config_File /etc/vmware/";
    Write-Host "Move configuraton file: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

if ($setCustomConf)
{
    Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$customConf_File -DestPath $destFolder

    $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
    Write-Host "Move configuraton file: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

Script de ejemplo de PowerCLI para actualizar Horizon Agent en máquinas de escritorios Linux

Puede personalizar y usar el siguiente script de ejemplo para actualizar Horizon Agent en varias máquinas virtuales Linux.

El script carga el archivo tar comprimido (.gz) del instalador en cada máquina virtual antes de instalar Horizon Agent. La tarea de carga puede requerir un tiempo considerable, sobre todo si hay un número considerable de máquinas virtuales y la velocidad de la red es baja. Para ahorrar tiempo, puede ejecutar el script que usa SSH o poner el archivo tar del instalador en una ubicación compartida que esté disponible para todas las máquinas virtuales, de modo que no sea necesario cargar el archivo.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en <https://docs.vmware.com/es/VMware-Horizon-7/index.html>.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Aceptación del acuerdo de licencia de usuario final (EULA) de Horizon Agent
- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de administrador para el host ESXi
- Contraseña de administrador para el host ESXi
- Nombre de inicio de sesión de usuario para el sistema operativo invitado Linux
- Contraseña de usuario para el sistema operativo invitado Linux
- Ruta de acceso del archivo tar comprimido (.gz) de Horizon Agent
- Actualizar a máquina virtual administrada
- Instalar la función de redireccionamiento de tarjeta inteligente

Contenido del script

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {

```

```

        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#-----Handle
input-----
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the Horizon Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))

```



```

{
write-host -ForegroundColor Red "CSV File not found"
exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "").ToLower());
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -

```

Source \$agentInstaller

```
#Check the uploaded installer md5sum
$cmd = "md5sum VMware-*linux-*"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
$output = Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -
GuestUser $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

if($output.Contains($installerMD5Hash))
{
    Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    Write-Host $VMName": Extract the installer and do installation";
    $cmd = "tar -xzf VMware-*linux-*.tar.gz"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -A yes -m $installSmartcard -M
$UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo shutdown -r +1&"
    Write-Host "Reboot to apply the Horizon Agent installation"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit
```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```
PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: HorizonUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no
```

Script de ejemplo para actualizar Horizon Agent en máquinas virtuales Linux mediante SSH

Puede personalizar y usar el siguiente script de ejemplo para actualizar Horizon Agent en varias máquinas virtuales Linux. Este script usa SSH para ejecutar comandos en las máquinas virtuales de Linux.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Aceptación del contrato de licencia de usuario final (EULA) de Horizon Agent
- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Nombre de inicio de sesión de administrador para el host ESXi
- Contraseña de administrador para el host ESXi
- Nombre de inicio de sesión de usuario para el sistema operativo invitado Linux

- Contraseña de usuario para el sistema operativo invitado Linux
- Ruta de acceso del archivo tar de Horizon Agent
- Actualizar a máquina virtual administrada
- Instalar la función de redireccionamiento de tarjeta inteligente

Contenido del script

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
```

```

    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file $LocalPath to VM $VM_Name with user $User"
    Invoke-Expression $command
}

#-----Handle
input-----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
}

```

```

        exit
    }
    $svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
    $svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
    $svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
    "-----"
    $guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
    $guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
    "-----"
    $agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
    "-----"
    $UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
    if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
    {
        write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
        exit
    }
    $installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
    IsPassword $false
    if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
    {
        write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
        exit
    }
    "-----"

    # $csvFile = Read-Host 'Csv File '
    $csvFile = '.\CloneVMs.csv'

    #check if file exists
    if (!(Test-Path $agentInstaller))
    {
        write-host -ForegroundColor Red "installer File not found"
        exit
    }

    #check if file exists
    if (!(Test-Path $csvFile))
    {
        write-host -ForegroundColor Red "CSV File not found"
        exit
    }
    #-----
    Functions-----
    function GetSourceInstallerMD5()
    {
        $agentInstallerPath = Convert-Path $agentInstaller;
        $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
        $md5HashWithFormat =
        [System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
        ;
        $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
        return $md5Hash;
    }

```

```
#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$agentInstaller -DestPath $destFolder

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    $output = RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd -
$returnOutput $true

    if($output.Contains($installerMD5Hash))
    {
        Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
        Write-Host $VMName": Extract the installer and do installation";

        $cmd = "tar -xzf VMware-*linux-*.tar.gz"
        Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

        $cmd = "sudo setenforce 0";
    }
}
```

```

Write-Host "Set the selinux to permissive mode: $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

$cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

#Run the upgrade command.
$cmd = "cd VMware-*--linux-* && sudo ./install_viewagent.sh -r yes -A yes -m $installSmartcard
-M $UpgradeToManagedVM"
Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
Write-Host -ForegroundColor Yellow "Linux Agent installer will reboot the Linux VM after
upgrade, and you may hit the ssh connection closed error message, which is expectation"
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```


Script de ejemplo para realizar operaciones en máquinas virtuales Linux

Puede personalizar y usar el siguiente script de ejemplo para realizar operaciones en varias máquinas virtuales Linux. Las operaciones incluyen encendido, desconexión, apagado, reinicio y eliminación de las máquinas virtuales.

Este script puede eliminar máquinas virtuales desde vCenter Server pero no desde View.

Para copiar y pegar el contenido del script sin saltos de página, use la versión HTML de este tema, disponible en la página de documentación de Horizon 7 en https://www.vmware.com/support/pubs/view_pubs.html.

Entrada del script

Este script lee un archivo de entrada, que se describe en [Archivo de entrada de los scripts PowerCLI de ejemplo para implementar escritorios Linux](#). Este script también solicita de manera interactiva la siguiente información:

- Dirección IP de vCenter Server
- Nombre de inicio de sesión de administrador para vCenter Server
- Contraseña de administrador para vCenter Server
- Acción que se realizará, que puede ser encendido, desconexión, apagado del invitado, reinicio de la máquina virtual, reinicio del invitado de máquina virtual o eliminación de la máquina virtual.
- El tiempo de espera, en segundos, entre las operaciones de las máquinas virtuales.

Contenido del script

```
<#
.DESCRIPTION
The Tool supports:
1. Power off VMs
2. Power on VMs
3. Shutdown VMs
4. Restart VMs
5. Restart VM guest
6. Delete VMs from Disk
.NOTES
#>

#----- Functions -----

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
```

```

    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ($VMExists)
{
    Write-Host "Checking if the VM $VMExists Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
            Write-Host "$VMExists is Exist"
        }
    }
    return $Exists
}

function Delete_VM($VMToDelete)
{
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"

$action = GetInput -prompt 'Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4).
Restart VM 5). Restart VM Guest 6). Delete VM' -IsPassword $false
$sleepTime = GetInput -prompt 'Wait time (seconds) between each VM' -IsPassword $false
"-----"

[Console]::ForegroundColor = "Yellow"
switch ($action)
{
    1
    {

```

```

    "Your selection is 1). Power On"
}
2
{
    "Your selection is 2). Power Off"
}
3
{
    "Your selection is 3) Shutdown"
}
4
{
    "Your selection is 4). Restart VM"
}
5
{
    "Your selection is 5). Restart VM Guest"
}
6
{
    "Your selection is 6). Delete VM"
}
default
{
    "Invalid selection for action: $action"
    exit
}
}
[Console]::ResetColor()
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
"-----"

#----- Main -----
#Read input CSV file
Disconnect-VIServer $vcAddress -Confirm:$false
#Connect-VIServer $vcAddress -ErrorAction Stop -user $vcAdmin -password $vcPassword
Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
$csvData = Import-CSV $csvFile

foreach ($line in $csvData)
{
    $VMName = $line.VMName
    switch ($action)
    {
        1
        {
            Get-VM $VMName | Start-VM -Confirm:$false
        }
    }
}

```

```

2
{
    Get-VM $VMName | Stop-VM -Confirm:$false
}
3
{
    Get-VM $VMName | Shutdown-VMGuest -Confirm:$false
}
4
{
    Get-VM $VMName | Restart-VM -Confirm:$false
}
5
{
    Get-VM $VMName | Restart-VMGuest -Confirm:$false
}
6
{
    if (IsVMExists ($VMName))
    {
        Delete_VM ($VMName)
    }
}
default{}
}
Start-Sleep -s $sleepTime
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Ejecución del script

Los siguientes mensajes son de una ejecución del script:

```

PowerCLI C:\scripts> .\VMOperations.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4). Restart VM 5). Restart VM Guest
6). Delete VM: 1
Wait time (seconds) between each VM: 20
-----
Your selection is 6). Delete VM

```

Para las operaciones de encendido, reinicio de la máquina virtual y reinicio del invitado de la máquina virtual, especifique un tiempo de espera entre máquinas virtuales de al menos 20 segundos para evitar sobrecargas que puedan causar fallos en operaciones.

Solucionar los problemas de escritorios Linux

9

Pueden aparecer algunos problemas cuando administre escritorios Linux. Puede seguir varios procedimientos para diagnosticar y fijar los problemas.

Este capítulo incluye los siguientes temas:

- [Usar Horizon Help Desk Tool en Horizon Console](#)
- [Recopilar información de diagnóstico de máquinas con Horizon 7 for Linux](#)
- [Se produce un error en Horizon Agent al desconectarse de Horizon Client para iPad Pro](#)
- [El escritorio SLES 12 SP1 no se actualiza automáticamente](#)
- [SSO no puede conectarse a un agente de desconexión](#)
- [No se puede acceder a la máquina virtual después de crear un grupo de escritorios manual para Linux](#)

Usar Horizon Help Desk Tool en Horizon Console

Horizon Help Desk Tool es una aplicación web que puede utilizar para obtener el estado de las sesiones de usuario de Horizon 7 y para realizar operaciones de mantenimiento y de solución de problemas.

En Horizon Help Desk Tool, puede buscar sesiones de usuarios para solucionar problemas y realizar operaciones de mantenimiento de escritorios, como reiniciarlos y restablecerlos.

Para configurar Horizon Help Desk Tool, debe cumplir los siguientes requisitos:

- Licencia de la edición Horizon Enterprise o de la edición Horizon Apps Advanced para Horizon 7. Para comprobar que tiene la licencia correcta, consulte el documento *Administración de Horizon 7*.
- Una base de datos de eventos para almacenar información acerca de los componentes de Horizon 7. Para obtener más información sobre cómo configurar una base de datos de eventos, consulte el documento *Administración de Horizon 7*.
- Las funciones Administrador del departamento de soporte técnico o Administrador del departamento de soporte técnico (solo lectura) para iniciar sesión en Horizon Help Desk Tool. Para obtener más información sobre estas funciones, consulte el documento *Administración de Horizon 7*.

- Habilite el generador de perfiles en cada instancia del servidor de conexión para ver los segmentos de inicio de sesión.

Utilice el siguiente comando `vdmadmin` para habilitar el generador de perfiles de intervalos en cada instancia del servidor de conexión:

```
vdmadmin -I -timingProfiler -enable
```

Utilice el siguiente comando `vdmadmin` para habilitar el generador de perfiles de intervalos en una instancia del servidor de conexión que use un puerto de administración:

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

- Habilite la opción `HelpDeskEnable` en el archivo de configuración `/etc/vmware/viewagent-custom.conf`.

Iniciar Horizon Help Desk Tool en Horizon Console

Horizon Help Desk Tool está integrado en Horizon Console. Puede buscar un usuario al que quiera solucionarle problemas en Horizon Help Desk Tool.

Procedimiento

- 1 Puede buscar un nombre de usuario en el cuadro de texto **Búsqueda de usuarios** o ir directamente a la herramienta **Horizon Help Desk Tool**.
 - En Horizon Console, introduzca un nombre de usuario en el cuadro de texto **Búsqueda de usuarios**.
 - Seleccione **Supervisor > Departamento de soporte técnico** e introduzca un nombre de usuario en el cuadro de texto **Búsqueda de usuarios**.

Horizon Console muestra una lista de usuarios en los resultados de búsqueda. La búsqueda puede devolver 100 resultados de coincidencia.

- 2 Seleccione un nombre de usuario.

La información del usuario aparece en una ficha de usuario.

Pasos siguientes

Para solucionar problemas, haga clic en las pestañas pertinentes de la ficha de usuario.

Solucionar los problemas de los usuarios en Horizon Help Desk Tool

En Horizon Help Desk Tool, puede consultar la información básica del usuario gracias a una ficha de usuario. Puede hacer clic en las pestañas de la ficha de usuario para obtener más información sobre los componentes específicos.

En ocasiones, los detalles de los usuarios pueden aparecer en tablas. Puede ordenar estos detalles en columnas.

- Para ordenar una columna en orden ascendente, haga clic una vez en la columna.
- Para ordenar una columna en orden descendente, haga clic dos veces en la columna.
- Para no ordenar la columna, haga clic en la columna tres veces.

Información básica del usuario

Muestra la información básica del usuario, como el nombre, el número de teléfono y la dirección de correo electrónico, así como si está conectado o desconectado. Si el usuario tiene una sesión de escritorio, el estado es conectado. Si el usuario no tiene ninguna sesión de escritorio, el estado es desconectado.

También puede hacer clic en la dirección de correo electrónico para enviarle un mensaje al usuario.

Sesiones

La pestaña **Sesiones** muestra la información sobre las sesiones de escritorios a las que el usuario está conectado.

Puede utilizar el cuadro de texto **Filtrar** para filtrar las sesiones de escritorios.

Nota La pestaña **Sesiones** no muestra información de las sesiones que acceden a las máquinas virtuales desde vSphere Client o ESXi.

La pestaña **Sesiones** incluye la siguiente información:

Tabla 9-1. Pestaña Sesiones

Opción	Descripción
Estado	<p>Muestra información sobre el estado de la sesión de escritorio.</p> <ul style="list-style-type: none"> ■ Si la sesión está conectada, aparece en verde. ■ L, si la sesión es local o si una sesión se ejecuta en el pod local.
Nombre del equipo	<p>Nombre de la sesión de escritorios. Haga clic en el nombre para abrir la información de la sesión en una ficha.</p> <p>Puede hacer clic en las pestañas de la ficha de sesión para ver información adicional:</p> <ul style="list-style-type: none"> ■ La pestaña Detalles muestra la información del usuario, como la información de la máquina virtual, la CPU o el uso de memoria. ■ La pestaña Procesos muestra la información de los procesos relacionados con la CPU y la memoria.
Protocolo	Protocolo de visualización para la sesión de escritorios.
Tipo	Indica si el escritorio es un escritorio publicado o de una máquina virtual.

Tabla 9-1. Pestaña Sesiones (continuación)

Opción	Descripción
Hora de conexión	La hora a la que se conectó la sesión al servidor de conexión.
Duración de la sesión	El tiempo durante el cual la sesión permaneció conectada al servidor de conexión.

Escritorios

La pestaña **Escritorios** muestra información sobre los escritorios publicados y los virtuales para los que el usuario tiene autorización.

Tabla 9-2. Escritorios

Opción	Descripción
Estado	Muestra información sobre el estado de la sesión de escritorio. ■ Si la sesión está conectada, aparece en verde.
Nombre de grupo de escritorios	Nombre del grupo de escritorios de la sesión.
Tipo de escritorio	Indica si el escritorio es un escritorio publicado o de máquina virtual. Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.
Tipo	Muestra información sobre el tipo de autorización de escritorio. ■ Local, para una autorización local.
vCenter	Muestra el nombre de la máquina virtual de vCenter Server. Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.
Protocolo predeterminado	Protocolo de visualización predeterminado de la sesión de escritorio.

Actividades

La pestaña **Actividades** muestra la información de los registros de eventos referentes a las actividades de los usuarios. Puede filtrar las actividades por un intervalo de tiempo, como por las últimas 12 horas, los últimos 30 días o por nombre de administrador. Haga clic en **Solo eventos del departamento de soporte técnico** para filtrar únicamente por actividades de Horizon Help Desk Tool. Haga clic en el icono de actualización para actualizar el registro de eventos. Haga clic en el icono de exportación para exportar el registro de eventos a un archivo.

Nota No se muestra la información del registro de eventos para los usuarios en un entorno Arquitectura Cloud Pod.

Tabla 9-3. Actividades

Opción	Descripción
Time	<p>Seleccione un intervalo de tiempo. El valor predeterminado es las últimas 12 horas.</p> <ul style="list-style-type: none"> ■ Últimas 12 horas ■ Últimas 24 horas ■ Últimos 7 días ■ Últimos 30 días ■ Todo
Administradores	Nombre del usuario administrador.
Mensaje	Muestra los mensajes de un usuario o administrador que sean específicos a las actividades que el usuario o administrador realizó.
Nombre del recurso	Muestra información sobre el nombre de la máquina virtual o del grupo de escritorios en el que se realizó la actividad.

Detalles de las sesiones para Horizon Help Desk Tool

La información de las sesiones aparece en la pestaña **Detalles** cuando hace clic en el nombre de un usuario en la opción **Nombre del equipo** que aparece en la pestaña **Sesiones**. Puede consultar información sobre Horizon Client y sobre la CPU y la memoria, así como el escritorio virtual o publicado.

Cliente

La información que muestra depende del tipo de Horizon Client e incluye detalles como el nombre de usuario, la versión de Horizon Client, la dirección IP del equipo cliente y el sistema operativo del equipo cliente.

Nota Si actualizó Horizon Agent, debe actualizar también Horizon Client a la versión más reciente. En caso contrario, no se muestra ninguna versión de Horizon Client. Para obtener más información sobre cómo actualizar Horizon Client, consulte el documento *Actualizaciones de Horizon 7*.

MV

Muestra información acerca de los escritorios virtuales o publicados.

Tabla 9-4. Detalles de la máquina virtual

Opción	Descripción
Nombre del equipo	Nombre de la sesión de escritorios.
Versión del agente	Versión de Horizon Agent.
Versión del SO	Versión del sistema operativo.
Servidor de conexión	El servidor de conexión al que la sesión está conectada.
Grupo	Nombre del grupo de escritorios.
vCenter	Dirección IP de vCenter Server.

Tabla 9-4. Detalles de la máquina virtual (continuación)

Opción	Descripción
Estado de la sesión	Estado de la sesión de los escritorios. Los estados de la sesión pueden ser conectado o desconectado.
Duración de la sesión	El tiempo durante el cual la sesión permaneció conectada al servidor de conexión.
Duración del estado	El tiempo durante el cual la sesión se mantuvo en el mismo estado.
Hora de inicio de sesión	La hora en la que el usuario inició la sesión.
Duración de inicio de sesión	La duración durante la que el usuario tiene la sesión iniciada en el escritorio de Linux.

Indicadores de la experiencia del usuario

Muestra información sobre el rendimiento de una sesión de escritorio publicada o virtual que usa el protocolo de visualización VMware Blast. Para consultar esta información sobre el rendimiento, haga clic en **Más**. Para actualizar esta información, haga clic en el icono para actualizar.

Tabla 9-5. Detalles del protocolo de visualización Blast

Opción	Descripción
Velocidad de fotogramas	La velocidad de fotogramas (en fotogramas por segundo) de una sesión Blast.
Estado de Skype	Para sesiones de escritorio de Linux, esta opción aparece como N/D.
Contadores de sesiones de BLAST	<ul style="list-style-type: none"> ■ Ancho de banda estimado (enlace ascendente). Ancho de banda estimado de la señal del enlace ascendente. ■ Pérdida de paquetes (enlace ascendente). Porcentaje de pérdida de paquetes de la señal del enlace ascendente.
Contadores de imágenes de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos de imágenes transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos de imágenes recibidos durante una sesión Blast.
Contadores de audio de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos de audio transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos de audio recibidos durante una sesión Blast.
Contadores de CDR de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos del redireccionamiento de la unidad cliente transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos del redireccionamiento de la unidad cliente recibidos durante una sesión Blast.

Rendimiento de disco y red, y uso de la memoria y la CPU

Muestra gráficos del uso de memoria y de CPU de los escritorios virtuales o publicados, y el rendimiento de disco o de red del protocolo de visualización Blast.

Nota Después de iniciar o reiniciar Horizon Agent en el escritorio, es posible que los gráficos de rendimiento no muestren la escala de tiempo inmediatamente. La escala de tiempo aparece después de algunos minutos.

Tabla 9-6. Uso de CPU

Opción	Descripción
CPU de la sesión	Uso de CPU de la sesión actual.
CPU del host	Uso de CPU de la máquina virtual a la que está asignada la sesión.

Tabla 9-7. Uso de memoria

Opción	Descripción
Memoria de la sesión	Uso de memoria de la sesión actual.
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.

Tabla 9-8. Rendimiento de la red

Opción	Descripción
Latencia	Muestra un gráfico de la latencia de la sesión Blast o PCoIP. El tiempo de latencia es el tiempo de ida y vuelta en milisegundos. El contador de rendimiento que realiza un seguimiento de este tiempo de latencia es Contadores de VMware Blast Session > RTT .

Tabla 9-9. Rendimiento del disco

Opción	Descripción
Lectura	El número de operaciones de entrada o salida (E/S) por segundo.
Escritura	El número de operaciones de E/S de escritura por segundo.
Latencia de disco	Muestra un gráfico con la latencia de disco. La latencia de disco es el tiempo en milisegundos de los datos de operaciones de E/S por segundo recuperados de los contadores de rendimiento de Windows.
Promedio de lectura	El número de operaciones de E/S de lectura por segundo.
Promedio de escritura	El número promedio de operaciones de E/S de escritura por segundo.
Promedio de latencia	Tiempo medio de latencia en milisegundo de los datos E/S por segundo recuperados de los contadores de rendimiento de Windows.

Segmentos de inicio de sesión

Muestra los segmentos de uso y de duración del inicio de sesión que se crean durante el proceso de inicio de sesión.

Tabla 9-10. Segmentos de inicio de sesión

Opción	Descripción
Duración de inicio de sesión	El periodo de tiempo calculado desde el momento en el que el usuario hace clic en el grupo de escritorios hasta el momento en el que el usuario inicia sesión en el escritorio de Linux.
Hora de inicio de la sesión	El tiempo durante el cual el usuario tuvo la sesión iniciada.
Segmentos de inicio de sesión	<p>Muestra los segmentos que se crean durante el inicio de sesión.</p> <ul style="list-style-type: none"> ■ Brokering. Tiempo total que tarda el servidor de conexión en procesar una conexión de sesión o en volver a conectarse. Se calcula desde que el usuario hace clic en el grupo de escritorios hasta la hora en la que se configura la conexión del túnel. Incluye los tiempos para tareas del servidor de conexión, como la autenticación del usuario, la selección del equipo y la preparación del equipo para configurar la conexión del túnel. ■ Interactivo. Tiempo total que tarda Horizon Agent en procesar una conexión de sesión o en volver a conectarse. Se calcula desde el momento en el que Blast Extreme usa la conexión en túnel hasta el momento en el que el usuario inicia sesión en el escritorio de Linux. ■ Conexión de protocolo. Tiempo total que tarda la conexión del protocolo PCoIP o Blast en completarse durante el proceso de inicio de sesión. ■ Script de inicio de sesión. Tiempo total que tarda un script de inicio de sesión en ejecutarse desde que se inicia hasta que se completa. ■ Autenticación. Tiempo total que tarda el servidor de conexión en autenticar la sesión. ■ Inicio de máquina virtual. Tiempo total que tarda una máquina virtual en iniciarse. Este tiempo incluye el tiempo que tarda en arrancar el sistema operativo, en reanudar una máquina en suspensión y el tiempo que tarda Horizon Agent en notificar que está preparado para establecer una conexión.

Procesos de las sesiones de Horizon Help Desk Tool

Los procesos de las sesiones aparecen en la pestaña **Procesos** cuando hace clic en el nombre de un usuario en la opción **Nombre del equipo** que aparece en la pestaña **Sesiones**.

Procesos

Puede consultar información adicional sobre los procesos de CPU y memoria de cada sesión. Por ejemplo, si advierte que el uso de memoria y de CPU de una sesión es demasiado elevado, puede consultar información del proceso en la pestaña **Procesos**.

En las sesiones del host RDS, la pestaña **Procesos** muestra los procesos de sesiones actuales del host RDS iniciadas por el proceso del sistema actual o el usuario actual.

Tabla 9-11. Detalles de los procesos de las sesiones

Opción	Descripción
Nombre del proceso	Nombre del proceso de la sesión. Por ejemplo, chrome.exe.
CPU	Porcentaje del uso de CPU del proceso.
Memoria	KB del uso de memoria del proceso.
Disco	E/S por segundo del disco de memoria. Se calcula con la siguiente fórmula: (Bytes de E/S totales en este momento) - (Bytes de E/S totales un segundo después). Este cálculo puede resultar en un valor de 0 KB por segundo si el Administrador de tareas muestra un valor positivo.
Nombre de usuario	Nombre del usuario propietario del proceso.
CPU del host	Uso de CPU de la máquina virtual a la que está asignada la sesión.
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.
Procesos	Recuento de procesos de la máquina virtual
Actualizar	El icono de actualización actualiza la lista de procesos.
Finalizar proceso	Finaliza un proceso que se está ejecutando. Nota Debe tener la función Administrador del departamento de soporte técnico. Para finalizar un proceso, selecciónelo y haga clic en el botón Finalizar proceso . No puede finalizar procesos críticos, como los procesos de núcleo de Windows, que puedan aparecer en la pestaña Procesos . Si finaliza un proceso crítico, Horizon Help Desk Tool muestra un mensaje que indica que no puede finalizar el proceso del sistema.

Solucionar problemas de sesiones de escritorios de Linux en Horizon Help Desk Tool

En Horizon Help Desk Tool, puede solucionar los problemas de las sesiones de escritorios de Linux según el estado de conexión del usuario.

Requisitos previos

- Inicie Horizon Help Desk Tool.

Procedimiento

- 1 En la ficha de usuario, haga clic en la pestaña **Sesiones**.

Aparece una ficha de rendimiento que muestra el uso de la memoria y la CPU, e incluye la información sobre Horizon Client y el escritorio virtual o publicado.

- 2 Seleccione una opción para solucionar el problema.

Opción	Acción
Enviar mensaje	Envía un mensaje al usuario del escritorio virtual o publicado. Puede seleccionar que la gravedad del mensaje incluya Advertencia, Información o Error. Haga clic en Enviar mensaje , escriba el tipo de gravedad y los detalles del mensaje y, a continuación, haga clic en Enviar .
Reiniciar	Inicia el proceso de reinicio en el escritorio virtual. Esta función no está disponible para una sesión de escritorio publicado. Haga clic en Reiniciar VDI .
Desconectar	Desconectar la sesión de aplicación o de escritorio. Haga clic en Más > Desconectar .
Cerrar sesión	Inicia el proceso de cierre de sesión para un escritorio publicado o un escritorio virtual. Haga clic en Más > Cerrar sesión .
Restablecer	Inicia el restablecimiento de la máquina virtual. Esta función no está disponible para un escritorio publicado. Haga clic en Más > Restablecer máquina virtual .
Nota El usuario puede perder el trabajo no guardado.	

Recopilar información de diagnóstico de máquinas con Horizon 7 for Linux

Puede recopilar información de diagnóstico para ayudar al equipo de soporte técnico de VMware a diagnosticar y resolver problemas con una máquina con Horizon 7 for Linux. Usted crea un paquete de herramientas de recopilación de datos (Data Collection Tool, DCT) que recopila los registros y la información de configuración de la máquina en un archivo tar comprimido.

Procedimiento

- 1 Inicie sesión en la máquina virtual Linux como un usuario con los privilegios requeridos.
- 2 Abra una ventana del símbolo del sistema y ejecute el script `dct-debug.sh`

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

El script genera un archivo tar que contiene el paquete de DCT. Por ejemplo:

```
ubuntu-12-vdm-sdct-20150201-0606-agent.tgz
```

El archivo tar se genera en el directorio desde el que se ejecutó el script (el directorio de trabajo actual).

Se produce un error en Horizon Agent al desconectarse de Horizon Client para iPad Pro

Se produce un error en la conexión SUSE de Horizon Agent al desconectarse después de reiniciar o apagar Horizon Client en el iPad Pro.

Problema

Cuando reinicia o apaga una máquina virtual SUSE en iPad Pro Horizon Client, el escritorio no responde. Horizon Agent no se puede desconectar.

Causa

Es posible que la máquina SUSE no mande mensajes correctamente a Horizon Client después de operaciones de reinicio o de apagado.

Solución

- ◆ Desconecte el escritorio de forma manual desde iPad Pro Horizon Client.

El escritorio SLES 12 SP1 no se actualiza automáticamente

SLES 12 SP1 no se actualiza automáticamente en modo multimonitor cuando arrastra GNOME Terminal.

Problema

Cuando inicia SLES 12 SP1 en modo multimonitor y vuelve al modo ventana, el escritorio no se actualiza automáticamente cuando arrastra un GNOME Terminal.

Causa

El GNOME Terminal no responde a la operación de arrastrar.

Solución

- 1 Cierre la sesión de GNOME Shell.

```
kill -9 <process id of gnome-shell>
```

- 2 Vuelva a iniciar la sesión de GNOME Shell.

SSO no puede conectarse a un agente de desconexión

Single Sign-On (SSO) no puede conectarse a un agente PowerOff.

Problema

Cuando inicia sesión como agente y se conecta a otro agente, SSO no puede conectarse al agente PowerOff.

Solución

- ◆ Inicie sesión manualmente en el escritorio o desconecte y vuelva a conectar el agente.

No se puede acceder a la máquina virtual después de crear un grupo de escritorios manual para Linux

La máquina virtual no responde.

Problema

El estado de la máquina virtual debe ser Esperando al agente o No se puede acceder después de crear un grupo de escritorios manual.

Causa

Es posible que existan varias causas en la configuración o que el usuario cometiera algún error durante el proceso de configuración para que el estado de la máquina virtual sea No se puede acceder o Esperando al agente.

- Verifique que la opción `machine.id` exista en el archivo de configuración `vmx` de las máquinas virtuales.

Si no existe, verifique que la máquina virtual se agregara al grupo de escritorios correctamente. Además, vuelva a crear el grupo de escritorios para que el agente vuelva a escribir la opción en el archivo de configuración `vmx`.

- Verifique que VMware Tool u Open VM Tool estén instalados correctamente.

Si los pasos para instalar VMware Tool u Open VM Tool no se realizaron correctamente, es posible que el comando `vmware-rpctool` no exista en `PATH` de la máquina virtual Linux. Debe seguir las instrucciones para instalar VMware Tool u Open VM Tool.

Ejecute el comando después de finalizar la instalación.

```
#vmware-rpctool "machine.id.get"
```

Los valores de `machine.id` se enumeran a partir del archivo de configuración `vmx` de las máquinas virtuales.

- Verifique si el FQDN del agente se puede resolver en la Dirección IP de la máquina virtual Linux agente.